International Journal of Hybrid Information Technology
Vol.6, No.6 (2013), pp.161-176
http://dx.doi.org/10.14257/ijhit.2013.6.6.14

A New Model on the Spread of Malicious Objects in Computer Network

Munna Kumar[1], Bimal Kumar Mishra[2#] and T. C. Panda[3]

[1]Research Scholar, Department of Mathematics, Utkal University, Bhubaneswar
Orissa, India – 751 004
[2]Department of Applied Mathematics, Birla Institute of Technology
Mesra, Ranchi, India – 835 215
[3]Orissa Engineering College, Bhubaneswar
Orissa, India – 752050

indian68mk@gmail.com, drbimalmishra@gmail.com

Abstract

In this paper, an attempt has been made to develop a compartmental Epidemic model on the transmission of malicious objects in a computer network with natural death (that is, crashing of nodes due to the reason other than the attack of malicious objects) and vertical transmission. In this model there are two possibilities of computer network: one of high infectious server nodes having high intensity rate of malicious attack while another is low infectious client nodes having low intensity rate of malicious attack. The high infectious server nodes transfer the malicious objects to the low infectious client nodes in the computer network. The low infectious client nodes recover with temporary immunity and becomes again susceptible to the high infectious server nodes but at a lower rate. This needs to develop effective immunity after a period of time and a fully automatic defense mechanism to protect computer networks from modern and fast propagating worms. The stability of the result is stated in terms of the Jacobian of the system and the basic reproduction number is also well-defined. Numerical methods and MATLAB are employed to solve and simulate the system of equations developed and analysis of the model gives remarkable exposure.

Keywords: *Malicious objects; Computer Network; Two Population Epidemic Transmission Model; Stability*

2000 AMS Classification: 92D30, 34D23, 34D05

1. Introduction

Our ever-growing dependence on computer networks is accompanied by ever growing concerns about the networks vulnerability to information attacks and the dependability of the existing network security systems. Major threats, well recognized by government, private institutions and individual users, are stemming primarily from self-replicating malicious software. Modern worms and viruses propagate through the Internet much faster and cause more damage than their predecessors. In 2001 the Code Red worm propagated faster than the Melissa virus in 1999 and much faster than Morris worm in 1988. Several months later, the Nimda worm caused severe damage within one hour of the detection of infection. The

[#] Corresponding author

ISSN: 1738-9968 IJHIT
Copyright ⓒ 2013 SERSC

Slammer worm caused harm in only a few minutes. In January 2003, the W32.SQLExp worm propagated so fast that human intervention could not prevent its spread.

Effective counter-measures to worm attacks consist of revealing the infected hosts as quickly as possible in order to minimize damage and searching for the vulnerabilities in security systems. However, there are many factors that decrease the efficiency of these efforts. Every year about four thousand new"holes" in security systems are revealed. At present more than 200 million computers are connected to the Internet and their numbers are growing rapidly. Every moment millions of vulnerable computers are interconnected through the Internet.

Many attacks are performed in a completely automatic fashion and are deployed at the speed of light throughout the Internet without regard to geographical and national borders. Technologies utilized by malicious software are becoming more and more complex and in some cases are completely concealed from detection that ultimately has the effect of increasing the time necessary for the detection and analysis of an attack. The combination of these factors results in a situation where even with the fastest response involving human intervention a major cyber attack would have enough time to cause significant damage to the national infrastructure. This reality is well recognized by a number of researchers and justifies the necessity for the development of novel, fully automatic, decentralized computer network defenses emulating known immune mechanisms honed to perfection by multi-million year evolution.

In 1991 Kephart pioneered the application of epidemiological models for the mathematical description of the complex dynamic phenomenon of propagation of self-replicating software such as simple file viruses [1]. File viruses distribution in networks was formalized in terms of probability laws [2, 3] for homogeneous, localized and random replication patterns. He should be credited for the introduction of the very concept of immune system for computers in [4] and its further development in [5] and [6, 7]. Worms have received true recognition after the attack of the Code Red worm in July, 2001. Consequently, the first propagation case study was presented in [8], where authors utilized the collected data for the analysis of the infection and disinfection rates. More fundamental analysis of the worm propagation dynamics was performed for SQL Slammer worm in [9].

Applications of various epidemiological models for modeling and analysis of real and theoretical worms with respect to different network topologies and scanning techniques could be found in [10-16]. In [13] and [16] special studies were conducted to investigate several key characteristics of infection, including the rate of infection through the network, the rate at which individual nodes are re-infected during an attack, and the effect of immunization of certain nodes in the network.

The action of worms throughout a network can be studied by using epidemiological models for disease propagation [17-19]. The model SEIR proposed by the authors [20] 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 [17] present an 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 model and antivirus countermeasures to study the prevalence of virus, *e.g.*, virus immunization [19] and Extending the SEIRS model of [17].

In summary, it could be noted that it is recently recognized that only a fully automatic defense mechanism can protect computer networks from modern and fast propagating worms.

Nomenclature:

S_H : Susceptible nodes with high infectious and suffer high intensity rate of attack.

E_H : Exposed nodes with high infectious and suffer high intensity rate of attack.

I_H : Infectious nodes with high infectious and suffer high intensity rate of attack.

S_L : Susceptible nodes with low infectious and suffer low intensity rate of attack.

E_L : Exposed nodes with low infectious and suffer low intensity rate of attack.

I_L : Infectious nodes with low infectious and suffer low intensity rate of attack .

R_L : Recovered nodes (having temporary immunity) with low infectious and suffer low intensity rate of attack.

N_H : Total nodes with high infectious and suffer high intensity rate of attack.

N_L : Total nodes with low infectious and suffer low intensity rate of attack.

Ψ_H : Birth rate (new nodes attached to the network) with high infectious.

Ψ_L : Birth rate (new nodes attached to the network) with low infectious.

β_{LH} : Probability of transmission of infection from an Infectious I_H to a Susceptible class S_L

β_{HL} : Probability of transmission of infection from an Infectious I_L to a Susceptible class $S_{H.}$

$\overline{\beta}_{HL}$: Probability of transmission of infection from a Recovered R_L to a Susceptible class $S_{H.}$

ϕ_H : The rate coefficient of Exposed class E_H to Infectious class $I_{H\,.}$

ϕ_L : The rate coefficient of Exposed class E_L to Infectious class $I_{L\,.}$

γ_L : The rate coefficient of Infectious class I_L to Recovered class R_L.

η_L : The rate coefficient of Infectious class I_L to Susceptible class S_L.

ρ_L : The rate coefficient of loss of immunity from Recovered class R_L to Susceptible S_L.

δ_H : The rate of crashing of the nodes due to the attack of malicious object for Infectious $I_{H\,.}$

δ_L : The rate of crashing of the nodes due to the attack of malicious object for Infectious $I_{L.}$

μ_H : The natural death rate for high infectious nodes.

μ_L : The natural death rate for low infectious nodes.

α_H : Vertical transmission for high infectious nodes.

α_L : Vertical transmission for low infectious nodes.

The following assumptions are made to characterize the model:

(i) Any new node added into the network is susceptible.

(ii) Death rate other than the attack of malicious objects is constant.

Copyright ⓒ 2013 SERSC

(iii) The natural death rate (crashing of the nodes due to the reason other than attack of malicious objects) of the nodes as they are once susceptible to any malicious objects decreases.

(iv) Low infectious nodes recover from infection (without immunity) and move right back to susceptible state OR gain temporary immunity before losing it and returning to the susceptible class.

(v) Duration of building effective immunity is right after the duration of recovery from the infection.

(vi) Recovered nodes are still able to transmit the infection but at a lower rate.

(vii) Duration of latent period and immune period are constant.

(viii) High infectious nodes and low infectious nodes are not constant.

2. Formulation of $S_HE_HI_H$-$S_LE_LI_LR_L$ Transmission Model

In the computer network, to derive the transmission model equation, the total number of computer nodes (N) is divided into two groups: $N_{H\,,}$ which is high infectious and suffer high intensity rate of attack and $N_{L\,,}$ which is low infectious and suffer low intensity rate of attack.

$$N_H + N_L = N \tag{1}$$

N_H consists of three classes: Susceptible (S_H), Exposed (E_H), Infectious (I_H).

That is,

$$S_H + E_H + I_H = N_H \tag{2}$$

There is no recovered class for the high infectious group of nodes (N_H) as highly infectious nodes have no time to recover and finally never recover and transfer the malicious objects to low infectious group of nodes (N_L).

N_L consists of four classes: Susceptible (S_L), Exposed (E_L), Infectious (I_L) and Recovered (R_L).

That is,

$$S_L + E_L + I_L + R_L = N_L \tag{3}$$

Susceptible nodes (S_L) can be infected when malicious objects transmitted by highly infectious nodes (I_H), which progresses through the Exposed (E_L) class. After the latent period, proportion of nodes population are transferred to the Infectious class (I_L) then finally move to the Recovered class (R_L) with temporary immunity or they can be susceptible again. As the immunity is temporary, the Recovered class (R_L) returns to Susceptible class (S_L) and (S_H) due to the lack of updated anti-virus and a fully automatic defense mechanism in the computer network.

Our assumption on the transmission of malicious objects in computer network is depicted in Figure 1.

Copyright ⓒ 2013 SERSC

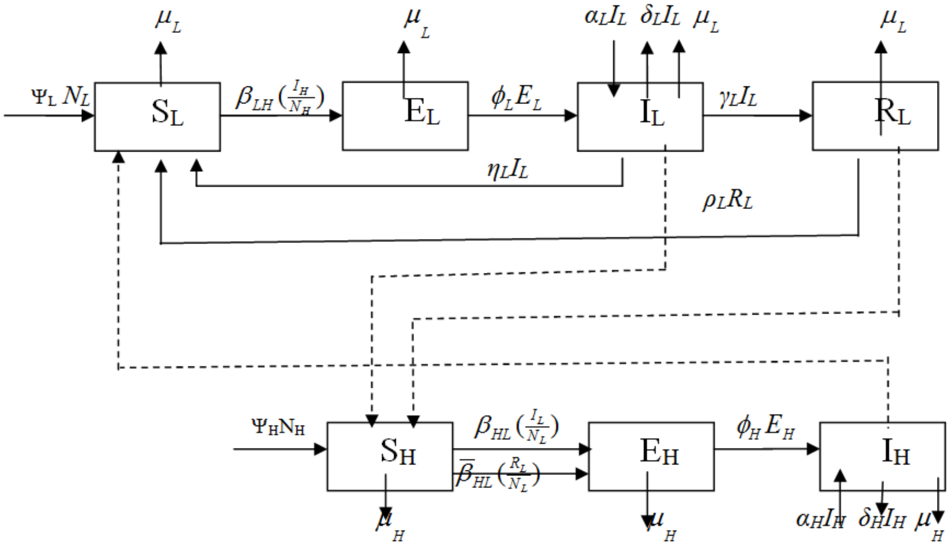

Figure 1. Schematic diagram for the flow of malicious objects in computer network

The transmission between model classes can be expressed by the following system of differential equations:

$$\frac{dS_H}{dt} = \psi_H N_H - \beta_{HL}(\tfrac{I_L}{N_L})S_H - \overline{\beta}_{HL}(\tfrac{R_L}{N_L})S_H - \mu_H S_H$$

$$\frac{dE_H}{dt} = \beta_{HL}(\tfrac{I_L}{N_L})S_H + \overline{\beta}_{HL}(\tfrac{R_L}{N_L})S_H - \phi_H E_H - \mu_H E_H$$

$$\frac{dI_H}{dt} = \phi_H E_H + \alpha_H I_H - \delta_H I_H - \mu_H I_H$$

$$\frac{dS_L}{dt} = \psi_L N_L + \rho_L R_L + \eta_L I_L - \beta_{LH}(\tfrac{I_H}{N_H})S_L - \mu_L S_L$$

$$\frac{dE_L}{dt} = \beta_{LH}(\tfrac{I_H}{N_H})S_L - \phi_L E_L - \mu_L E_L$$

$$\frac{dI_L}{dt} = \phi_L E_L + \alpha_L I_L - \delta_L I_L - \mu_L I_L - \gamma_L I_L - \eta_L I_L$$

$$\frac{dR_L}{dt} = \gamma_L I_L - \rho_L R_L - \mu_L R_L \qquad (4)$$

3. Basic Reproduction Number (R_0)

Since the model has four infected classes (E_H, $I_{H,}$ E_L, I_L), so, to get R_0, we take only four equations from the system (4) corresponding to these classes. That is,

$$\frac{dE_H}{dt} = \beta_{HL}(\tfrac{I_L}{N_L})S_H + \overline{\beta}_{HL}(\tfrac{R_L}{N_L})S_H - \phi_H E_H - \mu_H E_H$$

$$\frac{dI_H}{dt} = \phi_H E_H + \alpha_H I_H - \delta_H I_H - \mu_H I_H$$

$$\frac{dE_L}{dt} = \beta_{LH}(\tfrac{I_H}{N_H})S_L - \phi_L E_L - \mu_L E_L$$

$$\frac{dI_L}{dt} = \phi_L E_L + \alpha_L I_L - \delta_L I_L - \mu_L I_L - \gamma_L I_L - \eta_L I_L$$

On linearization, we get, $\begin{bmatrix} \frac{dE_H}{dt} \\ \frac{dI_H}{dt} \\ \frac{dE_L}{dt} \\ \frac{dI_L}{dt} \end{bmatrix}$ = (F – V) $\begin{bmatrix} E_H \\ I_H \\ E_L \\ I_L \end{bmatrix}$, where, F, a matrix of rates of infection and

V, a matrix of rates of transmission, is defined by, F = $\begin{bmatrix} 0 & 0 & 0 & \beta_{HL} \\ 0 & 0 & 0 & 0 \\ 0 & \beta_{LH} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

and

$$V = \begin{bmatrix} \phi_H + \mu_H & 0 & 0 & 0 \\ -\phi_H & \delta_H + \mu_H - \alpha_H & 0 & 0 \\ 0 & 0 & \phi_L + \mu_L & 0 \\ 0 & 0 & -\phi_L & \delta_L + \mu_L + \gamma_L + \eta_L - \alpha_L \end{bmatrix}$$

Then the basic reproductive number R_0 is calculated by the formula $\left|FV^{-1} - \lambda I\right| = 0$

That is,

$$R_0 = \sqrt{\frac{\beta_{LH}\phi_H\beta_{HL}\phi_L}{(\phi_H + \mu_H)(\delta_H + \mu_H - \alpha_H)(\phi_L + \mu_L)(\delta_L + \mu_L + \gamma_L + \eta_L - \alpha_L)}} \qquad (5)$$

4. Solutions and Stability

The system (4) is defined on the closed, positive invariant set D = {(S_H, E_H, I_H, S_L, E_L, I_L, R_L); S_H, $S_L > 0$ and E_H, I_H, E_L, I_L, $R_L \geq 0$: $S_H + E_H + I_H + S_L + E_L + I_L + R_L = N_H + N_L = N$} which has two possible equilibriums, first, the malicious objects free equilibrium, $D_0 = (N_H, 0, 0, N_L, 0, 0, 0)$ and second, the endemic equilibrium $D^* = (S_H{}^*, E_H{}^*, I_H{}^*, S_L{}^*, E_L{}^*, I_L{}^*, R_L{}^*)$ which is the interior of D and can be obtained by taking all the equations of system (4) equal to zero. That is,

$$N_H{}^* = \frac{(\delta_H - \alpha_H) I_H{}^*}{\psi_H - \mu_H}$$

$$E_H{}^* = \frac{(\delta_H + \mu_H - \alpha_H) I_H{}^*}{\phi_H}$$

$$S_H{}^* = \frac{[\phi_H + \mu_H)](\delta_H + \mu_H - \alpha_H) I_H{}^* N_L{}^*}{\phi_H [\beta_{HL}(I_L{}^*) + \bar{\beta}_{HL}(R_L{}^*)]}$$

$$N_L{}^* = \frac{(\delta_L - \alpha_L) I_L{}^*}{\psi_L - \mu_L}$$

$$E_L{}^* = \frac{(\delta_L + \mu_L + \gamma_L + \eta_L - \alpha_L) I_L{}^*}{\phi_L}$$

$$S_L{}^* = \frac{(\phi_L + \mu_L)(\delta_L + \mu_L + \gamma_L + \eta_L - \alpha_L) I_L{}^* N_H{}^*}{\beta_{LH}(I_H{}^*)\phi_L}$$

$$R_L{}^* = \frac{\gamma_L I_L{}^*}{\rho_L + \mu_L},$$

Notice that the functions for $N_H{}^*$, $S_H{}^*$, $E_H{}^*$, $N_L{}^*$, $S_L{}^*$, $E_L{}^*$ and $R_L{}^*$ depends on $I_H{}^*$ and $I_L{}^*$.

We obtain the values of $I_H{}^*$ and $I_L{}^*$ numerically and substitute it into the above functions together with the prescribed values of all parameters involved and calculate the values for above functions.

By using system (4), the Jacobian can be taken as,

$$J=\begin{bmatrix} -\bar{\beta}_{HL}(\frac{R_L}{N_L})-\mu_H & 0 & 0 & 0 & 0 & -\beta_{HL}(\frac{S_H}{N_L}) & -\bar{\beta}_{HL}(\frac{S_H}{N_L}) \\ \bar{\beta}_{HL}(\frac{R_L}{N_L}) & -(\phi_H+\mu_H) & 0 & 0 & 0 & \beta_{HL}(\frac{S_H}{N_L}) & \bar{\beta}_{HL}(\frac{S_H}{N_L}) \\ 0 & \phi_H & \alpha_H-(\delta_H+\mu_H) & 0 & 0 & 0 & 0 \\ 0 & 0 & -\beta_{LH}(\frac{S_L}{N_H}) & -\mu_L & 0 & \eta_L & \rho_L \\ 0 & 0 & \beta_{LH}(\frac{S_L}{N_H}) & 0 & -(\phi_L+\mu_L) & 0 & 0 \\ 0 & 0 & 0 & 0 & \phi_L & \alpha_L-(\delta_L+\mu_L+\gamma_L+\eta_L) & 0 \\ 0 & 0 & 0 & 0 & 0 & \gamma_L & -(\rho_L+\mu_L) \end{bmatrix}$$

Solving, we get the eigen values, $-\bar{\beta}_{HL}(\frac{R_L}{N_L})-\mu_H$, $-(\phi_H+\mu_H)$, $\alpha_H-(\delta_H+\mu_H)$, $-\mu_L$, $-(\phi_L+\mu_L)$, $\alpha_L-(\delta_L+\mu_L+\gamma_L+\eta_L)$, $-(\rho_L+\mu_L)$, which all are real negative if and only if $\alpha_H<(\delta_H+\mu_H)$ and $\alpha_L<(\delta_L+\mu_L+\gamma_L+\eta_L)$. So, the system (4) is locally asymptotically stable.

5. Numerical Methods and Simulation

R-K Method of order 4 is used to solve the system (4) and MATLAB is employed to simulate the system and the behavior of the different classes of nodes with respect to time is observed in Figure 2. The effect of highly infectious nodes (I_H) and susceptible nodes (S_L) is observed in Figure 3 and 9 which indicates that the highly infectious nodes (I_H) have no time to recover (as the attack rate is very high in comparison to recovery rate) and transfer the malicious objects to susceptible nodes (S_L) of low infectious group of nodes. The recovered nodes (R_L) are still able to transmit the infection to susceptible nodes (S_H) but at a lower rate due to gain temporary immunity. This effect of recovered nodes (R_L) and susceptible nodes (S_H) is observed and is depicted in Figure 4 and 10. Low infectious nodes (I_L) recover from infection without immunity and move right back to susceptible nodes (S_H). This effect of Low infectious nodes (I_L) and susceptible nodes (S_H) is observed and is shown in Figure 5 and 11. The effect of low infectious nodes ($I_{L)}$ and recovered nodes (R_L) is also observed and is depicted in Figure 6 and 12 and the effect of recovered nodes (R_L) and susceptible nodes (S_L) is observed and is shown in Figure 7 and 13, whereas the effect of low infectious nodes ($I_{L)}$ and susceptible nodes (S_L) is also shown in Figure 8 and 14. Simulation result agrees with the real life situation.

Copyright ⓒ 2013 SERSC

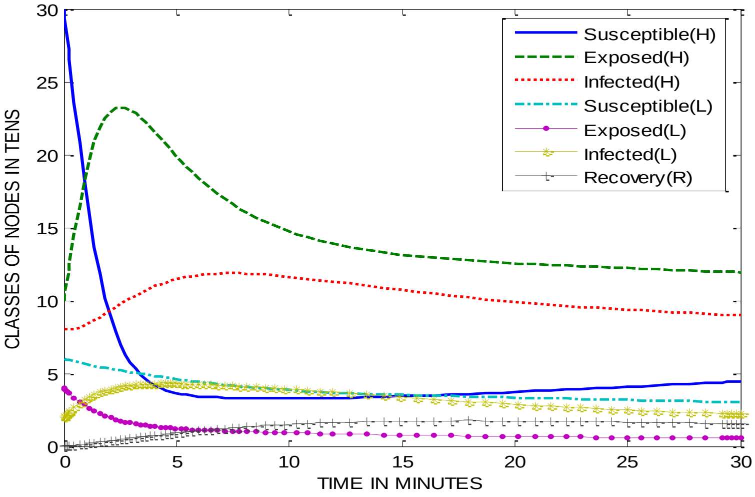

Figure 2. Dynamical behavior of the system (4) with the real parameters ψ_H =2.0; ψ_L =0.025; N$_H$=2.0; N$_L$=0.5; β_{HL} =0.1; $\overline{\beta}_{HL}$ =0.09; β_{LH} =0.02; μ_H =0.17; μ_L =0.025; ϕ_H =0.1; ϕ_L =0.5; α_H =0.06; α_L =0.03; δ_H =0.03; δ_L =0.01; ρ_L =0.08; γ_L =0.06; η_L =0.08

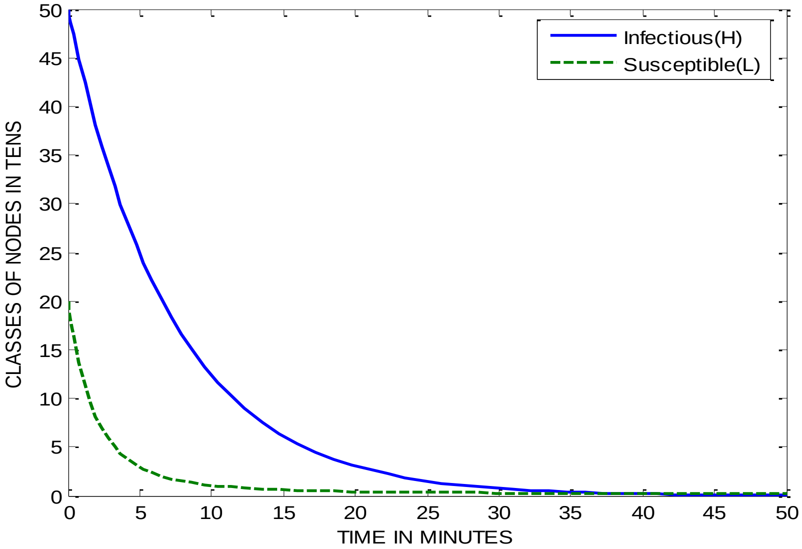

Figure 3. Dynamical behavior of the classes I$_H$ and S$_L$ with α_H =0.06; δ_H =0.03; N$_H$ =2.0; μ_H =0.17; $\overline{\beta}_{HL}$ =0.02; μ_L =0.025

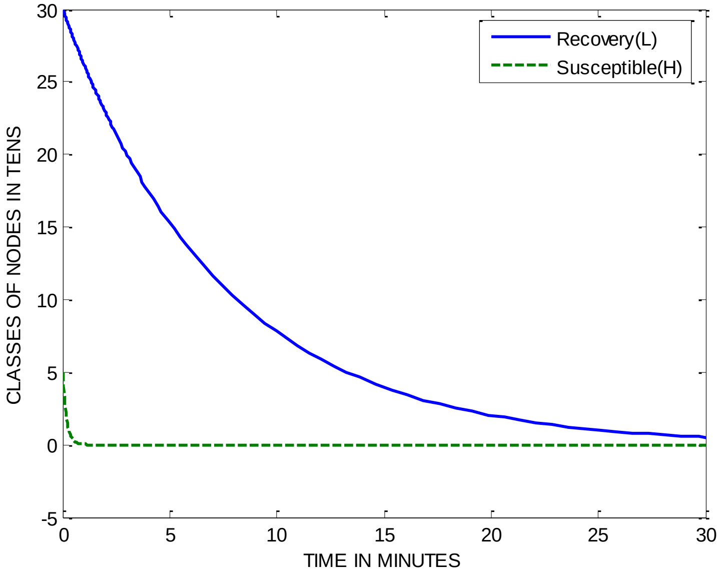

Figure 4. Dynamical behavior of the classes R_L and S_H with ρ_L=0.08; μ_H=0.17; N_H =2.0; μ_L=0.055; N_L =0.5; $\bar{\beta}_{HL}$=0.09

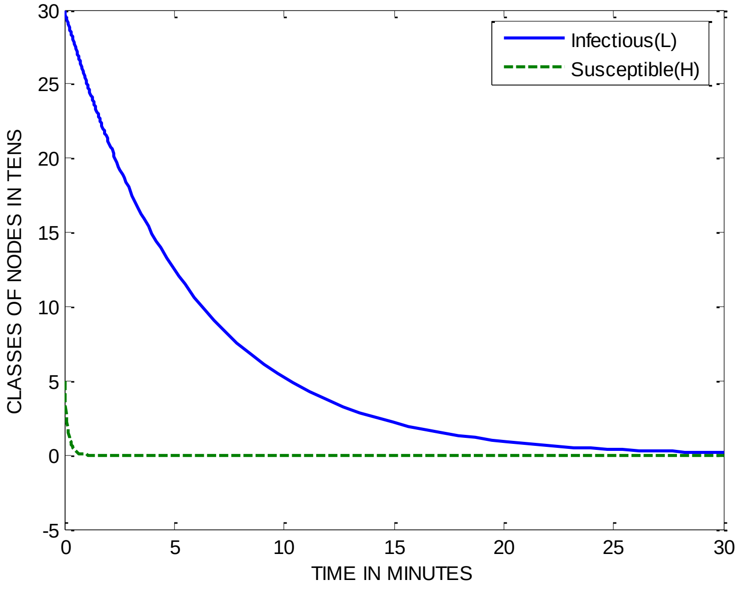

Figure 5. Dynamical behavior of the classes I_L and S_H with α_L=0.03; μ_H=0.17; μ_L=0.025; N_L =0.5; β_{HL}=0.1; δ_L=0.01; γ_L=0.06; η_L=0.08

Copyright ⓒ 2013 SERSC

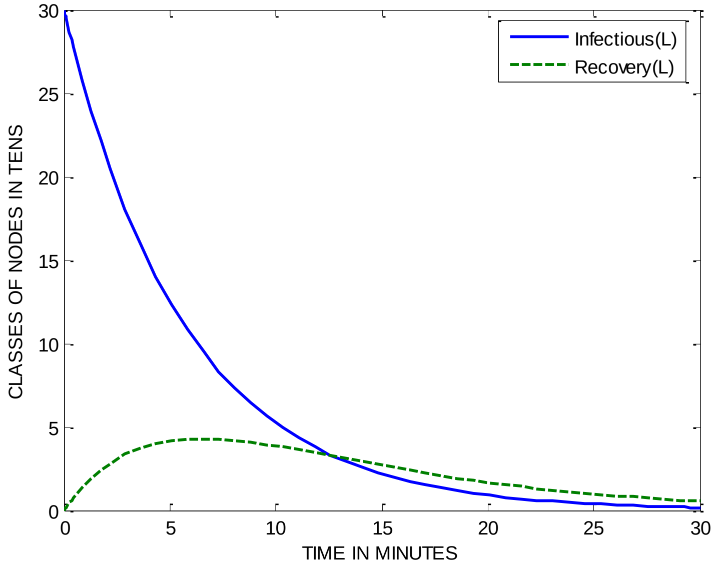

Figure 6. Dynamical behavior of the classes I_L and R_L with α_L =0.03; μ_L =0.025; N_L =0.5; ρ_L =0.08; δ_L =0.01; γ_L =0.06; η_L =0.08

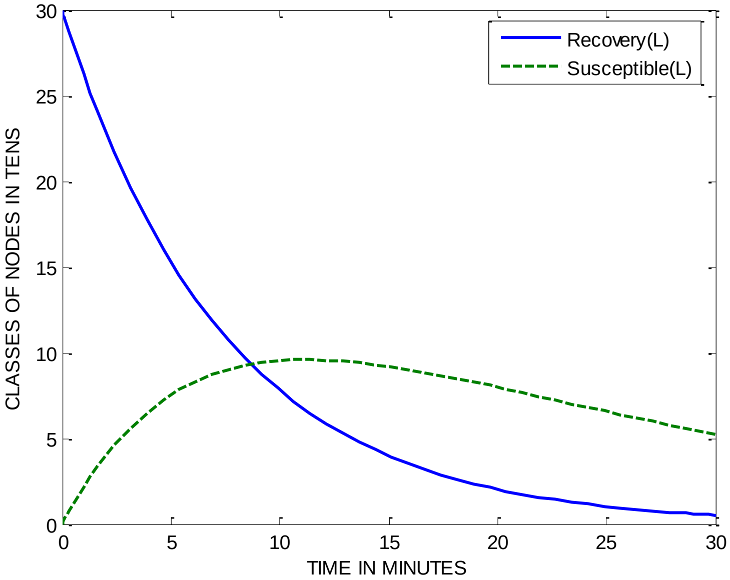

Figure 7. Dynamical behavior of the classes R_L and S_L with ρ_L =0.08; μ_L =0.055; N_L =0.5

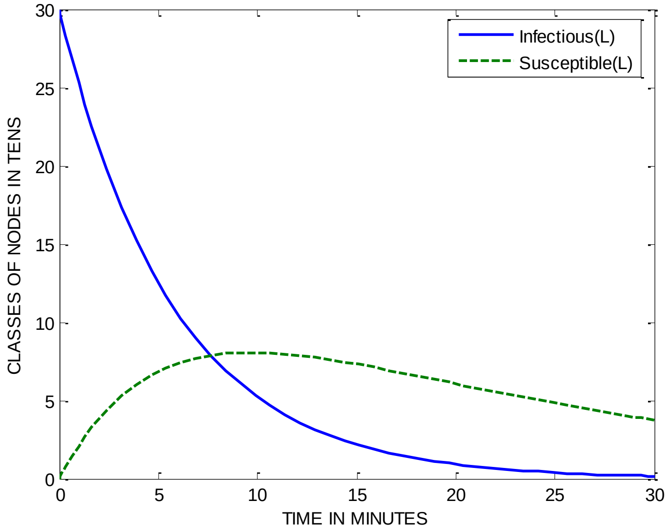

Figure 8. Dynamical behavior of the classes I_L and S_L with α_L=0.03; μ_L=0.055; N_L =0.5; δ_L =0.01; γ_L =0.06; η_L =0.08

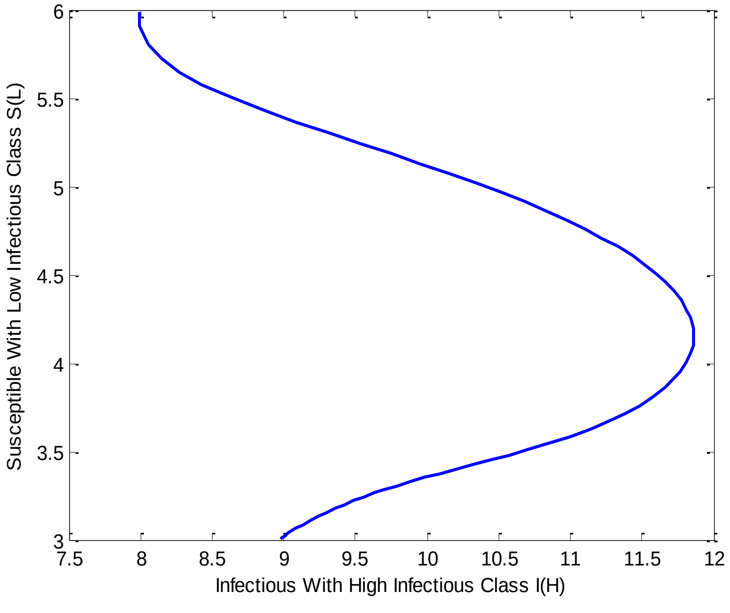

Figure 9. Dynamical behavior of the classes I_H and S_L with ψ_H =2.0; ψ_L =0.025; N_H=2.0; N_L=0.5; β_{HL} =0.1; $\overline{\beta}_{HL}$ =0.09; β_{LH} =0.02; μ_H =0.17; μ_L =0.025; ϕ_H =0.1; ϕ_L =0.5; α_H =0.06; α_L =0.03; δ_H =0.03; δ_L =0.01; ρ_L =0.08; γ_L =0.06; η_L =0.08

Copyright ⓒ 2013 SERSC

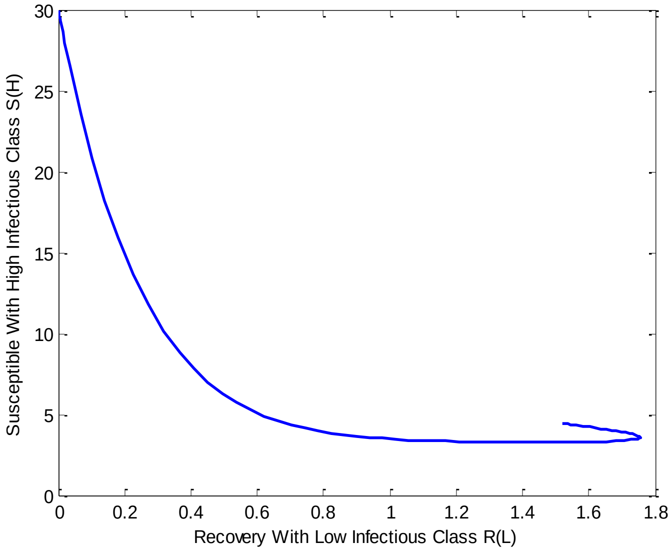

Figure 10. Dynamical behavior of the classes R_L and S_H with ψ_H =2.0; ψ_L =0.025; N_H=2.0; N_L=0.5; β_{HL} =0.1; $\overline{\beta}_{HL}$ =0.09; β_{LH} =0.02; μ_H =0.17; μ_L =0.025; ϕ_H =0.1; ϕ_L =0.5; α_H =0.06; α_L =0.03; δ_H =0.03; δ_L =0.01; ρ_L =0.08; γ_L =0.06; η_L =0.08

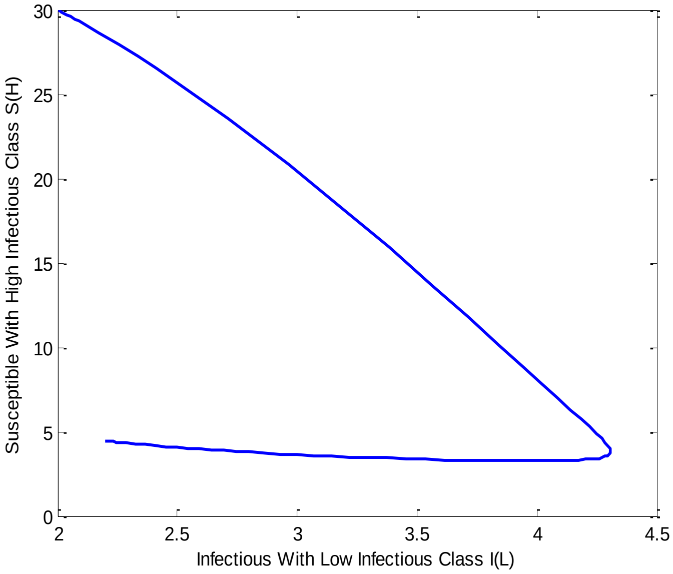

Figure 11. Dynamical behavior of the classes I_L and S_H with ψ_H =2.0; ψ_L =0.025; N_H=2.0; N_L=0.5; β_{HL} =0.1; $\overline{\beta}_{HL}$ =0.09; β_{LH} =0.02; μ_H =0.17; μ_L =0.025; ϕ_H =0.1; ϕ_L =0.5; α_H =0.06; α_L =0.03; δ_H =0.03; δ_L =0.01; ρ_L =0.08; γ_L =0.06; η_L =0.08

Copyright ⓒ 2013 SERSC

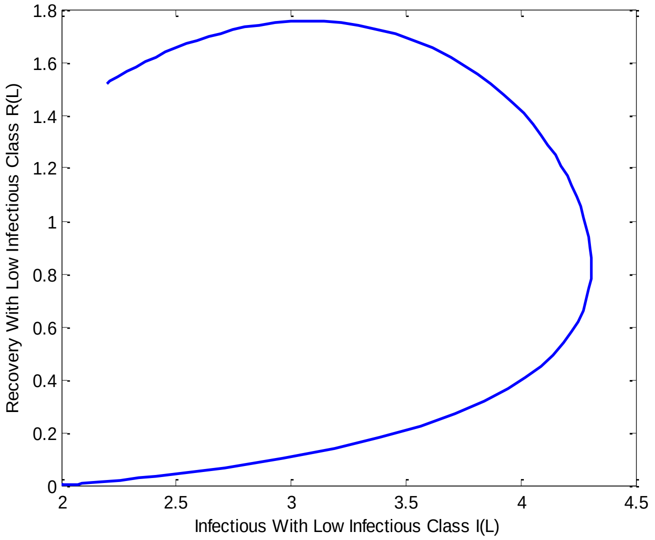

Figure 12. Dynamical behavior of the classes I_L and R_L with ψ_H =2.0; ψ_L =0.025; N_H=2.0; N_L=0.5; β_{HL} =0.1; $\overline{\beta}_{HL}$ =0.09; β_{LH} =0.02; μ_H =0.17; μ_L =0.025; ϕ_H =0.1; ϕ_L =0.5; α_H =0.06; α_L =0.03; δ_H =0.03; δ_L =0.01; ρ_L =0.08; γ_L =0.06; η_L =0.08

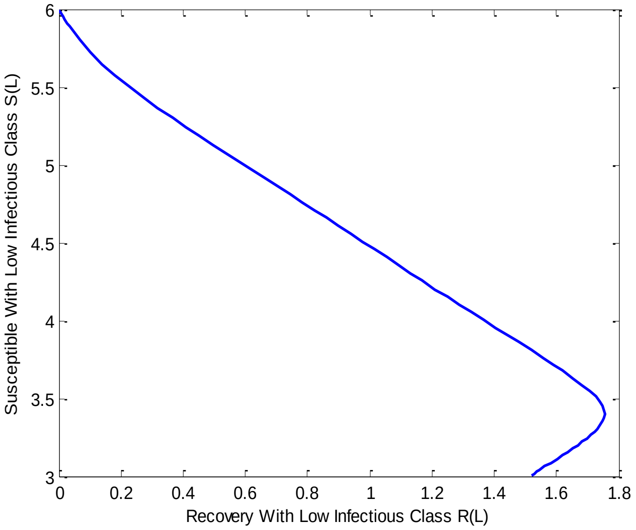

Figure 13. Dynamical behavior of the classes R_L and S_L with ψ_H =2.0; ψ_L =0.025; N_H=2.0; N_L=0.5; β_{HL} =0.1; $\overline{\beta}_{HL}$ =0.09; β_{LH} =0.02; μ_H =0.17; μ_L =0.025; ϕ_H =0.1; ϕ_L =0.5; α_H =0.06; α_L =0.03; δ_H =0.03; δ_L =0.01; ρ_L =0.08; γ_L =0.06; η_L =0.08

Copyright ⓒ 2013 SERSC

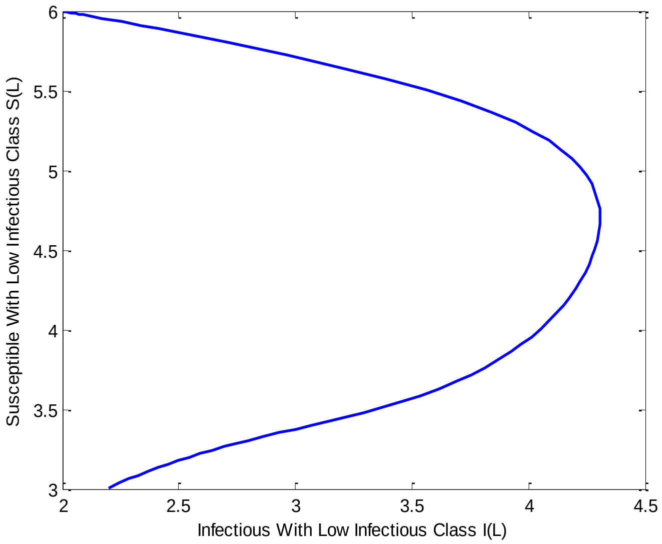

Figure 14. Dynamical behavior of the classes I_L and S_L with ψ_H =2.0; ψ_L =0.025; N_H=2.0; N_L=0.5; β_{HL} =0.1; $\overline{\beta}_{HL}$ =0.09; β_{LH} =0.02; μ_H =0.17; μ_L =0.025; ϕ_H =0.1; ϕ_L =0.5; α_H =0.06; α_L =0.03; δ_H =0.03; δ_L =0.01; ρ_L =0.08; γ_L =0.06; η_L =0.08

6. Conclusion

A dynamical two population Epidemic model for the transmission of malicious objects in computer network is formulated. We have assumed that the viruses possess a non-negligible latent period & infected nodes will stay in the latent period before they become infectious. From the Basic reproduction number and equilibrium points we are able to say that more the system is susceptible, lesser the secondary infection will be and vice – versa. It is observed that if the ability to build effective immunity is fast for those who recovered from the infection, the number of cases (Recovered nodes may become susceptible) can be reduced, that is, to get the system free of malicious objects, we have to update the anti- virus in a regular interval of time.

References

[1] J. O. Kephart and S. R. White, “Directed graph epidemiological models of computer viruses”, Proceedings of the IEEE Symposium on Security and Privacy, **(1991)**.

[2] J. O. Kephart and S. R. White, “Measuring and Modeling Computer Virus Prevalence”, Proceedings of the IEEE Symposium on Security and Privacy, **(1993)**.

[3] J. O. Kephart, S. R. White and S. R. Chess, Comp. and Epi. IEEE Spectrum, **(1993)** May.

[4] J. Kephart, “A Biologically Inspired Immune System for Computers”, IBM Thomas J. Watson Research Center, High Integrity Computing Laboratory, **(1994)**.

[5] J. O. Kephart, “How topology affects population dynamics”, In C. Langton, ed., Artificial Life III, Studies in the Sciences of Complexity, **(1994)**, pp. 447– 463.

[6] J. Kephart, G. Sorkin, D. Chess and S. White, “Fighting Computer Viruses”, Scientific American, **(1997)** November.

[7] J. Kephart, G. Sorkin, D. Chess, M. Swimmer and S. White, “Blueprint for a Computer Immune System”, The Virus Bulletin International Conference in San Francisco, **(1997)** October.

[8] D. Moore, C. Shanning and K. Claffy, “CodeRed: a case study on the spread and victims of an Internet worm”, Proceedings of the 2nd Internet Measurement Workshop, **(2002)** November.

Copyright ⓒ 2013 SERSC

[9] D. Moore, S. Savage, C. Shannon, S. Staniford and N. Weaver, “Inside the Slammer worm”, IEEE Security and Privacy, **(2003)** July.

[10] R. PastorSatorras and A. Vespignani, “Epidemics and immunization in scalefree networks”, Handbook of Graphs and Networks: From the Genome to the Internet, **(2002)**.

[11] R. PastorSatorras and A. Vespignani, “Immunization of complex networks”, Phy. Rev. E, vol. 65, **(2002)**.

[12] M. Boguna and R. PastorSatorras, “Epidemic spreading in correlated complex networks”, Phy. Rev. E, vol. 66, **(2002)**.

[13] C. Wang, J. C. Knight and M. C. Elder, “On Computer Viral Infection and the Effect of Immunization”, Proceedings of the 16th Annual Computer Security Applications Conference, **(2000)**.

[14] C. C. Zou, D. Towsley and W. Gong, “On the Performance of Internet Worm Scanning Strategies”, Univ. Massachusetts Amherst Technical Report TR-03-CSE-07, **(2003)**.

[15] C. Zou, W. Gong and D. Towsley, “Code Red Worm Propagation Modeling and Analysis”, Proceedings of 9th ACM Conference on Computer and Communication Security, **(2002)**.

[16] J. Kim, S. Radhakrishnan and S. Dhall, “Measurement and analysis of worm propagation on Internet Network Topology”, School of Computer Science, University of Oklahoma, USA, **(2003)**.

[17] B. K. Mishra and D. K. Saini, “SEIRS epidemic model with delay for transmission of malicious objects in computer network”, App. Math. and Comp., vol. 188, no. 2, **(2007)**, pp. 1476-1482.

[18] B. K. Mishra and D. Saini, “Mathematical models on computer viruses”, App. Math. and Comp., vol. 187, no. 2, **(2007)**, pp. 929-936.

[19] B. K. Mishra and N. Jha, “Fixed period of temporary immunity after run of anti-malicious software on computer nodes”, App. Math. and Comp., vol. 190, no. 2, **(2007)**, pp. 1207 – 1212.

[20] Y. Ping and L. Shengqiang, “SEIR epidemic model with delay”, J. Aust. Math. Soc. Series B – Appl. Math., vol. 48, no. 1, **(2006)**, pp. 119 – 134.

Authors

Munna Kumar is a research scholar pursuing his Ph. D. degree. His research interests include Mathematical Modeling on cyber attack and defense.

Bimal Kumar Mishra is a Professor in the Department of Applied Mathematics, Birla Institute of Technology, Mesra, Ranchi, India. He received his Master’s in Mathematics and Master’s 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.

T. C. Panda is a Retired Professor in the Department of Mathematics, Berhampur University, India. He has published in journals of high repute and supervised several Ph. D. scholars. His research areas include Fluid Mechanics, and Nonlinear Analysis.

Copyright ⓒ 2013 SERSC