Mathematical Model for Cyber Attack in Computer Network

Yerra Shankar Rao, Department of Mathematics, Gandhi Institute of Excellent Technocrats (GIET), Ghangapatana, India
Aswin Kumar Rauta, Department of Mathematics, S. K. C. G. Autonomous College, Paralakhemundi, India
Hemraj Saini, Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, India
Tarini Charana Panda, Department of Mathematics, Ravenshaw University, Cuttack, India

ABSTRACT
This investigation focuses to develop an e-SEIRS (susceptible, exposed, infectious, recovered) epidemic computer network model to study the transmission of malicious code in a computer network and derive the approximate threshold condition (basic reproduction number) to examine the equilibrium and stability of the model. The authors have simulated the results for various parameters used in the model and Runge-Kutta Fehlberg fourth-fifth order method is employed to solve system of equations developed. They have studied the stability of crime level to equilibrium and found the critical value of threshold value determining whether or not the infectious free equilibrium is globally asymptotically stable and endemic equilibrium is locally asymptotically stable. The simulation results using MATLAB agree with the real life situations.

KEYWORDS
Computer Network, Epidemic Model, Globally Asymptotically Stable, Locally Asymptotically Stable, Threshold Value

INTRODUCTION
The advancement of society with the usage of computer software and hardware has created a new sort of crime in all domains known as cyber crime which is a new form of crime in the 21st century across the globe. So, criminal investigation is a major topic for research in the present scenario to many academicians and practitioners. Improvements of correspondence systems have made computers more critical in our day by day life. Diverse kind of specialized gadgets expanded human reliance on computers. Unfortunately, with the advancement of internet and other communication network, some mischievous individuals who differ in their opportunity cost for committing crime by various means of technological through computers involves in malicious activities. Links of computer networks and their communication channels spreads an infection and preventing the networks from doing its proper functionality which causes a huge loss to the society. Thus, the indefinite number of existing malicious codes and their appearance has a vital risk factor for every individuals and large sectors. Computer viruses or malicious objects such as worms and Trojan horses travel through a process in the computer networks which resembles to the way toward spreading plagues through a populace. The diseases that can be transmitted by vectors when managing with public health are comparable to the Virtual viruses that can propagate in a system of interacting computers. Therefore, concerning this
similarity an epidemic model like SEIR has been adopted and used to study the action of malicious objects through networks.

Transmission of malevolent codes in computer network is pandemic in nature, and different epidemiological models for disease propagation have been studied by many researchers (Mishra & Saini, 2007; Mishra & Nayak, 2009; Zou et al., 2003) for the activity of malicious objects during a network. The dynamic models for malicious objects transmission were developed on the basis of classical SIR model developed by Karmack and Kendrick (Kermack & McKendrick, 1933; Lahrouz et al., 2012) and provided the assessments for temporal advancements of infected nodes depending on network metrics which considered the topological facets of the network (Mishra & Saini, 2007; Zou et al., 2005; Kermack & McKendrick, 1932; Yan & Liu, 2006). This approach was also applied to e-mail circulation schemes (Piqueira et al., 2005) and alteration by using the theory of epidemiological threshold (Mishra & Saini, 2007; Draief et al., 2008; Gan et al., 2013) of SIR models produced the guides for infection anticipation. Richard et al, (Richard & Mark, 2005) simulated virus propagation using an enhanced SEI (susceptible-exposed-infected) model. Recently, the combination of antivirus countermeasures to revise the prevalence of virus and virus propagation models such as: virus immunization (Mishra & Nayak, 2009; Hale, 1980; Kephart et al., 1993; Kermack & McKendrick, 1927; Chen & Jamil, 2006; Yang et al., 2013; Hua & Guoqing, 2008; Zhu et al., 2012; Zhu et al., 2013) has become the growing research area for providing attentive solutions.

Substantial efforts have been made by many researchers to understand the effect of malicious behaviors on infection dynamics. However such efforts have not always made its way into mathematical models. Therefore, by accepting the spread law of virus upon the network and model analysis along with the characteristics of computer virus, we have developed reasonable computer virus propagation model. Based on our model, we would be able to obtain estimation from efficiency of different immunization method without assuming a set of initial infected agents and relying on a specific epidemiological model for spread of epidemics. It also provides a mean to human behaviors to infection dynamics by having informed individuals try to buy the anti malware soft ware and reduce susceptibility of their system. This model reveals the equilibrium and stability condition both qualitatively and quantitatively.

**MATHEMATICS MODEL AND ASSUMPTI ONS**

Consider the total computer nodes N (t) divided into four group, each of whom can either susceptible (S) or otherwise infected (I) with an infectious malicious object. Once the malicious objects enter into the network, the nodes become susceptible (S) and after a certain time delay the nodes become infected (E) and then it gets infectious (I). After it gets infectious, anti-malicious software is run which helps the nodes to recover (R) temporarily from the attack and provide temporary immunity to the node in the network.

The flow of malicious objects in the computer network is depicted in Figure 1.

\[
\frac{dS}{dt} = A - \beta SI - dS + \varepsilon R \\
\frac{dE}{dt} = \beta SI - dE - \alpha E \\
\frac{dI}{dt} = \alpha E - (d+\delta) I - \gamma I \\
\frac{dR}{dt} = \gamma I - dR - \varepsilon R
\]

Where N (t) = S (t) + E (t) + I (t) + R (t)
The TREND Meter: Monitoring the Energy Consumption of Networked Devices
Luca Chiaraviglio, Roberto Bruschi, Antonio Cianfrani, Olga Maria Jaramillo Ortiz and George Koutitas (2013). International Journal of Business Data Communications and Networking (pp. 27-44).
www.igi-global.com/article/the-trend-meter/88940?camid=4v1a