Analysis on Virus Propagation in the Computer Network

S M Omair[A], Samir Kumar Pandey[B]

[A]Department of Mathematics, Delhi Public School, Ranchi, India – 834 004
[B]Department of Mathematics, Xavier Institute of Polytechnic & Technology, Ranchi, India – 834 010

Abstract

A dynamical model on the propagation of viruses is established with vertical transmission in the computer network. We study the qualitative properties of this model and determined the basic reproduction number. By using Lyapunov function it is proved that, if R0 is less than or equal to one the virus free equilibrium is globally asymptotically stable and the viruses die out from the network. Numerical methods and MATLAB are used to solve and simulate the system of differential equations developed.

Keywords: *Virus, Computer Network, Differential Equation, Lyapunov Function, Mathematical Modelling.*

I. 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 are built to propagate without warning or user interaction, causing an increase in traffic service requests that will eventually lead to Cyber-attack.

To stop, or at least to decrease the attack 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.

II. FORMULATION OF MODEL AND EQUILIBRIUM POINTS

In this model, all the computers connected to the network are classified into four classes: Susceptible, Latent, Quarantine and Protected computers. Here, the susceptible class S(t) means virus free computers but have active potential to the virus attack , the latent class L(t) means infected computers and are able to propagate the viruses, the quarantine class Q(t) means such infected computers that are currently seized for the short period of time and the protected class P(t) means protected or recovered computers from the viruses using latest antivirus software which may again become susceptible. Without loss of generality, it is reasonable to assume that the total number of computers is constant. So, we may take,

$$S + L + Q + P \equiv 1 \qquad (1)$$

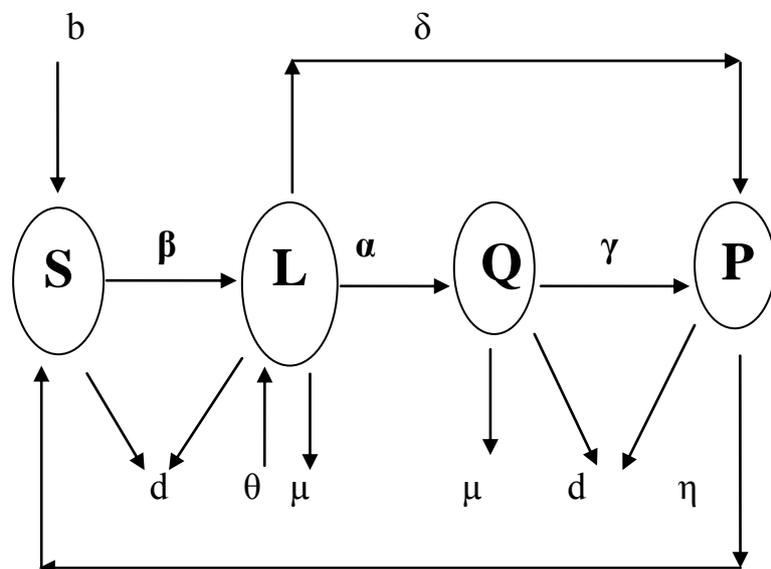The transmission of nodes between model classes is represented in figure 1.

Figure 1: Schematic diagram of the model

Where, β is the rate of contact to the network such that the total number of infections at time t becomes $\beta S(L+Q)$ which means that both classes (L & Q) have infectivity, b denotes the rate at which the new computers are introduced to the network. The parameters μ & d represents the rates at which computers are crashed due to reasons of attacks and other than attacks respectively. The parameters δ and γ and with (δ > γ > 0) are represented as two cure rates (L to P and Q to P respectively). The parameters α and η denote the rates of transmissions between the classes L to Q and P to S respectively. This model also assumes that the flow of viruses between the model classes can be spread through vertical transmission. In this case, the attack of viruses through vertical transmission increases at the rate θ and introduced directly at the class L. This model is formulated as the following system of differential equations:

$$\frac{dS}{dt} = b - \beta S(L+Q) - dS + \eta P$$

$$\frac{dL}{dt} = \beta S(L+Q) - (d + \mu + \alpha + \delta)L + \theta L$$

$$\frac{dQ}{dt} = \alpha L - (d + \mu + \gamma)Q$$

(2)

$$\frac{dP}{dt} = \gamma Q - (d + \eta)P$$

Using equation (1), it is sufficient to consider the following reduced model:

$$\frac{dS}{dt} = b - \beta S(L+Q) - dS + \eta(1 - S - L - Q)$$

$$\frac{dL}{dt} = \beta S(L+Q) - (d + \mu + \alpha + \delta)L + \theta L$$

$$\frac{dQ}{dt} = \alpha L - (d + \mu + \gamma)Q$$

(3)

The feasible region for the system (3) can be given as,

U = {(S, L, Q) : S ≥ 0, L ≥ 0, Q ≥ 0, S + L + Q ≤ 1} which is positive invariant.

Clearly, the system (3) has a virus free equilibrium U^0 (1, 0, 0) and a unique endemic equilibrium U^* (S^*, L^*, Q^*) that can be obtained by solving the equations of system (3). That is,

$$S^* = \frac{(d + \mu + \alpha + \delta - \theta)(d + \mu + \gamma)}{\beta(d + \mu + \gamma + \alpha)} = \frac{1}{R_0},$$

$$Q^* = \frac{\alpha}{(d + \mu + \gamma)} L^*$$

$$L^* =$$

$$\frac{(d + \eta)(d + \mu + \gamma)}{[d(d + \mu + \gamma)(d + \mu + \alpha + \delta - \theta) - b\beta(d + \mu + \gamma + \alpha)]}$$

$$\beta(d + \mu + \gamma + \alpha)$$

$$[\eta\delta(d + \mu + \gamma) + \eta\gamma\alpha - (d + \eta)(d + \mu + \gamma)(d + \mu + \alpha + \delta - \theta)]$$

(4)

Where, R_0 is the basic reproduction number defined as the average number of secondary infections that a single viral computer can produce in a totally susceptible class during its life cycle. This can be obtained by linearization of the last two equations of system (3) as,

$$\begin{vmatrix} L \\ Q \end{vmatrix} = (F - V)\begin{vmatrix} L \\ Q \end{vmatrix}$$, where, F and V can be defined by,

$$F = \begin{vmatrix} \beta & \beta \\ 0 & 0 \end{vmatrix}$$

and

$$V = \begin{bmatrix} (d + \mu + \alpha + \delta - \theta) & 0 \\ -\alpha & (d + \mu + \gamma) \end{bmatrix}$$

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

$$R_0 = \frac{\beta(d + \mu + \gamma + \alpha)}{(d + \mu + \gamma)(d + \mu + \alpha + \delta - \theta)}$$

(5)

III. STABILITY ANALYSIS

In this section, we discuss the local and global stability of the equilibrium U^0.

Theorem 1: The virus free equilibrium U^0 is locally asymptotically stable in U if $R_0 \le 1$ and is unstable if $R_0 > 1$.

Proof: For virus free equilibrium U^0 (1, 0, 0), the Jacobian matrix of the linearized system (3) can be given as,

$$J = \begin{vmatrix} -d - \eta & -\beta - \eta & -\beta - \eta \\ 0 & \beta - (d + \mu + \alpha + \delta - \theta) & \beta \\ 0 & \alpha & -d - \mu - \gamma \end{vmatrix}$$

Clearly, the characteristic roots of this matrix are $-d - \eta$, $\beta - (d + \mu + \alpha + \delta - \theta)$ and $-d - \mu - \gamma$ where first and third roots are negative. Since $R_0 \le 1$, then using (5), we can find that $\beta < (d + \mu + \alpha + \delta - \theta)$ which shows that the third root of the matrix becomes negative. Hence, the virus free equilibrium is locally asymptotically stable.

Consequently, if $R_0 > 1$, $\beta > (d + \mu + \alpha + \delta - \theta)$, so U_0 becomes unstable.

Theorem 2: if $R_0 \leq 1$, then U^0 is the only equilibrium and it is globally asymptotically stable in U, but if $R_0 > 1$ then it is unstable and there exists a unique endemic equilibrium U^*, also all solutions starting in U sufficiently close to U^0 move away from U^0.

Proof: Let us define the Lyapunov function,

$$M = \frac{1}{2}(L^2 + kQ^2) \tag{6}$$

Where, k is a positive constant and it can be easily seen that M is positive definite. Differentiating equation (6) w.r.t. t, we get,

$$\frac{dM}{dt} = L\frac{dL}{dt} + kQ\frac{dQ}{dt}$$

Using system (3) and without loss of generality, we can take $k = R_0$, we have,

$$\frac{dM}{dt} = \beta SL^2 + \beta SLQ - (d + \mu + \alpha + \delta - \theta)L^2 + \alpha R_0 LQ - R_0(d + \mu + \gamma)Q^2$$

$$= \beta\left(S - \frac{1}{R_0}\right)L^2 + \beta\left(S - \frac{1}{R_0}\right)LQ -$$

$$\left(\frac{\alpha\beta}{R_0}L^2 + R_0(d + \mu + \gamma)Q^2\right) + \left(\alpha R_0 + \frac{\beta}{R_0}\right)LQ$$

Since $R_0 \leq 1$, it can be easily verified that, $\frac{dM}{dt} \leq 0$ and

$\frac{dM}{dt} = 0$ iff, L = 0 and B = 0. Also, M → ∞ when L → ∞ or Q → ∞. So, according to LaSalle invariance principle [7], the virus free equilibrium U^0 is globally asymptotically stable. The other part of the theorem follows from the fact that $\frac{dM}{dt} > 0$ if $\frac{1}{R_0} < S$.

IV. CONCLUSION

A dynamic compartmental model has been developed for the transmission of viruses using vertical transmission in the computer network. We have discussed the characteristic of the different classes of nodes and obtained the basic reproduction number (which is less than

or equal to one) which shows that the system is locally asymptotically stable. Using the linear combination of the variables, a Lyapunov function is developed and the global stability of the system is established. The analysis of numerical simulations conclude that the system is totally recovered from the computer viruses (depicted in figure 2 - 4).
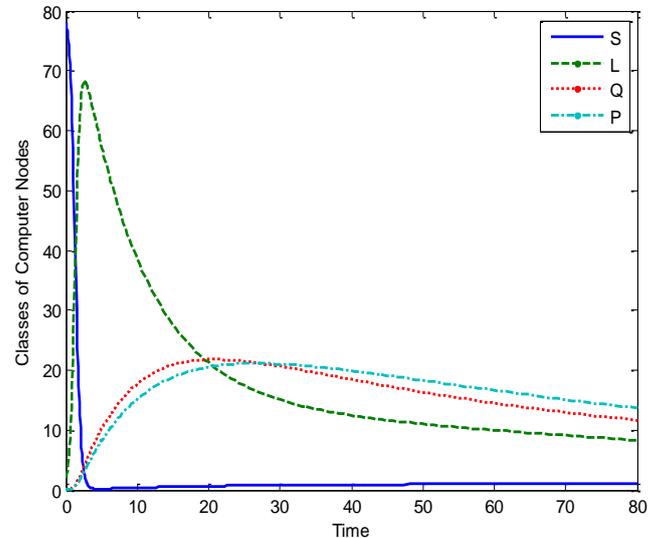

Figure 2: Dynamical behavior of the system with real parametric values, b = 0.09, β = 0.035, d = 0.0075, μ=0.01, α=0.045, η=0.045, δ = 0.035, γ = 0.025, θ = 0.005, $R_0 < 1$.
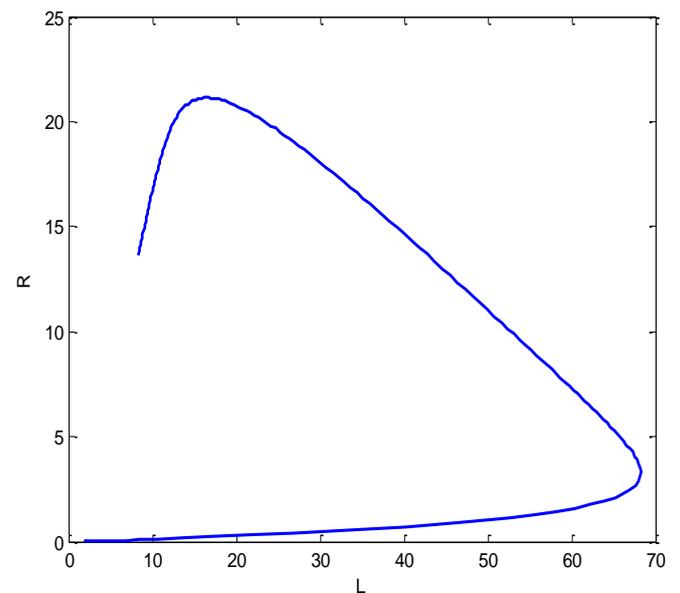

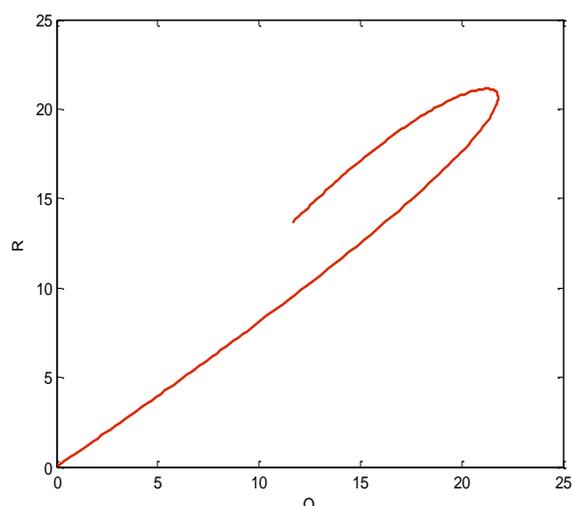Figure 3: Effect of L with respect to R with real parametric values, b = 0.09, β = 0.035, d = 0.0075, μ=0.01, α=0.045, η=0.045, δ = 0.035, γ = 0.025, θ = 0.005, $R_0 < 1$.

Figure 4: Effect of Q with respect to R with real parametric values, b = 0.09, β = 0.035, d = 0.0075, μ=0.01, α=0.045, η=0.045, δ = 0.035, γ = 0.025, θ = 0.005, R_0 < 1.

REFERENCES

[1] W.O. Kermack, A.G. McKendrick, Contributions of mathematical theory to epidemics, Proc. R. Soc. London – Series A, 115 (1927) 700–721.

[2] W.O. Kermack, A.G. McKendrick, Contributions of mathematical theory to epidemics, Proc. R. Soc. London – Series A, 138 (1932) 55 – 83.

[3] W.O. Kermack, A.G. McKendrick, Contributions of mathematical theory to epidemics, Proc. R. Soc. London – Series A, 141 (1933) 94 – 122.

[4] E. Gelenbe, Dealing with software viruses: A biological paradigm, Inform. Sec. Tech. Rep. 12 (4) (2007) 242 – 250.

[5] Erol Gelenbe, Keeping viruses under control, in: Computer and Information Sciences – ISCIS 2005, 20th International Symposium, Vol. 3733, Lecture notes in Comput. Sci. Springer (2005) 304 – 311.

[6] Erol Gelenbe, Varol Kaptan, Yu Wang, Biological Metaphors for agent behavior, in: Computer and Information Sciences – ISCIS 2004, 19th International Symposium Vol. 3280, Lecture notes in Comput. Sci., Springer-Verlag (2004) 667 - 675.

[7] R. C. robinson, An introduction to Dynamical System: Continuous and Discrete, Prentice Hall, 2004

[8] J.R.C. Piqueira, B.F. Navarro, L.H.A. Monteiro, Epidemiological models applied to virus in computer network, J. Comput. Sci. 1 (1) (2005) 31 – 34.

[9] C.C. Zou, W. Gong, D. Towsley, Malicious codes propagation modeling and analysis under dynamic quarantine defense, in: Proceeding of the ACM CCS Workshop on Rapid Malcode, ACM (2003), pp:51 – 60.

[10] D. Moore, C. Shannon, G.M. Voelker, S. Savage, Internet quarantine: requirements for containing self-propagating code, in: Proceeding of IEEE INFOCOM2003, IEEE (2003) 85 - 91.

[11] C.C. Zou, W.B. Gong, D. Towsley, L.X. Gao, The monitoring and early detection of internet malicious codes, IEEE/ACM Trans. Network. 13 (5) (2005) 961-974.

[12] B.K. Mishra, D. K. Saini, SEIRS epidemic model with delay for transmission of malicious objects in computer network, Appl. Maths. Comp., 188 (2) (2007) 1476-1482.

[13] B.K. Mishra, D. K. Saini, Mathematical models on computer viruses, Appl. Maths. Comp., 187 (2) (2007) 929-936.

[14] B.K. Mishra, N. Jha, Fixed period of temporary immunity after run of anti-malicious software on computer nodes, Appl. Maths. Comp., 190 (2) (2007) 1207 – 1212.

[15] B. K. Mishra, S. K. Pandey. Dynamic Model of worms with vertical transmission in computer network, Appl. Maths. Comput., 217(21) (2011) 8438 - 8446.

[16] B. K. Mishra, N. Jha, SEIQRS model for the transmission of malicious objects in computer network, Appl. Math. Modell., 34 (2010) 710 –715.

[17] B. K. Mishra, S. K. Pandey, Fuzzy epidemic model for the transmission of worms in computer network, Nonlin. Anal: Real world Applications, 11 (2010) 4335 - 4341.

[18] B. K. Mishra, S. K. Pandey, Effect of antivirus software on infectious nodes in computer network: A mathematical model, Physics Letters A, 376 (2012), 2389 – 2393.

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

[20] M.J. Keeling, K.T.D. Eames, Network and epidemic models, J. Roy. Soc.Interf., 2 (4) (2005) 295 – 307.

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

[22] J.O. Kephart, A biologically inspired immune system for computers, in: Proceeding of International Joint Conference on Artificial Intelligence (1995) 137 - 145.

[23] M.E.J. Newman, S. Forrest, J.Balthrop, Email networks and the spread of computer virus, Phys. Rev. E 66 (2002) 232 - 369.

[24] M. Draief, A. Ganesh, L. Massouili, Thresholds for virus spread on network, Ann. Appl. Prob. 18 (2) (2008) 359 - 369.

[25] N. Madar, T. Kalisky, R. Cohen, D. Ben Avraham, S. Havlin, Immunization and epidemic dynamics in complex networks, Eur. Phys. J. B 38 (2004) 269-276.

[26] R. Pastor-Satorras, 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] R.M. May, A.L. Lloyd, Infection dynamics on scale-free networks, Phys. Rev. E 64 (066112) (2001) 1 – 3.

[28] S. Datta, H. Wang, The effectiveness of vaccinations on the spread of email-borne computer virus, in: IEEE CCECE/CCGEL, IEEE (2005) 219 – 223.

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

[30] T. Chen, N. Jamil, Effectiveness of quarantine in malicious codes epidemic, in: IEEE International Conference on Communications 2006, IEEE (2006) 2142 - 2147.