Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2015, 2(9): 78-82

Research Article ISSN: 2394 - 658X

e – Epidemic Model on the Computer Viruses in the Network

SM Omair[1] and Samir Kumar Pandey[2]

[1]Department of Mathematics, Delhi Public School, Ranchi, India
[2]Department of Mathematics, Xavier Institute of Polytechnic & Technology, Ranchi, India
samir.phd2009@gmail.com

ABSTRACT

An e-epidemic SI_1I_2R (susceptible - Infectious1 - Infectious2 - Recovered) model characterizing the spread of viruses in a computer network has been developed to have a better understanding of the reason of virus attack. A study of the basic reproduction number reveals the affect of virus attack. Moreover, primary simulation results show the positive impact of increasing security measures on virus propagation in computer network. We have analyzed the behavior of the Susceptible, Infected and Recovered nodes in the computer network with real parametric values. Efficiency of antivirus software and crashing of the nodes due to virus attack critically analyzed. Numerical methods and MATLAB are employed to solve and simulate the system of equations developed and interpretation of the model yields interesting revelations.

Key words: Computer Network, Basic Reproduction network, Epidemic Model, Virus, MATLAB

INTRODUCTION

At present scenario, 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. The Internet is the primary medium used by attackers to commit computer crimes. Virus's attacks are considered by network experts the highest security risk on computer network. Computers virus is built to propagate without warning or user interaction, causing an increase in traffic service requests that will eventually lead to Cyber attack.

Our culture, financial system, and critical infrastructures/communications have become mostly dependent on computer networks and information technology solutions. Cyber attacks become more striking and potentially more disastrous as our dependence on information technology increases. To stop, or at least to decrease the such attacks of viruses we need e-epidemic models that can correctly capture the most important characteristics of such objects, as accepting the spread of viruses is critical for the most effective reactive measures. As mathematical models give a clear view and can be a good help to identify and solve many complex problems, we develop dynamic models for computer viruses and analyze the effect of different classes with vertical transmissions in computer network.

In past several decades, many authors have studied different mathematical models which illustrate the dynamical behavior of the transmission of biological disease and / or computer viruses. Based on SIR classical epidemic models [1–3] and due to the lots of similarities between biological viruses and computer viruses, several extended research articles are proposed to study the spreading and attacking behavior of computer viruses in different phenomenon, e.g. virus propagation [4–8, 11, 19, 20, 23, 29], quarantine [9, 10, 16, 30], virus immunization [13, 15, 21, 22, 24-26], time delay [12], fuzziness [17], effect of antivirus software [14, 18], vaccination [28], etc. May et al [27] studied the dynamical behavior of viruses on scale free networks. Also, Hincapie et al [31] has discussed the algorithmic method on SIIR model of epidemics.

FORMULATION OF THE MODEL

In a computer network, to derive the model equation, the total number of nodes (N) is divided into four classes: Susceptible nodes (S), Infectious nodes (I_1), fully Infectious nodes (I_2), Recovered nodes (R). In this model, the flow of viruses is from class S to class I_1, class I_1 to class I_2, and class I_2 to class R which can be seen in Fig. 1.

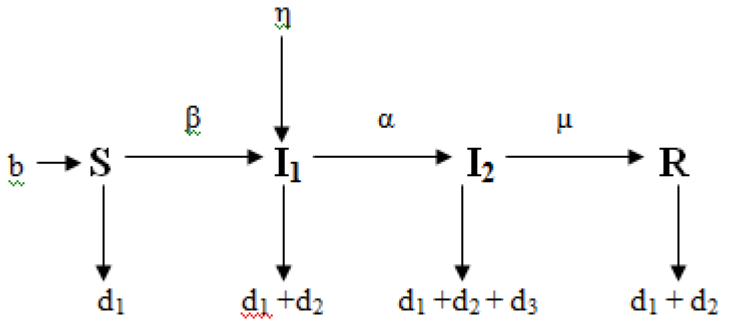

Fig. 1 Schematic diagram for the flow of viruses in different classes of nodes in network

Where, the rate constant β is the rate of contact by which the attacks are occurring in the network. The parameters α and μ are the rates of transmissions from class I_1 to I_2 and I_2 to R respectively. The constant b is the birth rate introduced at the susceptible class. The rate constants d_1 and d_2 are the death rates due to natural and the virus attacks respectively. The parameter d_3 is the death rate due to the reason of natural as well as the virus attack simultaneously and can be introduced only in the class I_2. It can be understood in the way that a computer node is crashed naturally and simultaneously it is harmed by the virus attack (i.e. the data disappears due to the attack). The parameter η is the rate of attack of viruses via vertical transmission directly introduced at the class I_1. The transmission between model classes can be expressed by the following system of differential equations:

$$\begin{aligned}\frac{dS}{dt} &= b-\beta SI_1 - d_1S\\ \frac{dI_1}{dt} &= \beta SI_1 - (d_1+d_2+\alpha)I_1 + \eta I_1\\ \frac{dI_2}{dt} &= \alpha I_1 - (d_1+d_2+d_3+\mu)I_2\\ \frac{dR}{dt} &= \mu I_2 - (d_1+d_2)R\end{aligned} \tag{1}$$

Where, $S + I_1 + I_2 + R = N$ (2)

Virus – Free Equilibrium & Local Stability

In this section, to analyze the virus - free equilibrium, we get the basic reproduction number for the virus control or eradication. By the system (1) and the equation (2), we get, $dN / dt = b - d_1N$ which is also called as equation for the total population. Thus, $N \rightarrow b/d_1$ as $t \rightarrow \infty$. This shows that, the feasible region, $U = \{(S, I_1, I_2, R) : S, I_1, I_2, R \geq 0, S + I_1 + I_2 + R \leq b/d_1\}$ is a positive invariant set for the model. In the absence of infection, the model has a unique virus - free equilibrium P_0 $(b/d_1, 0, 0, 0)$ and an endemic equilibrium point P^* (S^*, I_1^*, I_2^*, R^*), where these points can be obtained by taking all the equations of system (1) equal to zero, given by,

$$S^* = \frac{d_1+d_2+\alpha-\eta}{\beta},$$

$$I_1^* = \frac{\beta b - d_1(d_1+d_2+\alpha-\eta)}{\beta(d_1+d_2+\alpha-\eta)},$$

$$I_2^* = \frac{\alpha}{(d_1+d_2+d_3+\mu)}\,\frac{\beta b - d_1(d_1+d_2+\alpha-\eta)}{\beta(d_1+d_2+\alpha-\eta)},$$

$$R^* = \frac{\mu\alpha}{(d_1+d_2)(d_1+d_2+d_3+\mu)}\,\frac{\beta b - d_1(d_1+d_2+\alpha-\eta)}{\beta(d_1+d_2+\alpha-\eta)},$$

To get the local stability of virus – free equilibrium, we take the Jacobian matrix of the system (1), that is,

$$J = \begin{bmatrix} -d_1 & -\beta & 0 & 0\\ 0 & -d_1-d_2-\alpha & 0 & 0\\ 0 & \alpha & -d_1-d_2-d_3-\mu & 0\\ 0 & 0 & \mu & -d_1-d_2\end{bmatrix}$$

Since all eigen values ($-d_1$, $-d_1-d_2-\alpha$, $-d_1-d_2-d_3-\mu$ and $-d_1-d_2$) are negative, hence the system is locally asymptotically stable.

Basic Reproduction Number

The basic reproduction number can be obtained by calculating V, the matrix of rate of infectivity and F, the matrix of rates of transmission, for this purpose, we consider the equations of infected classes of the nodes as,

$$\frac{dI_1}{dt} = \beta S I_1 - (d_1 + d_2 + \alpha) I_1 + \eta I_1$$

$$\frac{dI_2}{dt} = \alpha I_1 - (d_1 + d_2 + d_3 + \mu) I_2$$

and by linearization, we get,

$$\begin{bmatrix} I_1 \\ I_2 \end{bmatrix} = (F - V)\begin{bmatrix} I_1 \\ I_2 \end{bmatrix}$$, where, F and V can be obtained by,

$$F = \begin{bmatrix} 0 & \beta \\ 0 & 0 \end{bmatrix} \text{ and } V = \begin{bmatrix} d_1 + d_2 + \alpha - \eta & 0 \\ -\alpha & d_1 + d_2 + d_3 + \mu \end{bmatrix}$$

Then, R_0 will be given by the dominant eigen value of F V^{-1}. That is,

$$R_0 = \frac{\alpha\beta}{(d_1 + d_2 + \alpha - \eta)(d_1 + d_2 + d_3 + \mu)} .$$

The characteristic of the basic reproduction number is that if $R_0 \le 1$, the virus free equilibrium is globally stable in the feasible region & the virus fade out from the network, whereas if $R_0 > 1$, a unique endemic equilibrium is globally stable in the interior of the feasible region & the virus persists at a constant endemic level (depicted in Figs 2 – 6).

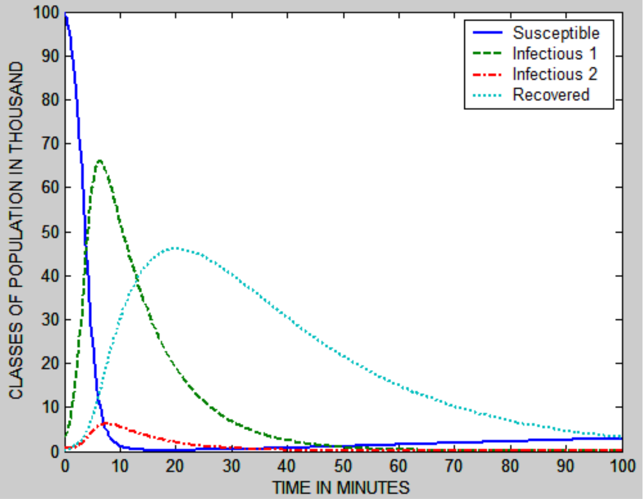

Fig. 2 Dynamical behavior of the system of population of nodes with real parametric values, b=0.03, d_1=0.01, d_2=0.03, d_3=0.03, β=0.01, μ=0.90, α=0.095, η=0.03; $R_0 < 1$

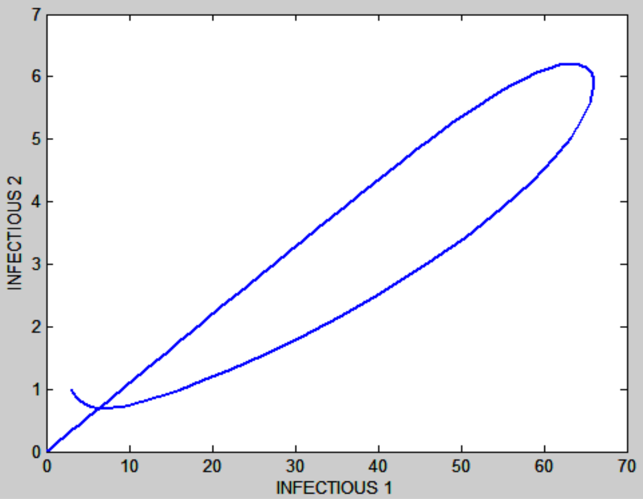

Fig. 3 Effect of I_1 with respect to I_2 with real parametric values, b=0.03, d_1=0.01, d_2=0.03, d_3=0.03, β=0.01, μ=0.90, α=0.095, η=0.03; $R_0 < 1$

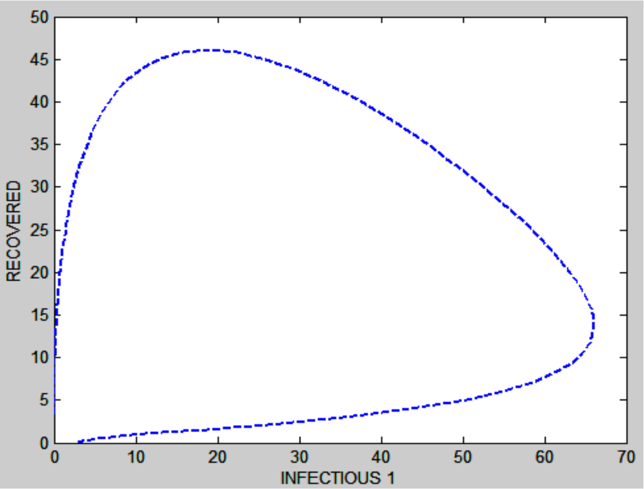

Fig. 4 Effect of I_1 with respect to R with real parametric values, b=0.03, d_1=0.01, d_2=0.03, d_3=0.03, β=0.01, μ=0.90, α=0.095, η=0.03; $R_0 < 1$

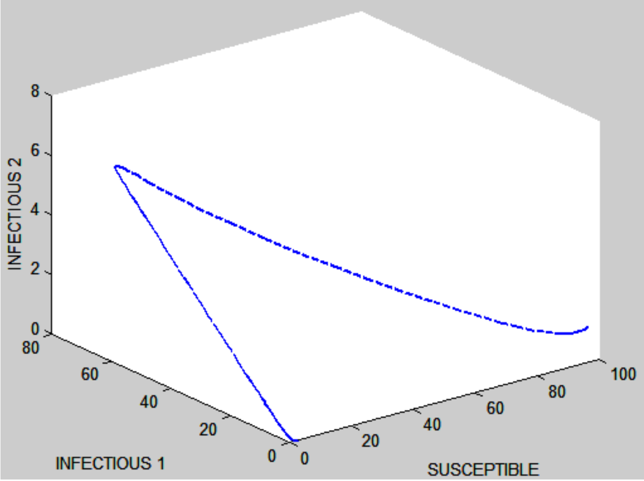

Fig. 5 Effect of S, I_1 with respect to I_2 with real parametric values, b=0.03, d_1=0.01, d_2=0.03, d_3=0.03, β=0.01, μ=0.90, α=0.095, η=0.03; $R_0 < 1$

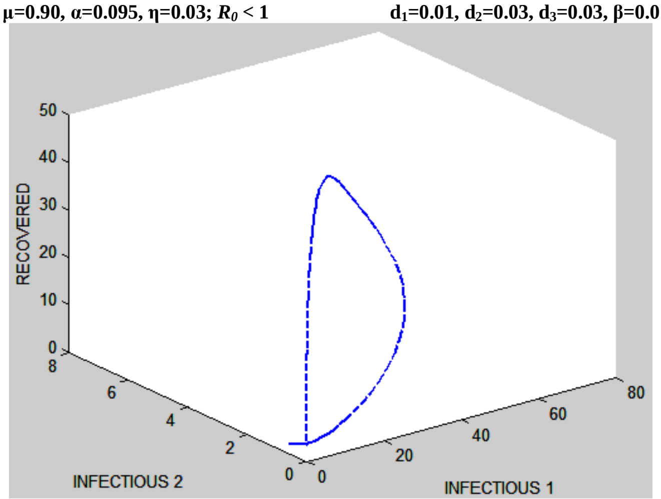

Fig. 6 Effect of I_1, I_2 with respect to R with real parametric values, b=0.03, d_1=0.01, d_2=0.03, d_3=0.03, β=0.01, μ=0.90, α=0.095, η=0.03; $R_0 < 1$

CONCLUSION

A compartmental model has been developed for the propagation of viruses using vertical transmission in the computer network. We assume that the viruses possess a non-negligible latent period & infected nodes (Infectious 1) will stay in the latent period before they become fully infectious (Infectious 2). We have discussed the characteristic of the different classes of nodes (Fig. 2) which shows that the system is asymptotically stable. Further, we have individually analyzed all the classes of nodes comparatively by using real parametric values (Figs 3 – 6). Here, we have observed that the simulation results for different classes as, comparison between I_1 - I_2 (fig 3), I_1 – R (fig 4), S – I_1 – I_2 (fig 5) and I_1 – I_2 – R (fig 6) give the clear view to show the stability of the system. It is shown that the antivirus software will be highly efficient if the rate of recovery of nodes from infectious nodes is very high and crashing of the nodes due to the attack of worms in the presence of the antivirus software is very less. Thus these types of mathematical models will be very helpful in developing good antivirus software, keeping into mind the attacking behavior of viruses, which may reduce the attack.

REFERENCES

[1] WO Kermack, AG McKendrick, Contributions of Mathematical Theory to Epidemics, *Proceedings of Royal Society, London – Series A*, **1927**, 115, 700–721.

[2] WO Kermack, AG McKendrick, Contributions of Mathematical Theory to Epidemics, *Proceedings of Royal Society, London – Series A*, **1932**, 138, 55 – 83.

[3] WO Kermack, AG McKendrick, Contributions of Mathematical Theory to Epidemics, *Proceedings of Royal Society, London – Series A*, **1933**, 141, 94 – 122.

[4] E Gelenbe, Dealing with Software Viruses: A Biological Paradigm, *Inform. Sec. Tech. Rep*., **2007**, 12 (4) 242 – 250.

[5] Erol Gelenbe, Keeping Viruses under Control, *20th International Symposium on Computer and Information Sciences – ISCIS 2005, Lecture Notes in Computer Science, Springer*, **2005**, 3733, 304 – 311.

[6] Erol Gelenbe, Varol Kaptan, Yu Wang, Biological Metaphors for Agent Behaviour, *19th International Symposium on Computer and Information Sciences–ISCIS 2004, Lecture notes in Computer Science, Springer-Verlag*, **2004**, 3280, 667 - 675.

[7] JRC Piqueira and FB Cesar, Dynamic Models for Computer Virus Propagation, *Math. Prob. Eng.*, **2008,** Article ID 940526, 1 - 11.

[8] JRC Piqueira, BF Navarro and LHA Monteiro, Epidemiological Models Applied to Virus in Computer Network, *J. Comput. Sci.*, **2005**, 1 (1) 31 – 34.

[9] CC Zou, W Gong and D Towsley, Malicious Codes Propagation Modelling and Analysis under Dynamic Quarantine Defence, *Proceeding of the ACM CCS Workshop on Rapid Malcode, ACM*, **2003**, 51 – 60.

[10] D Moore, C Shannon, GM Voelker andS Savage, Internet Quarantine: Requirements for Containing Self-Propagating Code, *Proceeding of IEEE INFOCOM-2003,* **2003**, 85 - 91.

[11] CC Zou, WB Gong, D Towsley and LX Gao, The Monitoring and Early Detection of Internet Malicious Codes, *IEEE/ACM Trans. Network*, **2005**, 13 (5), 961-974.

[12] BK Mishra and DK Saini, SEIRS epidemic Model with Delay for Transmission of Malicious Objects in Computer Network, *Appl. Maths. Comp*., **2007**, 188 (2), 1476-1482.

[13] BK Mishra and DK Saini, Mathematical Models on Computer Viruses, *Appl. Maths. Comp.*, **2007**, 187 (2) 929-936.

[14] BK Mishra and N Jha, Fixed Period of Temporary Immunity After Run of Anti-Malicious Software on Computer Nodes, *Appl. Maths. Comp.,* **2007**, 190 (2), 1207 – 1212.

[15] BK Mishra and SK Pandey, Dynamic Model of Worms with Vertical Transmission in Computer Network, *Appl. Maths. Comput.,* **2011**, 217 (21), 8438 - 8446.

[16] BK Mishra and N Jha, SEIQRS Model for the Transmission of Malicious Objects in Computer Network, *Appl. Math. Modell.,* **2010**, 34, 710 –715.

[17] BK Mishra and SK Pandey, Fuzzy Epidemic Model for the Transmission of Worms in Computer Network, *Nonlin. Anal: Real World Applications*, **2010**, 11, 4335 - 4341.

[18] BK Mishra and SK Pandey, Effect of Antivirus Software on Infectious Nodes in Computer Network: A Mathematical Model, *Physics Letters A*, **2012**, 376, 2389 – 2393.

[19] JO Kephart, SR White and DM Chess, Computers and Epidemiology, *IEEE Spectrum*, **1993**, 20–26.

[20] MJ Keeling and KTD Eames, Network and Epidemic Models, *J. Roy. Soc. Interf.,* **2005**, 2 (4) 295 – 307.

[21] Ma M Williamson and J Leill, An Epidemiological Model of Virus Spread and Cleanup, **2003**.

[22] JO Kephart, A Biologically Inspired Immune System for Computers, *Proceeding of International Joint Conference on Artificial Intelligence,* **1995**, 137 - 145.

[23] MEJ Newman, S Forrest and J Balthrop, Email Networks and the Spread of Computer Virus, *Phys. Rev. E* **2002**, 66, 232 - 369.

[24] M Draief, A Ganesh and L Massouili, Thresholds for Virus Spread on Network, *Ann. Appl. Prob*., **2008**, 18 (2), 359 - 369.

[25] N Madar, T Kalisky, R Cohen, D Ben Avraham and S Havlin, Immunization and Epidemic Dynamics in Complex Networks, *Eur. Phys. J.*, **2004**, B 38 269-276.

[26] 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**.

[27] RM May and AL Lloyd, Infection Dynamics on Scale-Free Networks, *Phys. Rev. E*, **2001**, 64, 1– 3.

[28] S Datta and H Wang, The Effectiveness of Vaccinations on the Spread of Email-Borne Computer Virus, *IEEE CCECE/CCGEL*, **2005**, 219 – 223.

[29] S Forest, S Hofmeyr, A Somayaji and T Longstaff, Self-nonself Discrimination in a Computer, *Proceeding of IEEE Symposium on Computer Security and Privacy,* **1994**, 202– 212.

[30] T Chen and N Jamil, Effectiveness of Quarantine in Malicious Codes Epidemic, *IEEE International Conference on Communications*, **2006**, 2142–2147.

[31] D Hincapie, J Ospina and AU Afuwape, Epidemic Thresholds in SIR and SIIR Models Applying an Algorithmic Method, *Biosurveillance and Biosecurity*, **2008**, 119–130.