International Journal of Signal System Control and Engineering Application 2 (3-4): 56-60, 2009
ISSN: 1997-5422

Epidemic Model for Active Infectious Nodes in Computer Sub-Networks

[1]Bimal Kumar Mishra and [2]Prasant Kumar Nayak
[1]Department of Applied Mathematics, Birla Institute of Technology, Mesra, Ranchi 835 215, India
[2]Department of Mathematics, G.I.E.T., Gunupur 675 022, Orissa, India

Abstract: An epidemic model for active infectious nodes in computer sub-networks has been proposed where nodes continuously interact with each other. Nodes become infectious due to the attack of malicious objects (virus, worms, trojan horse etc.) either through internet or through secondary devices. Threshold condition and the doubling time for an epidemic to start have been obtained and it has been found that larger the basic reproductive rate, shorter is the doubling time. Numerical method has been employed to solve the system of equations and the behavior of the proportion for active and non-active nodes of infectious class has been critically analyzed. The simulation results may be helpful in simulating malicious objects epidemics in network.

Key words: Computer sub-networks, malicious objects, epidemic model, threshold, active infectious nodes

INTRODUCTION

The world has become a more interconnected place. Electronic communication, e-commerce, tele-therapy, e- governance, network services and the internet have become vital components of business strategies, government operations and private communications. Many organizations have become dependent on this cyber world for their daily activities. This interconnectivity has also brought forth those who wish to exploit it. Computer security has thus become a necessity in the cyber age.

While information dependence is increasing, the threat from malicious objects (virus, worms, trojan horse, etc.) is also on the rise. The number of computer viruses has been increasing exponentially from their first appearance in 1986 to over 74,000 different strains identified today. Viruses were once spread by sharing disks now, global connectivity allows malicious code to spread farther and faster. Similarly, computer misuse through network intrusion is on the rise.

There are several computational techniques that look to biology for inspiration. Some common examples include networks, evolutionary algorithms and immunological computation (Harmer *et al*., 2002). Many researchers have taken help of the biological system to understand the behavior of spread of malicious objects in a computer network and how to immune the computer system (Mishra and Saini, 2007a, b; Mishra and Jha, 2007; Cohen, 1987; Serazzi and Zanero, 2003; Kephart, 1995; Kephart and White, 1993; Kephart *et al*., 1993; Piqueira and Cesar, 2008; Navarro *et al*., 2005; Richard and Mark, 2005; Forest *et al*., 1994; Chen and Jamil, 2006; Wang and Wang, 2003). The action of malicious objects throughout a network can be studied by using epidemiological models for disease propagation (Mishra and Saini, 2007a, b; Mishra and Jha, 2007; Piqueira and Cesar, 2008; Navarro *et al*., 2005; Wang and Wang, 2003).

Based on the Kermack and McKendrick SIR model (Kermack and Mckendrick, 1927, 1932, 1933), dynamical models for malicious objects propagation were proposed, providing estimations for temporal evolutions of infected nodes depending on network parameters considering topological aspects of the network (Mishra and Saini, 2007a, b; Mishra and Jha, 2007; Kephart *et al*., 1993; Zou *et al*., 2005; Keeling and Eames, 2005; Williamson and Laeveillae, 2003).

This kind of approach was applied to e-mail propagation schemes (Newman *et al*., 2002) and modification of SIR models generated guides for infection prevention by using the concept of epidemiological threshold (Mishra and Saini, 2007a, b; Mishra and Jha, 2007; Draief *et al*., 2008). Richard and Mark (2005) propose an improved SEI (susceptible-exposed-infected) model to simulate virus propagation. However, they do not show the length of latency and take into account the impact of anti-virus software. The model SEIR proposed by the researchers. Yan and Liu (2006) assumes that recovery hosts have a permanent immunization period with a certain probability which is not consistent with real

Corresponding Author: Bimal Kumar Mishra, Department of Applied Mathematics, Birla Institute of Technology, Mesra, Ranchi 835 215, India

situation. In order to overcome limitation, Mishra and Saini (2007a, b) present a 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 models and antivirus counter measures to study the prevalence of virus, for example, virus immunization (Mishra and Jha, 2007; Kephart, 1995; Madar *et al*., 2004; Pastor-Satorras and Vespignani, 2002; May and Lloyd, 2001; Datta and Wang, 2005) and quarantine (Chen and Jamil, 2006; Zou *et al*., 2003; Moore *et al*.,. 2003; Mishra and Jha, 2010).

In this study, an epidemic model for active infectious nodes in computer sub-networks are discussed. This will provide an opportunity for us to study the behavior of malicious objects with self replicating properties and the time during which we must be cautious enough for the safety of the nodes in computer sub networks which are deemed important and desirable for understanding the malicious objects spread patterns as well as for management and control of the spread.

MATERIALS AND METHODS

Mathematical model formulation: To avoid the total crash of the computer network, researcher divide the complete computer network in various sub-networks. Each of the sub-networks has several nodes attached to it and has a continuous interaction with each other.

Assumptions:

- The number of nodes attached to a specific network at any time t and is assumed to be a variable
- Infected node is introduced into an infection-free population of susceptible nodes intentionally or non-intentionally
- Susceptible nodes die naturally at a rate μ
- Active infectious nodes die at a rate d due to the attack of malicious objects
- When a node is infected, it may self-replicate with a probability and may not self-replicate with a probability (1-q)
- Rate of transferal from a susceptible to infectious class is λc
- A proportion of infectious class is assumed to become non-active. These non-active nodes have been detected to have malicious objects present within them but they do not infect other nodes when interacted

Natural death of nodes equivalently mean to say the crashing of the nodes due to hardware and (or) software,

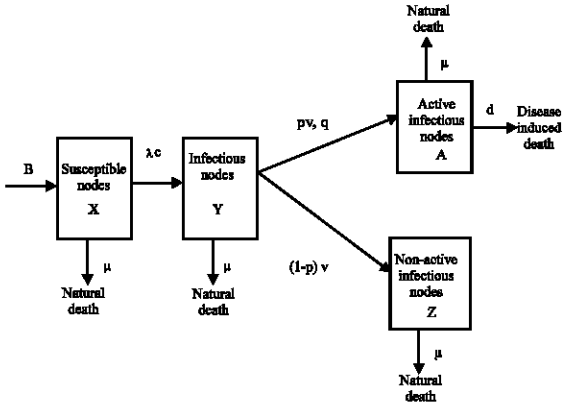

Fig. 1: Transmission of malicious objects in computer sub-networks

whereas the death due to disease of nodes equivalently mean to say the crashing of the nodes due to the attack of malicious objects. Based on the assumptions and computer network diagram (Fig. 1), we have the following systems of Equations (Murray, 2004):

$$\frac{dX}{dt} = B - \mu X - \lambda cX, \quad \lambda = \frac{\beta Y}{N} \tag{1}$$

$$\frac{dY}{dt} = \lambda cX - (q + v + \mu)Y \tag{2}$$

$$\frac{dA}{dt} = pvY + qY - (d + \mu)A \tag{3}$$

$$\frac{dZ}{dt} = (1 - p)vY - \mu Z \tag{4}$$

$$N(t) = X(t) + Y(t) + Z(t) + A(t) \tag{5}$$

As N (t) is variable, adding Eq. 1-5, we get:

$$\frac{dN}{dt} = B - \mu N - dA \tag{6}$$

If the number of secondary infection which arises from primary infection is >1 that is basic reproductive ratio R_0>1, then epidemic starts.

Initially that is at t = 0 if infected node (intentionally or non-intentionally) is introduced into an infection-free population of susceptible nodes of the computer sub-networks, X≈N then using Eq. 5, we have:

$$\frac{dY}{dt} \approx (\beta c - v - \mu)Y \approx v(R_0 - 1)Y \tag{7}$$

as the time lag 1/v from infection to active infectious stage is very much shorter than the average life expectancy $1/\mu$ of a susceptible node that is $v>>\mu$. We thus arrive to the approximate threshold condition for the start of an epidemic from Eq. 7 shown by:

$$R_0 \approx \frac{\beta c}{v} > 1 \tag{8}$$

The steady state when the epidemic starts for the system 1-5 is given by:

$$\begin{aligned} X^* &= \frac{(v+\mu)N^*}{c\beta} \\ Y^* &= \frac{(d+\mu)(B-\mu N^*)}{qpvd} \\ Z^* &= \frac{(1-p)(d+\mu)(B-\mu N^*)}{pd\mu} \\ A^* &= \frac{B-\mu N^*}{d} \\ N^* &= \frac{B\beta[\mu(v+d+\mu+q)+vd(1-p)]}{[v+\mu][B(d+\mu+q)-pv]} \end{aligned} \tag{9}$$

RESULTS ANS DISCUSSION

During the early stage of an epidemic (t = 0), all the nodes attached to the sub-networks are susceptible that is $X \approx N$ and the equation for the growth of the active infectious nodes is approximated by Eq. 7 whose solution is given by:

$$Y(t) = Y(0)e^{v(R_0-1)t} = Y(0)e^{rt}$$

Where Y (0) is the initial number of infectious nodes introduced into the susceptible population of the computer sub-networks.

Lemma: The intrinsic growth rate $r = v(R_0-1)$ is positive only if an epidemic exists that is $R_0>1$. Equation 10 will be helpful to obtain the doubling time for the epidemic that is the time t_d when $Y(t_d) = 2Y(0)$ as:

$$t_d = r^{-1}\ln 2 = \frac{\ln 2}{v(R_0-1)} \tag{10}$$

It is clear from Eq. 10 that larger the basic reproductive rate R_0, shorter is the doubling time. If we substitute Eq. 10 into Eq. 3 for the active infectious node we get:

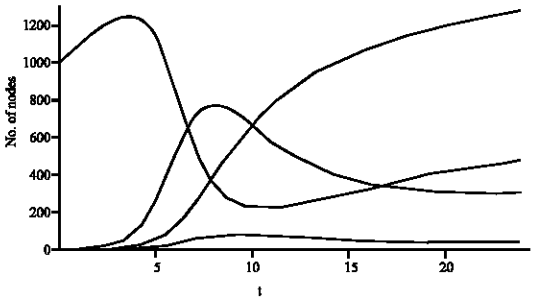

Fig. 2: Numerical simulation of the system Eq. 1-5 having parameter values b = 131, p = 0.3, v = 0.3 , c = 5, μ = 1/30, d = 0.8, R_0= 5 and β = 0.3, q = 0.05 with initial conditions X (0) + Y (0) = N (0) = 1000, A (0) = 0 = Z (0)

$$\frac{dA}{dt} = (pv+q)Y_0e^{rt} - (d+\mu)A$$

Early on in the epidemic there are no active infectious node that is A (0) = 0 and so the solution is given by:

$$A(t) = (pv+q)Y(0)\frac{e^{rt}-e^{-(d+\mu)t}}{r+d+\mu} \tag{11}$$

Numerical method has been employed to solve the system of Eq. 1-5 and the result is shown in Fig. 2. From Fig. 2, the model predicts that infectious active class A reaches at a maximum in 8-10 h. Further, there is the same observation for the nodes of infectious class Y which also reaches a maximum during 8-10 h. This is the time when we must be cautious for the safety of the nodes in the computer sub-networks. It is advised to run anti-malicious software during this time interval to minimize the spread of malicious objects when nodes of susceptible class X interact with the nodes of A class or Y class.

CONCLUSION

Inspired by the biological epidemic compartment models, a general epidemic model for the transmission of malicious objects in computer sub networks is developed. It has been shown that as the number of secondary infection which arises from primary infection is >1 that is basic reproductive ratio $R_0>1$ then epidemic starts. Numerical method has been employed to solve the system of equations and the behavior of the proportion for active and non-active nodes of infectious class has been analyzed. Time for the maximum infection is simulated using real parametric values and its use might help in estimating the dynamic behavior of malicious objects in

active infectious nodes of real systems. The future research will center on linearization about the steady state and it may be shown that (X, Y, Z, A) tends to (X*, Y*, Z*, A*) in a damped oscillatory manner with a period of oscillation given in terms of the model parameters. The model may be validated with simulations obtained by NS2 (Network simulator).

NOMENCLATURE

- $N(t)$ = Total number of nodes attached to a computer sub-networks
- $X(t)$ = Number of susceptible nodes in the computer sub-networks
- $Y(t)$ = Number of infectious nodes in the computer sub-networks
- $A(t)$ = Number of active infectious nodes (proportion of infectious class) in the computer sub-networks and interacting continuously with each other
- $Z(t)$ = Number of non-active nodes (proportion of infectious class) in the computer sub-networks
- B = Immigration rate of susceptible nodes into a computer sub-networks having population size of $N(t)$
- μ = Natural death rate of susceptible nodes
- d = Death rate of active infected nodes
- λ = Probability of acquiring infection from a randomly chosen node while interacting in the computer sub-networks
- c = Number of interacting nodes in the computer sub-networks
- β = Transmission probability
- p = Proportion of infectious class which are active infectious
- $1 - p$ = Proportion of infectious class which is assumed to become non-active
- v = Rate of conversion from infectious class to active infectious class and is assumed to be constant
- q = Probability of self replication of the kth malicious agent
- t_d = Doubling time of an epidemic

REFERENCES

Chen, T. and N. Jamil, 2006. Effectiveness of quarantine in worm epidemics. Proceedings of IEEE International Conference on Communications, Nov. 27-30, IEEE, pp: 2142-2147.

Cohen, F., 1987. Computer viruses: Theory and experiments. Comput. Security, 6: 22-35.

Datta, S. and H. Wang, 2005. The effectiveness of vaccinations on the spread of email-borne computer viruses. Proceedings of Canadian Conference on Electrical and Computer Engineering, May 1-4, Saskatoon, Sask, pp: 219-223.

Draief, M., A. Ganesh and L. Massouili, 2008. Thresholds for virus spread on networks. Ann. Applied Probability, 18: 359-378.

Forest, S., S. Hofmeyr, A. Somayaji and T. Longstaff, 1994. Self-nonself discrimination in a computer. Proceedings of IEEE Symposium on Computer Security and Privacy, May 16-18, IEEE Computer Society, USA., pp: 202-202.

Harmer, P.K., P.D. Williams, G.H. Gunsch and G.B. Lamont, 2002. An artificial immune system architecture for computer security applications. IEEE Trans. Evol. Comput., 6: 252-280.

Keeling, M.J. and K.T.D. Eames, 2005. Networks and epidemic models. J. R. Soc. Interface, 2: 295-307.

Kephart, J.O. and S.R White, 1993. Measuring and modeling computer virus prevalence. Proceedings of the IEEE Computer Security Symposium on Research in Security and Privacy, May 24-26, IEEE Computer Society, Washington, DC, USA., pp: 2-15.

Kephart, J.O., S.R. White and D.M. Chess, 1993. Computers and epidemiology. IEEE Spectrum, 30: 20-26.

Kephart, J.O., 1995. A biologically inspired immune system for computers. Proceedings of International Joint Conference on Artificial Intelligence, 1995. http://www.research.ibm.com/antivirus/SciPapers/Kephart/ALIFE4/alife4.distrib.html.

Kermack, W.O. and A.G. McKendrick, 1927. Contributions of mathematical theory to epidemics. Proc. R. Soc. London Ser. A, 115: 700-721.

Kermack, W.O. and A.G. McKendrick, 1932. Contributions of mathematical theory to epidemics. Proc. R. Soc. London Ser. A, 138: 55-83.

Kermack, W.O. and A.G. McKendrick, 1933. Contributions of mathematical theory to epidemics. Proc. R. Soc. London Ser. A, 141: 94-122.

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

May, R.M. and A.L. Lloyd, 2001. Infection dynamics on scale-free networks. Phys. Rev. E, 64: 066112-1-066112-3.

Mishra, B.K. and D.K. Saini, 2007a. Mathematical models on computer viruses. Applied Math. Comput., 187: 929-936.

Mishra, B.K. and D.K. Saini, 2007b. SEIRS epidemic model with delay for transmission of malicious objects in computer network. Applied Math. Comput., 188: 1476-1482.

Mishra, B.K. and N. Jha, 2007. Fixed period of temporary immunity after run of anti-malicious software on computer nodes. Applied Math. Comput., 190: 1207-1212.

Mishra, B.K. and N. Jha, 2010. SEIQRS model for the transmission of malicious objects in computer network. Applied Math. Modell., 34: 710-715.

Moore, D., C. Shannon, G.M. Voelker and S. Savage, 2003. Internet quarantine: Requirements for containing self-propagating code.IEEE INFOCOM, 3: 1901-1910.

Murray, J.D., 2004. Mathematical Biology I: An Introduction. 3rd Edn., Springer, USA.

Navarro, B.F., J.R.C. Piqueira and L.H.A. Monteiro, 2005. Epidemiological models applied to viruses in computer networks. J. Comput. Sci., 1: 31-34.

Newman, M.E.J., S. Forrest and J. Balthrop, 2002. Email networks and the spread of computer viruses. Phys. Rev. E, 66: 035101-1-035101-4.

Pastor-Satorras, R. and A. Vespignani, 2002. Epidemics and Immunization in Scale-Free Networks. Wiley-VCH, Berlin.

Piqueira, J.R.C. and F.B. Cesar, 2008. Dynamical models for computer viruses propagation. Math. Problems Eng., 2008: 1-11.

Richard, W.T. and J.C. Mark, 2005. Modeling virus propagation in peer-to-peer networks. Proceedings of IEEE International Conference on Information, Communications and Signal Processing, (ICICSP'05), McGill University, pp: 981-985.

Serazzi, G. and S. Zanero, 2003. Computer Virus Propagation Models. In: Analysis and Simulation of Computer and Telecom, Calzarossa, M.C. and E. Gelenbe (Eds.). Springer-Verlag, USA.

Wang, Y. and C.X. Wang, 2003. Modeling the effects of timing parameters on virus propagation. Proceedings of the 2003 ACM Workshop on Rapid Malcode, Oct. 27, ACM Press, Washington DC, USA., pp: 61-66.

Williamson, M.M. and J. Laeveillae, 2003. An epidemiological model of virus spread and cleanup. Technical Reports HPL-2003-39. http://www.hpl.hp.com/techreports/2003/HPL-2003-39.html.

Yan, P. and S. Liu, 2006. SEIR epidemic model with delay. J. Aust. Mathematical Soc. Ser. B Applied Mathematics, 48: 119-134.

Zou, C.C., W. Gong and D. Towsley, 2003. Worm propagation modeling and analysis under dynamic quarantine defense. Proceedings of the ACM CCS Workshop on Rapid Malcode, Oct. 27, ACM, Washington DC, USA., pp: 51-60.

Zou, C.C., W.B. Gong, D. Towsley and L.X. Gao, 2005. The monitoring and early detection of internet worms. IEEE/ACM Trans. Networking, 13: 961-974.