International Journal of Advanced Science and Technology
Vol.63, (2014), pp.83-94
http://dx.doi.org/10.14257/ijast.2014.63.08

Cyber Warfare: Worms' Transmission Model

Bimal Kumar Mishra and Apeksha Prajapati

Department of Applied Mathematics, Birla Institute of Technology, Mesra, Ranchi, India – 835 215

drbimalmishra@gmail.com, prajapatiapeksha@gmail.com

Abstract

The major way of attack in cyber world is cyber war. Cyber war is a form of war which takes places on computers and the Internet, through electronic means rather than physical ones. With an increasing global reliance on technology for everything from managing national electrical grids to ordering supplies for troops the security of cyber world become an important issue worldwide. In this paper, an e-epidemic SEIR (susceptible-Exposed-Infectious-Recovered) model for the transmission of worms in a computer network is developed to have a better understanding of the reason for Cyber war. An analysis of the basic reproduction number has been made. We derive global stability of a worm-free state. Furthermore, initial simulation results show the positive impact of increasing security measures on worm propagation in computer network. Efficiency of antivirus software and crashing of the nodes due to worms attack is critically analyzed.

Keywords: *Cyber war, Epidemic model, Malicious code, Basic Reproduction number*

1. Introduction

There is no doubt the Internet is a wondrous creation. The entire world is rapidly becoming obsessed with it. In today's world, the internet is considered to be one of the most useful tools for people to communicate, find information and to buy goods and services. Most computers are connected to each other in some way. They usually share the same operating system software and communicate with all other computers using the standard set of TCP/IP protocols. This has spawned a new generation of criminals. These cyber criminals develop programs or software called malicious codes that invades the government computers as well as personal computer and starts gathering information such as financial or personal details.

The Internet is the primary medium used by attackers to commit computer crimes. Worms' attacks are considered by network experts the highest security risk on computer network. Computers worms are built to propagate without warning or user interaction, causing an increase in traffic service requests that will eventually lead to Cyber attack. Attacker uses a malicious worm as a primary tool to target software vulnerabilities. Cyber attacks occur on a frequent basis and in a near-instantaneous manner, as the world becomes more connected, more machines and more people will be affected by an attack. A successful cyber war could inflict major damage on both a country's information infrastructure and its utility grids [1].

ISSN: 2005-4238 IJAST

The Slammer worm, for example, exploited a vulnerability in Microsoft's SQL database software that led to cascading effects in our electronic infrastructure that were certainly not predicted earlier. Airline booking systems and bank Automated Teller Machines (ATMs) were among other systems impacted by Slammer infections. The Slammer worm also significantly degraded computer systems that control monitoring capabilities at the Davis-Besse nuclear power plant in Ohio. The most likely targets of cyber warfare are critical networks. Critical networks are those that if interrupted for significant portions of time (several days or several weeks or indefinitely) or perform erratically or occasionally would disrupt daily life.

We can stop these crimes from happening by simply installing the best kind of internet security software available. Antivirus programs are designed to protect computers and used to prevent, detect and remove malware. A variety of strategies are usually employed. Signature-based detection involves searching for known patterns of data within executable code. However, it is possible for a computer to be infected with new malware for which no signature is yet recognized. To optimize the performance of antivirus it is prefer to update it in regular interval.

1.1 Related works.

The similarity between the spread of a biological virus and worm propagation encourages researchers to adopt an epidemic model to the network environment [24].Epidemic system particularly it deals with infectious disease. In these models, the estimation of parameters is usually based on statistical methods, starting from data obtained experimentally to the choice of the method adapted to their identification. Recently, more research attention has been paid to the combination of virus/worms propagation model and antivirus countermeasures to study the dominance of virus and worms, e.g., virus immunization [2, 5, 15]. Pattern of global cyber war and crime, the way of attack has discussed [1].There is an ample literature on the different model in epidemiology [6-8, 11, 14], starting with the work of Kermack and McKendrick SIR classical epidemic model [14, 20-21]. More and more scholars have conducted research on the vaccinations of virus in email networks [9, 16, 24]. Research in modeling computer viruses and worms implement epidemic models like SIS [25]. Dynamical models for malicious objects propagation were proposed, providing estimations for temporal evolutions of nodes depending on network parameters [18, 19]. A key concept in these studies is the basic reproductive number R_0 [2-4, 10], which denotes the expected number of secondary infective caused by a single primary infective. If $R_0 > 1$, the infection spreads to some sizeable fraction of the entire population; if $R_0 < 1$, then the fraction eventually infected is close to zero.

The subsequent content of this paper is organized as follows: Section 2 introduces SEIR model. Section 3 and 4 describe equilibrium points and basic reproduction number. Next section explains about global stability of the infectious-free equilibrium point. Section 6, finally summarizes the work with simulated results.

2. Formulation of SEIR Models

A simple classical epidemic worm's transmission model on cyber war illustrates the dynamics of direct transmission of worms among susceptible, exposed, infected and recovered classes of the computer network. I and R denote the Infective and recovered class respectively.

b is the inclusion rate of new nodes for susceptible class. μ is the death rate due to worms attack. δ is the crashing rate of the nodes in the network. β is infectivity contact rate, τ is the infection rate in exposed class. We have also assumed that, there is vital dynamics. The susceptible individuals are assumed to have logistic growth with carrying capacity $k > 0$ as well as an intrinsic growth rate $r > 0$. The performance of the antivirus software in a network is limited due to (i) gap time log in having updated antivirus software (ii) cost effectiveness, so we consider the following recovery function:

$$Re(I) = \begin{cases} \rho I & if\ 0 \leq I \leq I_{min} \\ \xi & if\ I > I_{min} \end{cases}$$

Where ρ is the recovery rate when the antivirus is not fully utilized, $\xi = \rho I_{min}$.

The flow of worms in computer network can be depicted in Figure 1.

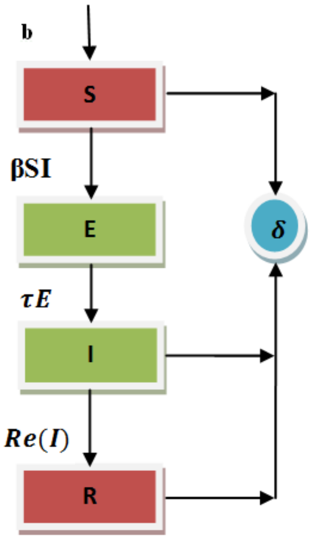

Figure 1. The flow of worms in computer network

The set of differential equations which governs the model is

$$\begin{aligned} \frac{dS}{dt} &= rS\left(1-\frac{S}{k}\right) - \beta SI - \delta S \\ \frac{dE}{dt} &= \beta SI - (\tau + \delta)E \\ \frac{dI}{dt} &= \tau E - (\mu + \delta)I - Re(I) \\ \frac{dR}{dt} &= Re(I) - \delta R \end{aligned} \qquad (1)$$

The first three equations of (1) are independent of R so we can consider the reduced model

$$\frac{dS}{dt} = rS\left(1-\frac{S}{k}\right) - \beta SI - \delta S$$

$$\frac{dE}{dt} = \beta SI - (\tau + \delta)E \qquad (2)$$

$$\frac{dI}{dt} = \tau E - (\mu + \delta)I - Re(I)$$

3. Solution and Equilibrium Points

Equilibrium points are the points where the variables do not change with time. In order to know about the growth of infected nodes, that is, the number of infected nodes increases indefinitely or not, we study the stability of equilibrium points.

To study the stability of model (2), first, we find the equilibrium points at steady states of the model which satisfy the following equations:

$$\frac{dS}{dt} = 0, \frac{dE}{dt} = 0, \frac{dI}{dt} = 0$$

The system of equation (2) reduces to

$$\left.\begin{aligned} \frac{dS}{dt} &= rS\left(1 - \frac{S}{k}\right) - \beta SI - \delta S \\ \frac{dE}{dt} &= \beta SI - (\tau + \delta)E \\ \frac{dI}{dt} &= \tau E - (\mu + \delta + \rho)I \end{aligned}\right\} \quad \text{if } 0 \le I \le I_{min} \qquad (3)$$

and,

$$\left.\begin{aligned} \frac{dS}{dt} &= rS\left(1 - \frac{S}{k}\right) - \beta SI - \delta S \\ \frac{dE}{dt} &= \beta SI - (\tau + \delta)E \\ \frac{dI}{dt} &= \tau E - (\mu + \delta)I - m \end{aligned}\right\} \quad \text{if}, I > I_{min} \qquad (4)$$

System (3) has trivial equilibrium $E_0 = (0,0,0)$,worm-free equilibrium point

$E_0^* = \left(\frac{k(r-\delta)}{r}, 0,0\right)$and endemic equilibrium at

$$E = (S^*, E^*, I^*) = \left(\frac{a(\delta+\tau)}{\beta\tau}, \frac{a}{\tau}\frac{r(k\beta-a\delta-a\tau)-k\delta\beta\tau}{\tau k\beta^2}, \frac{r(k\beta-a\delta-a\tau)-k\delta\beta\tau}{k\tau\beta^2}\right)$$

Where $a = \delta + \rho + \mu$

E_0^* is worm free equilibrium of (3) if and only if $0 < R_0 < \frac{1}{r-\delta k-k\beta I_{min})}$

From (4) we get,

$$\tau\beta^2 kI^2 - nI + mq = 0$$

Where $n = \tau k\beta(r - \delta) - r(\delta + \tau)(\mu + \delta) and\ q = r(\tau + \delta)$

$I_1 = \frac{n+\sqrt{t}}{2k\tau\beta^2}$ and $I_2 = \frac{n-\sqrt{t}}{2k\tau\beta^2}$ where $t = n^2 - 4mqk\tau\beta^2$

Accordingly

$$E_1 = (S_1, I_1) = \left(\frac{k\{(r-\delta)2k\tau\beta^2 - \beta(n+\sqrt{t})\}}{2k\tau\beta^2}, \frac{n+\sqrt{t}}{2k\tau\beta^2}\right)$$

$$E_2 = (S_2, I_2) = \left(\frac{k\{(r-\delta)2k\tau\beta^2 - \beta(n-\sqrt{t})\}}{2k\tau\beta^2}, \frac{n-\sqrt{t}}{2k\tau\beta^2}\right)$$

E_1 *and* E_2 are worm free equilibrium points if $I_1, I_2 > I_{min}$ which is equivalent to $2k\tau\beta^2 I_{min} - n \leq \sqrt{t}$.

Jacobian are given as

$$\begin{bmatrix} r - \frac{2rS}{k} - \beta SI - \delta & 0 & -\beta S \\ \beta I & -(\tau+\delta) & \beta S \\ 0 & \tau & -(\mu+\delta+\rho) \end{bmatrix} \qquad (5)$$

and

$$\begin{bmatrix} r - \frac{2rS}{k} - \beta SI - \delta & 0 & -\beta S \\ \beta I & -(\tau+\delta) & \beta S \\ 0 & \tau & -(\mu+\delta) \end{bmatrix} \qquad (6)$$

From (5) at E_0 eigenvalues are $(r-\delta), -(\tau+\delta) and\ -(\mu+\delta+\rho)$ for (3), when $r-\delta < 0$

From (6) at E_0 eigenvalues are $r-\delta, -(\tau+\delta) and\ -(\mu+\delta)$ for (4), when $r-\delta < 0$

E_0 is locally globally asymptotically stable if $r - \delta < 0$

At E_0^*,

$$J = \begin{bmatrix} r - \frac{2rS}{k} - \delta & 0 & -\beta S \\ \beta I & -(\tau+\delta) & \beta S \\ 0 & \tau & -(\mu+\delta) \end{bmatrix}$$

eigenvalues are $r-\delta, \frac{-f-\sqrt{g^2-4f}}{2}, \frac{-f+\sqrt{g^2-4f}}{2}$, when $r-\delta < 0$ and $f > \sqrt{g^2-4f}$

where $f = 2\delta + \mu + \tau\ and\ g = (\delta+\tau)(\mu+\delta) - \frac{\beta\tau k(r-\delta)}{r}$

E_0^* is locally asymptotically stable.

4. The basic Reproduction number(R_0)

It is defined as the expected number of new cases of infection caused by an infected introduced into the susceptible population.

The basic reproduction number can be obtained by calculating V and F. The F is the new infections; while the V represents transfers of infections from one compartment to another where V and F are given as,

$$V = \begin{bmatrix} \delta+\tau & 0 \\ -\tau & \mu+\delta+\rho \end{bmatrix}, \qquad F = \begin{bmatrix} 0 & \beta \\ 0 & 0 \end{bmatrix}$$

The basic reproduction number is given by the dominant Eigen value of FV^{-1}.

That is, $R_0 = \frac{\beta\tau}{(\delta+\tau)(\mu+\delta+\rho)}$, which states that the worm will not be in the network if $\frac{\beta\tau}{(\delta+\tau)(\mu+\delta+\rho)} < 1$ and it will attack the network if $\frac{\beta\tau}{(\delta+\tau)(\mu+\delta+\rho)} > 1$.

5. Global Stability of the Worms-free Equilibrium

Theorem 1: If $R_0 < 1$ the worm- free equilibrium E_0^* is locally asymptotically stable. If $R_0 = 1, E_0^*$ is stable; $R_0 > 1$, E_0^* is unstable.
Let $f_\infty = \lim_{t\to\infty} inf_{\theta\geq t}\, f(\theta), f^\infty = \lim_{t\to\infty} sup_{\theta\geq t}\, f(\theta)$
Lemma 1*:* Assume that a bounded real valued function $f: [0, \infty) \to R$ is twice differentiable with bounded second derivative.Let k → ∞ and f(t_k) converges to $f^\infty\, or\, f_\infty$ then $\lim_{t\to\infty} f'(t_k) = 0$.

Theorem 1: If $R_0 < 1$ then the worm - free equilibrium E_0^* is globally asymptotically stable.

Proof: From system (3), we have

$$\frac{dS}{dt} \leq rS\left(1 - \frac{S}{k}\right) - \delta S$$

A solution of the equation $\frac{dX}{dt} \leq rX\left(1 - \frac{X}{k}\right) - \delta X$ is super solution of S(t)

Since x→ $\frac{k(r-\delta)}{r}$ as t→∞, then for a given ε > 0 there exists a t_0 such that

$$S(t) \leq X(t) \leq \frac{k(r-\delta)}{r} + \varepsilon\; for\; all\; t \geq t_0$$

Thus $S^\infty \leq X(t) \leq \frac{k(r-\delta)}{r} + \varepsilon$

Let ε→0 then $S^\infty \leq \frac{k(r-\delta)}{r}$

Second equation of (3) reduces to

$$\frac{dE}{dt} = \beta I \frac{k(r-\delta)}{r} - (\tau + \delta)E \tag{7}$$

Now taking third equation of (3) with (7)

$$\begin{bmatrix} \dot{E} \\ \dot{I} \end{bmatrix} \leq P \begin{bmatrix} E \\ I \end{bmatrix} \tag{8}$$

$$\mathrm{P} = \begin{bmatrix} -(\delta+\tau) & 0 \\ \tau & -(\mu+\delta+\rho) \end{bmatrix}$$

Let $M \in R^+$, such that $M \geq max\;((\delta+\tau),\; (\mu+\delta+\rho))$

Thus $P + M\, I_{2\times2}$ is a strictly positive matrix if $\omega_{1,}$ and ω_2 are the eigen values of P then ω_1 + M, ω_2+ M are eigen value of $P + M\, I_{2\times2}$. Thus form the Perron- Frobenius theorem [12]. $P + M\, I_{2\times2}$ has a simple positive eigen value equal to dominant eigen value and corresponding eigen vector e > 0, which implies that ω_1 and ω_2 are real. If ω_1+M is the dominant eigen value of $P + M\, I_{2\times2}$, then $\omega_1 > \omega_2$and eP = e^{ω_1}. Obviously ω_1 , ω_2 are the roots of the equation

$$\lambda^2 + (\tau + \mu + 2\delta + \rho)\lambda + (\delta + \tau)(\mu + \delta + \rho) = 0 \tag{9}$$

Since $R_0 < 1$ for $\varepsilon > 0$, sufficiently small, we have,

$$(\delta + \tau)(\mu + \delta + \rho) > 0$$

Therefore, the coefficients of the quadratic equation (9) are positive

Thus ω_1, ω_2 all are negative, from equation (9), for $t \geq t_0$

$$\frac{d}{dt}(e[E(t), I(t)]) \leq \omega_1 . e[E(t), I(t)]$$

Integrating the above in equation, we have,

$$0 \leq e.[E(t), I(t)] \leq e.[E(t_1), I(t_1)]e^{\omega_1(t-t_1)}\, for\, t \geq t_1 \geq t_0$$

Since $\omega_1 < 0$, $e.[E(t), I(t)] \to 0\ as\ t \to \infty$

Using $e > 0$, we have $E(t), I(t) \to (0,0)\ as\ t \to \infty$

By lemma 1, we choose a sequence $t_n \to \infty , S_n \to \infty(n \to \infty)$ such that $S(S_n) \to S^\infty$

S(t_n)→ S_∞, $\dot{S}$ (S_n) → 0, $\dot{S}$(t_n) → 0

Since $E(t), I(t) \to 0\ for\ t \to \infty$ thus from the first equation of (2), we have,

$$\lim_{n\to\infty} S(t) = \frac{k(r-\delta)}{r}$$

Hence, by incorporating lemma1, the worm-free equilibrium E_0^* is globally asymptotically stable, if $R_0 < 1$.

Similarly we can show that $E_0^*and\ E\ are$ globally asymptotically stable, if $R_0 < 1$.

6. Conclusion

Due to the latent time between the susceptible and the infectious state, the e-SEIR epidemic model is more suitable for modeling worm attack in a computer network than a computer virus. Figure 2 and 3 show the system behavior with respect to time and behavior of infected nodes versus Recovered node respectively. The recovery of the nodes from the attack of worms is very high approximately 95% when antivirus software is run appropriate interval of time, which is clearly observed from Figure 2. With an approximately calculated value of $R_0 = 0.55$, the result show highest recovery in the worm infection network. Figure 4 and 5 show the worms' propagation with respect to time and phase plot of susceptible class with respect to Infectious class. The simulated results, supported by the theoretical approach show that all worms died out when the basic reproduction rate is smaller than one.

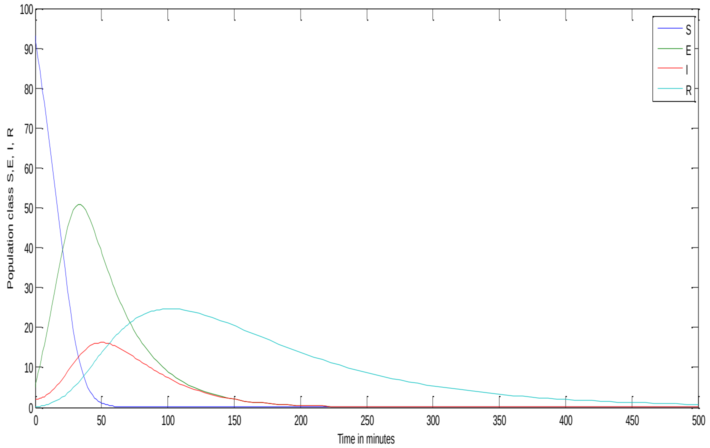

Figure 2. Dynamical behavior of the system with time when $R_0 < 1$ and $\mathbf{I_{min}} = 2$

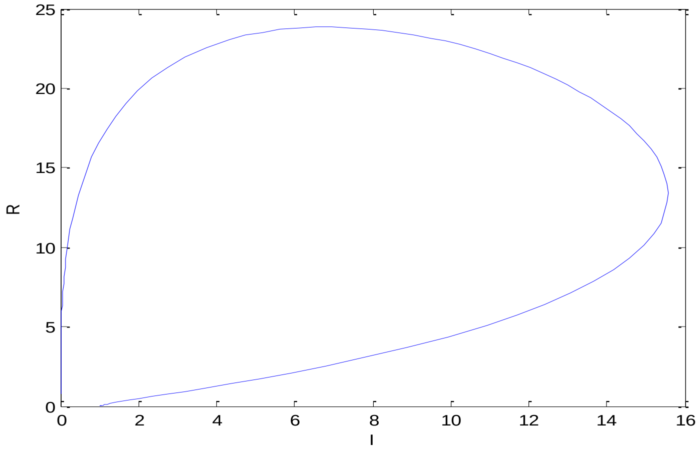

Figure 3. Dynamical behavior of Recovered class versus Infectious class

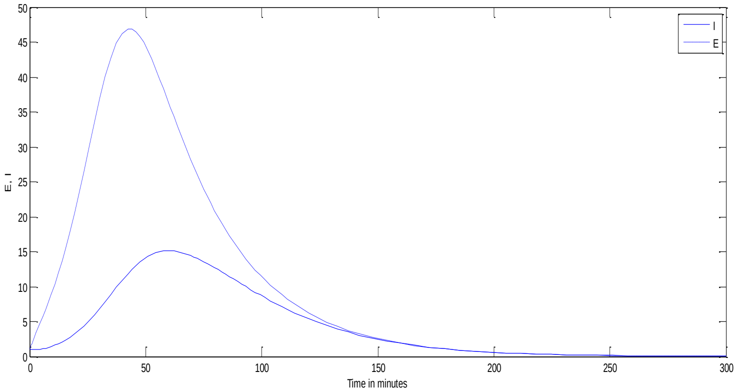

Figure 4. Worms' propagation with respect to time

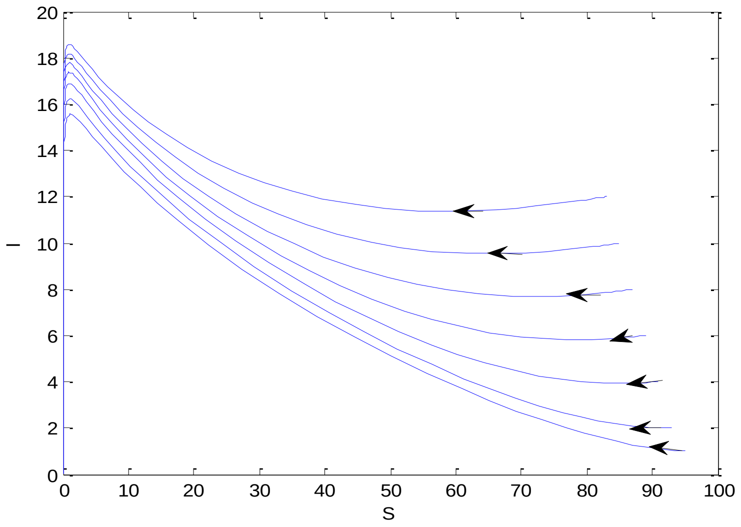

Figure 5. Phase plot S versus I

Table 1.

Notation	Explanation	Initial value
S(t)	Number of susceptible node due to virus at time	S(0)= 93
E(t)	Number of susceptible node due to virus at time t	E(0) = 5
I(t)	Number of Infectious nodes at time t	I(0) = 2
R(t)	Number of recovered nodes at time t	R(0) = 0
β	Infectivity contact rate	0.05
δ	Natural death rate	0.02
τ	Infection rate	0.04
r	Intrinsic growth rate	0.2
k	carrying capacity	100
ρ	Recovery rate	0.03
μ	Death rate due to attack	0.01

References

[1] N. Kshetri, "Pattern of global cyber war and crime: A conceptual frame work", Journal of International Management, vol. 11, **(2005)**, pp. 541-562.

[2] 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, **(2007)**, pp. 1207– 1212.

[3] B. K. Mishra and N. Jha, "SEIQRS model for the transmission of malicious objects in computer network", Applied Mathematical Modelling, vol. 34, **(2010)**, pp. 710-715.

[4] B. K. Mishra and A. Prajapati, "Dynamical model on the transmission of malicious codes in the network", I. J. Computer Network and Information Security, vol. 10, **(2013)**, pp. 17-23.

[5] J. O. Kephart, "A biologically inspired immune system for computers", Proceeding of International Joint Conference on Artificial Intelligence, **(1995)**.

[6] J. O. Kephart, S. R. White and D. M. Chess, "Computers and epidemiology", IEEE Spectrum, **(1993)**, pp. 20 – 26.

[7] M. J. Keeling and K. T. D. Eames, “Network and epidemic models”, J. Roy. Soc. Interf., vol. 2, no. 4, **(2005)**, pp. 295 – 307.

[8] M. M. Williamson and J. Leill, “An Epidemiological Model of Virus Spread and cleanup”, **(2003)**, http://www.hpl.hp.com/techreports/.

[9] M. E. J. Newman, S. Forrest and J. Balthrop, “Email networks and the spread of computer virus”, Phys. Rev. E, vol. 66, **(2002)**, pp. 035101-1-035101-4.

[10] M. Draief, A. Ganesh and L. Massouili, “Thresholds for virus spread on network”, Ann. Appl. Prob., vol. 18, no. 2, (2008), pp. 359 – 369.

[11] G. Li and J. Zhen, “Global stability of an SEI epidemic model with general contact rate”, Chaos Solitons and Fractals, vol. 23, **(2004)**, pp. 997–1004.

[12] J. K. Hale, “Ordinary Differential Equations”, 2nd Ed, Krieger, Basel, **(1980)**.

[13] T. Chen and N. Jamil, “Effectiveness of quarantine in worm epidemic”, IEEE International Conference on Communications, IEEE, **(2006)**, pp. 2142-2147.

[14] W. O. Kermack and A. G. Mckendrick, “A contribution to the mathematical theory of epidemics”, Proc. Roy. Soc. Lond. A, vol. 115, **(1927)**, pp. 700–721.

[15] J. O. Kephart, “A biologically inspired immune system for computers”, Proceeding of International Joint Conference on Artificial Intelligence, **(1995)**.

[16] S. Datta, H. Wang, “The effectiveness of vaccinations on the spread of email-borne computer virus”, IEEE CCECE/CCGEL, IEEE, **(2005)**, pp. 219-223.

[17] R. Pastor-Satorras and A. Vespignani, “Epidemics and immunization in scale-free networks”, Handbook of Graphs and network: From the Genome to the Internet, Willey-VCH, Bsrlin, **(2002)**.

[18] R. M. May and A. L. Lloyd, “Infection dynamics on scale-free networks”, Phys. Rev. E, vol. 64, no. 066112, **(2001)**, pp. 1–3.

[19] C. C. Zou, W. Gong and D. Towsley, “Worm propagation modelling and analysis under dynamic quarantine defense”, Proceeding of the ACM CCS Workshop on Rapid Malcode, ACM, **(2003)**, pp. 51–60.

[20] W. O. Kermack and A. G. McKendrick, “Contributions of mathematical theory to epidemics”, Proc. R. Soc. Lon. Ser. A, vol. 138, **(1932)**, pp. 55–83.

[21] W. O. Kermack and A. G. McKendrick, “Contributions of mathematical theory to epidemics”, Proc. R. Soc. Lon. Ser. A, vol. 141, **(1933)**, pp. 94–122.

[22] H. Yuan and G. Chen, “Network virus epidemic model with the point – to – group information propagation”, Appl. Math. Comput., vol. 206, no. 1, **(2008)**, pp. 357–367.

[23] J. R. C. Picqueria, “A modified epidemiological model for computer viruses”, Appl. Math. Comput., vol. 213, no. 2, **(2009)**, pp. 355–360.

[24] X. Han and Q. Tan, “Dynamical behavior of computer virus on internet”, Appl. Math. Comput., vol. 217, no. 6, **(2010)**, pp. 2520–2526.

[25] J. Kim, S. Radhakrishana and J. Jang, “Cost Optimization in SIS Model of Worm Infection”, ETRI Journal, vol. 28, no. 5, **(2006)**, pp. 692-695.

Authors

Bimal Kumar Mishra is a Professor in the Department of Applied Mathematics, Birla Institute of Technology, Mesra, Ranchi, India. He received his Master’s degree in Mathematics and Master’s degree in Operational Research from University of Delhi, India and earned his Ph. D. from Vinoba Bhave University, Hazaribag, India in 1997. He was awarded D. Sc. in 2007 from Berhampur University, India. He has published more than 100 research papers in journals of high repute and conference proceedings. His research interests include Nonlinear Analysis and Bifurcation and presently working in the area of Cyber attack and defence.

Apeksha Prajapati, is pursuing her Ph. D. program from Birla Institute of Technology, Ranchi, India. Domain of her research includes Mathematical model on Cyber War, Cyber attack and its defense mechanism.