ISSN 1749-3889 (print), 1749-3897 (online)
International Journal of Nonlinear Science
Vol.13(2012) No.3,pp.357-362

SI$_j$RS E-Epidemic Model With Multiple Groups of Infection In Computer Network

Bimal Kumar Mishra[1] *, Aditya Kumar Singh[2]
[1] Department of Applied Mathematics, Birla Institute of Technology, Mesra, Ranchi, India – 835 215
[2] Department of Applied Mathematics, Nilai Educational Trust's Group of Institutions, Thakurgaon, Ranchi -835 205
(Received 17 April 2011, accepted 9 February 2012)

Abstract: In order to protect cyber world from different kind of malicious objects, we strived to develop SI$_1$I$_2$I$_3$RS(Susceptible, Infectious due to worm, Infectious due to virus, Infectious due to Trojan Horse, Recovered and Susceptible) model for the transmission of malicious objects with simple mass action incidence in computer network. Threshold, equilibrium and their stability are discussed for the simple mass action incidence. We have derived an explicit formula for the reproductive number and have shown that the malicious object infection free equilibrium, whose component of infective is zero, are locally as while as globally asymptotic stable if threshold number is less than one. Numerical methods have been used to solve and simulate the system of differential equations which will help us to understand the attacking behavior of malicious object in computer network, and efficiency of antivirus software.

Keywords: epidemic model; malicious objects; computer network; threshold; global stability

Mathematics Subject Classification: 92D30, 34D23, 34K20, 34K25

1 Introduction

It is a fact beyond doubt that man made a quantum jump by the augmentation of cyber world which brought revolutionary changes in the society. It has made the life easier and world accessible with the touch button. But as all revolution has its favorable and adverse impact, cyber technology is no exception. The advancement in cyber technology also brought objects which are malicious in nature and great threat cyber world. These malicious objects are worm, virus and Trojan horse and they are different in accordance with their propagation behavior, characteristics, means and limitation. These malicious objects come to the system as important files and keep knocking at the door of the users which results in undesired and nasty impact. To put in another word these malicious objects are threatening the existence and utility of the cyber world. It is a known fact that malicious objects in cyber world spread like infectious diseases in biological world and are epidemic in nature. It is high time we take the measure to curb the spread and effects of those malicious objects before it becomes unmanageable. Hyman and Li [1,2] proposed a DI (Differential Infectivity) compartment for SIR model that describes the transmission dynamics of an infectious disease assuming infectious population divided into three compartments. Mishra et al has introduced mathematical models for the transmission of malicious objects in the computer network and has given epidemic models on times delays, the fixed period of temporary immunity after the use of anti-malicious software, effect of quarantine, fuzziness of the system [3-7]. The action of malicious object throughout a network can be studied by using epidemiological models for disease propagation [8-13]. Richard and Mark [14] proposed an improved SEI (Susceptible – Exposed – Infectious) model to simulate virus propagation. Anderson and May [15-16] discussed the spreading nature of biological viruses, parasite etc leading to infectious diseases in human population through several epidemic models. Several authors have discussed stability of the system of equations [17-25]. We try to develop a SI$_j$RS model for different kind of infections that does not confer permanent immunity; infectious class has been divided into three sub compartments: first compartment for the worm infected nodes, second compartment for the virus infected nodes and third compartment for the Trojan horse infected nodes. Susceptible nodes go to the infectious class in accordance with the attacking behavior of malicious objects such as worm, virus, and Trojan horse and then move to the recovered class after the run of anti-malicious software. The model here have a variable total population size, because

*Corresponding author. *E-mail address*: drbimalmishra@gmail.com

IJNS.2012.06.15/615

they have recruitment into the susceptible class by inclusion of some new nodes and nodes may crash due to the reason other than the attack of malicious objects and also due to the attack of malicious objects.

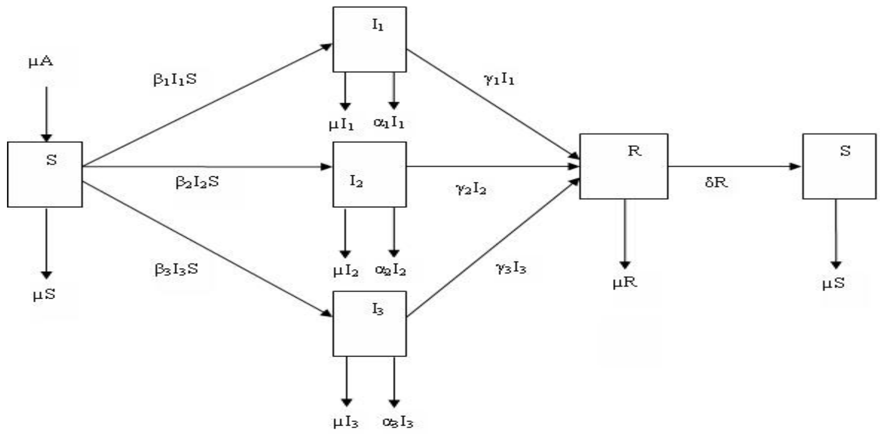

Figure 1: Schematic diagram for the flow of malicious objects in computer network.

2 $SI_1I_2I_3RS$ model with different infectivity and simple mass action incidence

Let S(t) be the number of susceptible, I_1(t), I_2(t) and I_3(t) be the number of nodes infected by worm, virus and Trojan horse respectively, R(t) be the recover nodes after the run of anti malicious software and N(t) be the total population size.

We have the following system of differential equations as depicted in Figure 1:

$$\frac{dS}{dt} = \mu(A - S) - q_j \sum_{j=1}^{3} \beta_j I_j S + \delta R$$

$$\frac{dI_j}{dt} = q_j \sum_{j=1}^{3} \beta_j I_j S - (\mu + \alpha_j + \gamma_j) I_j; j = 1, 2, 3.$$

$$\frac{dR}{dt} = \sum_{j=1}^{3} \gamma_j I_j - (\mu + \delta) R$$

where q_j is the probability of infective nodes which enter into the group I_j from the susceptible class. A is the recruitment of susceptible nodes in the computer network, μ is the per capita birth rate and death rate due to the reason other than the attack of malicious objects, γ_1, γ_2, and γ_3 are the rates of nodes leaving the infectious class I_1, I_2, and $I_3$to the recover class respectively. α_1, α_2, and α_3 are the crashing rate of the nodes due to the attack of malicious objects in infectious class I_1, I_2 and I_3 respectively. δ is the rate of transmission of nodes from recovered class to susceptible class.

Let, N = S + I_1+ I_2+ I_3+ R

$$\frac{dN}{dt} = \mu A - \mu N - q_j \sum_{j=1}^{3} \alpha_j I_j$$

3 Malicious objects free endemic equilibrium stage

In the absence of malicious objects, when$t \to \infty, N \to A$.

Let us define the solution region$G = \left\{(S, I_j R) \in R^5 / S \geq 0; I_j \geq 0; R \geq 0; S + I_j + R \leq A\ \forall j = 1\ to\ 3\right\}$

The system (1) has the infectious-free equilibrium stage E_0 = (A, 0, 0, 0, 0).

The basic reproduction number is thus $R_0 = A \sum_{j=1}^{3} \frac{\beta_j q_j}{\mu + \alpha_j + \gamma_j}$

We have an endemic equilibrium $E^*= (S^*, I^*_1, I_2^*, I_3^*, R^*)$ where

$$S^* = \frac{A}{R_0}; I_j^* = \frac{\mu A(R_0-1)\gamma_j(\mu+\delta)}{\{\beta_j\,(\mu+\delta)\,A-\delta\gamma_j R_0\}\,\gamma_j}; R^* = \frac{\mu A(R_0-1)\gamma_j}{\beta_j(\mu+\delta)A-\delta\gamma_j R_0}$$

Theorem 1 *Consider the system (1). If $R_0 < 1$ then solution set $G = (S, I_1, I_2, I_3, R) \in R^3 : S \geq 0; I_j \geq 0; S + I_1 + I_2 + I_3 + R \leq$ is locally asymptotically stable for infection free equilibrium E_0*

Proof. To show the local stability of the system (1), we construct the Jacobian matrix of (1) for the infection free equilibrium E_0.

$$J_0 = \begin{bmatrix} -\mu & D_{12} & D_{13} \\ 0 & D_{22} & 0 \\ 0 & D_{32} & -(\mu+\delta) \end{bmatrix}, \text{ where } D_{22} = \begin{bmatrix} -\sigma + q_1\beta_1 S & q_1\beta_2 S & q_1\beta_3 S \\ q_2\beta_1 & -\sigma_2 + q_2\beta_2 S & q_2\beta_3 S \\ q_3\beta_1 S & q_3\beta_2 S & -\sigma_3 + q_3\beta_3 S \end{bmatrix}$$

The eigen values of the Jacobian matrix J are real and negative. Therefore, the system is locally asymptotically stable. ■

Theorem 2 *For the system (1), the infection free equilibrium E_0 is globally asymptotically stable in the solution set $G = (S, I_1, I_2, I_3, R) \in R^3 : S \geq 0; I_j \geq 0; R \geq 0; S + I_1 + I_2 + I_3 + R \leq A$, if $R_0 < 1$.*

Proof. We define vectors B = $(\beta_1, \beta_2, \beta_3)^T$, D = diag $(\sigma_1, \sigma_2, \sigma_3)$ and Q^T = (q_1, q_2, q_3).

System (1) can be written as:

$$\frac{dS}{dt} = \mu(A-S) - B^T IS + \delta R$$
$$\frac{dI}{dt} = Q^T B^T IS - DI$$
$$\frac{dR}{dt} = YI - (\mu+\delta)R$$

where $I = (I1, I2, I3)^T andY = (\gamma 1, \gamma 2, \gamma 3)$. We express the basic reproduction number as

Let us define the Liapunov function V = $B^T D^{-1}$I. Then V is the positive definite for $I_j \geq 0$.

$$\frac{dV}{dt} = \frac{d}{dt}\left(B^T D^{-1} I\right) = B^T D^{-1}\frac{d}{dt}I \quad = B^T D^{-1}(Q^T B^T IS - DI)$$
$$= (Q^T D^{-1} B^T S - 1)B^T I = \left(\frac{R_0}{A}S - 1\right)B^T I \leq 0$$

where S $\leq$ A and R_0¡ 1. Hence, the infection free equilibrium $E_0$is the only positive invariant in $\{(S, I_j R) \in G; \frac{dV}{dt} = 0; for\ I = 0\}$.

Therefore, it follows from the Liapunov stability theory that the infection free equilibrium E0 is globally asymptotically stable. ■

4 Conclusion

Inspired by the biological compartment epidemic model, we made an attempt to develop a DI (differential - infectivity) compartment for SI_jRS epidemic model for the simple mass action incidence in which infected population is divided into three groups where first group consists of those nodes which are infected by the worms, second for nodes which infected by virus and third group for the nodes which are infected by the Trojan horse. We discussed the characteristic of the threshold parameter and established that if $R_0 \leq 1$, the system is locally asymptotically stable and globally asymptotically stable with help of Liapunov function. Runge-Kutta Fehlberg fourth fifth order method is used to solve and simulate the system (1) by using real parametric values depicted in *Table 1.* Eventually, we find that with the decrease of susceptible and all kind of infection, recovered nodes increases due to the run of antivirus software and these are asymptotically stable with respect to time, which is depicted in *Figure 2*. Furthermore, analysis and simulation results show some managerial insights that are helpful for the practice of antivirus in information sharing networks. The nature of attacking behavior of different malicious codes (virus, worms, trozans) for transforming recovered nodes to susceptible nodes is depicted in figure 3, 4, and 5 respectively. The efficiency of the antivirus software can be analyzed by (i) observing the rate through which it cleans the nodes on attack of different kind of malicious objects, (ii) the rate through which the nodes crashes due to the attack of malicious objects. This will help the software organization to develop more efficient antivirus software that can minimize the attack and maximize the rate of recovery.

Table 1: Parametric values used in simulation.

Parameter	**Value**
N	17,000
S(0)	9,500
$I_1(0)$	2,500
$I_2(0)$	2,000
$I_3(0)$	3,000
R(0)	0
A	0.009
μ	0.05
β_2	0.001
β_3	0.003
δ	0.005
q_1	0.26
q_2	0.27
q_3	0.47
α_1	0.992
γ_1	0.008
γ_2	0.007
γ_3	0.006

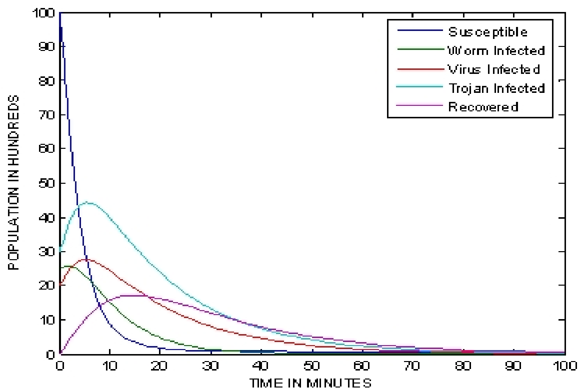

Figure 2: Dynamical behavior of the system (1).

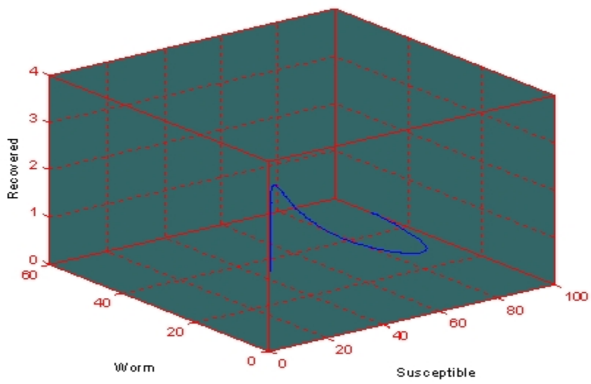

Figure 3: Transformation of nodes from recovered class to susceptible class when attacked by worms.

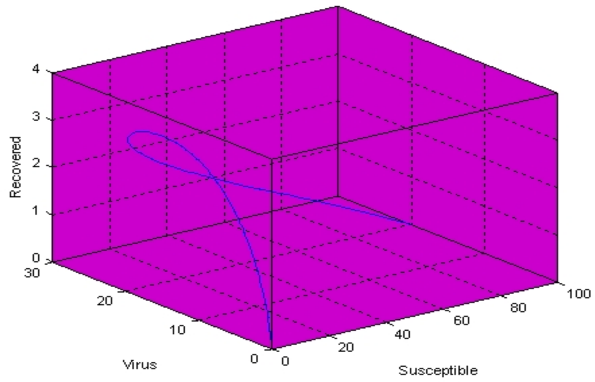

Figure 4: Transformation of nodes from recovered class to susceptible class when attacked by viruses.

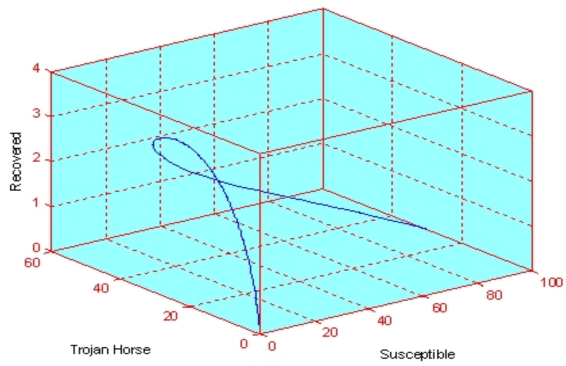

Figure 5: Transformation of nodes from recovered class to susceptible class when attacked by Trojan horse.

Acknowledgement

The authors are grateful to the anonymous reviewers for their constructive suggestions that greatly improve the quality of this paper.

References

[1] Hyman J. M., Li Jia, Stanley E. A.. The differentiated infectivity and staged progression models for the transmission of HIV. *Math. Biosci.*, 155 (1999): 77–109.

[2] Hyman, J. M. and Li, Jia. An intuitive formulation for the reproductive number for the spread of diseases in heterogeneous populations. *Math. Biosci.*, 167(2000): 65–86.

[3] Bimal Kumar Mishra, N. Jha. SEIQRS model for the transmission of malicious object in computer network. *Appl. Math. Model.*, 34(2010) :710-715.

[4] Bimal Kumar Mishra, D. K. Saini. SEIRS epidemic model with delay for transmission of malicious objects in computer network. *Appl. Math. Comput.*, 188(2)(2007) :1476-1482.

[5] Bimal Kumar Mishra, Dinesh Saini. Mathematical models on computer virus. *Appl. Math. Comput.*, 187(2) (2007):929-936.

[6] Bimal Kumar Mishra, Navnit Jha. Fixed temporary immunity after run of anti malicious software on computer nodes. *Appl. Math. Comput.*, 190(2) (2007): 1207-1212.

[7] Bimal Kumar Mishra, Samir Kumar Pandey. Fuzzy epidemic model for the transmission of worms in computer network. *Nonlinear Analysis RWA*, 11 (2010): 4335-4341.

[8] E. Gelenbe. Dealing with software viruses: a biological paradigm. *Inform. Secur. Tech. Rep.*, 12(4) (2007): 242-250.

[9] Erol Gelenbe. Keeping viruses under control, in: Computer and Information Sciences_ISCIS 2005. *20th International Symposium, in: Lecturer Notes in Computer Science, Springer*,3733(2005).

[10] Erol Gelenbe, Varol Kaptan, Yu Wang. Biological metaphors for agent behavior, in: Computer and Information Sciences_ISCIS 2004. *19th International Symposium, in: Lecturer Notes in Computer Science, Springer-Verlag*, 3280(2004): 667-675.

[11] J. R. C. Piqueira, F.B. Cesar. Dynamical model for computer virus propagation. *Math, Probl. Eng.*, doi: 10.1155/2008/940526.

[12] J.R.C. Piqueira, B.F. Navarro, L.H.A. Monteiro. Epidemiological models applied to virus in computer networks. *J. Comput. Sc.*, 1(1)(2005): 31-34.

[13] S. Forest, S. Hofmeyr, A.Somayaji, T. Longstaff. Self-nonself discrimination in a computer. *proceedings of IEEE, Symposium on computer security and privacy*, (1994):202-212.

[14] W. T. Richard, J. C. Mark. Modeling virus propagation in peer-to-peer networks. *IEEE International Conference on Information, Communications and Signal Processing,*(2005): 981-985.

[15] R.M. Anderson, R. M. May. Population biology of infection disease. *Nature*, 180 (1999):361-367.

[16] R. M. Anderson, R. M. May. Infection Disease of humans; Dynamics and control. *Oxford University Press, Oxford*,(1992).

[17] D Green Halgh. Hopf bifurcation in epidemic models with a latent period and non permanent immunity. *Math. Comput. Modell*, 25 (1997): 85-107.

[18] H. W. Hethcote, H. W. Stech, P.van dan Driessche. Periodicity and Stability in endemic models: a survey, in : K. L. Cook(Ed.) Differential Equations and Applications in Ecology, Epidemics and Population Problems. *Academic Press, New York*, (1981): 65-85.

[19] K. L. Cook, P.van den Drissche. Analysis of SEIRS epidemic model with two delays. *J. Math. Biol.*, 35(1996): 240-260.

[20] M. Y. L. J. R. Graff, L. C. Wang, J. Karsai. Global Dynamics of a SEIR model with a varying total population size. *Math. Biosci.*, 160 (1999):191-213.

[21] M .Y. Li, J.S Muldowney. Global Stability for the SEIR model in epidemiology. *Math. Biosci.*, 125(1995): 155-164.

[22] M. Y .Li, L. Wang. Global stability in some SEIR epidemic models ; C.C Chavez, S .Blower, P. Vanden Driessche , D. Kirscner, A.A Yakhdu (Eds). *Mathematical approaches for emerging and reemerging in infectious diseases, Models, Method and Theory, Springer*,126 (2002): 295-312.

[23] Y. Michel, H. Smith, L. Wang. Global dynamics of SEIR epidemic model with vertical transmission. *SIAM J. Appl. Math.*, 62(1) (2001): 58-69.

[24] J .K. Hale. Ordinary differential equations, second ed. *Krieger, Basel*, (1980).

[25] H. Hethcote, M. Zhein, L. Shengbing. Effects of quarantine in six epidemic models for the infectious diseases. *Math. Biosci.*, 180(2002):141-160.