World Journal of Pharmaceutical and Life Sciences
WJPLS
www.wjpls.org
SJIF Impact Factor: 7.409

DYNAMIC MODEL ON E-COMMERCE NETWORK

Samir Kumar Pandey*

ICFAI University Jharkhand, Ranchi, India – 834001.

***Corresponding Author: Samir Kumar Pandey**
ICFAI University Jharkhand, Ranchi, India – 834001.

Article Received on 20/02/2024 **Article Revised on 10/03/2024** **Article Accepted on 30/03/2024**

ABSTRACT

Now-a-days, the major aim of e-commerce is to trade products and services online. Growing habits of e-commerce network increases the safety issues in the network. It means an e-commerce network can be simply compromised by attacks of malware. The nature of the spread of malware among the nodes can be easily related with the spread of biological viruses (infectious diseases) within human population of any locality. So we can easily apply the epidemic model for the spread of infectious disease within human population into the spread of malware among the nodes of a computer network. In this paper, we formulate a dynamic model for the propagation of malwares in an e-commerce network and study its vibrant behaviour. After categorizing the nodes of the network, based on their interface to the Internet. A schematic compartmental model is designed to represent the transmission of bots within the network and then differential equation model is formulated to represent the dynamics of all the compartments, respectively. We have also shown the result of numerical simulations using MATLAB to support the dynamism of our proposed model.

KEYWORDS: Cyber-attack, Dynamic Model, e-Commerce, Stability.

I. INTRODUCTION

Major types of cyber-attacks on e-commerce network includes fraudulent-email, pharming, snooping the shopper's computer, malware, man in the middle attack, Cross Site Scripting (CSS), password attacks, etc. Here, in this paper, we concentrate on a specific type of malware attack, known as bots attack, which is the basis for formulation of our proposed model and its solution, is discussed throughout the remaining portion of this paper.

The category of ecommerce which is discussed above is known as B2C type ecommerce. Examples of B2C type ecommerce are amazone.com, flipkart.com, etc. Similarly we have other categories of ecommerce like B2B, C2C, B2G, C2B, etc. In B2B type ecommerce, the business organization sells products or services to other business organizations or brings multiple buyers and sellers together in a central marketplace; e.g. metalsite.com. In C2C type ecommerce, consumers sell directly to other consumers via online classified ads and auctions or by selling personal services or expertise online, e.g. ebay.com. In B2G model, business organization sells to local, state and federal agencies; e.g. iGov.com. The C2B model, also called a reverse auction or demand collection model, enables buyers to name their own price, often binding, for a specific good or service generating demand. The website collects the "demand bids" and then offers the bids to the participating sellers. The examples of C2B e-commerce models are reverseaution.com andpriceline.com, etc.

So it is the requirement of all the above mentioned e-commerce model to connect all the departmental workstationsthrough the intranet. Here the growth of the e-commerce network may be vertical and / or horizontal; i.e. its growth may be hybrid. Each department of the organization has its own data and the data of their customers and all of these data are stored in the server(s) and all the workstations are connected to that server to store and retrieve those data as when required by the respective applications.

There are many different classes of malware that have varying ways of infecting systems and propagating themselves. Some of the more commonly known types of malware are viruses, worms, Trojans, bots, back doors, spyware, and adware. The activity of malware (virus/worms) throughout an e-commerce network can be captured by using epidemiological models for disease propagation.[1 – 7, 14 - 17] Based on the Kermack and McKendrick S-I-R classical epidemic model,[8 – 10] a dynamical mathematical model (S-Sp-I-Q) for malicious objects propagation is proposed.

II. Formulation of the Model

Dynamic models for infectious diseases or computer malware are mostly based on compartment structures that were initially proposed by Kermack and McKendrick.[8-10] and later developed by other mathematicians. To formulate a dynamic model or the transmission of an epidemic disease, the population in a given region is often divided into several different groups or compartments. Such a model describing the dynamic relations among these compartments is called a compartment model. Quarantine being the important remedial processes for malware attack in e-commerce network, several researchers developed model taking quarantine as one of the compartment in the epidemic models.[11 - 13] The total number of nodes (N) in our e-commerce network is divided into four classes (compartments): Susceptible (S), Susceptible with Protection (Sp), Infected (I), Quarantine (Q).

That is, $S + Sp + I + Q = N$ (1)

Susceptible (S) Class: This class includes those nodes of the network which are free from infection i.e. they are healthy but they have an active potential threat of infection by the malicious software at any point of time. These nodes do not include antivirus software.

Susceptible with Protection (Sp) Class: This class includes those nodes of the network which are protected by the firewall and/or antivirus software.

Infected (I): The nodes of this class includes the units that have been infected and which now have the potential to transmit the malicious software to the rest of the nodes of the population on having adequate contacts with the Susceptible and 'Susceptible with Protection' class of the population.

Quarantine (Q): This class is used to separate the infectious nodes which may have been exposed to any infected node to see if that become affected. Once the nodes are added to the network it becomes the member of the S class. Initially all the nodes belong to the S class.

Once the antivirus software is installed into the nodes of the S class, it moves to the Sp class. If a node from S class is attacked by any virus or worms, then it moves to the I class. This model also assumes that the antivirus software may not be too much effective as it may be an expired version which has not been updated. In that case the nodes with expired version of antivirus software, may be moved back to the S class again or due to attack of antivirus that node may move directly to I class. This model also assumes that a node from I class may rescued by cleaning the malware from that node through the use of updated antivirus software. In that case, it moves back to the Sp class, otherwise that node is moved to the Q class. The nodes from the Q class are moved to the S class once it is confirmed that the node is free from any effect of malware. The above fact can be shown graphically by using the following model in Fig. 1.

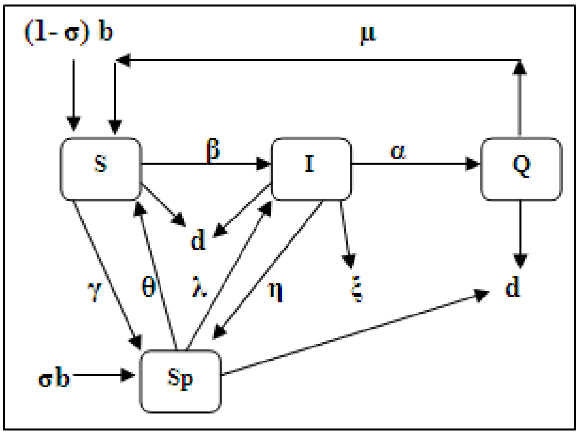

Fig. 1: (S – Sp – I – Q) Model – An epidemic model for the flow of worms in the e-commerce network.

The transmission between model classes can be expressed by the following system of differential equations

$$dS / dt = (1- \sigma) b + \mu Q + \theta Sp - \beta SI - \gamma S - dS \quad (2)$$

$$dSp / dt = \sigma b + \gamma S + \eta I - \theta Sp - dSp - \lambda Sp \quad (3)$$

$$dI / dt = \beta SI + \lambda Sp - \eta I - \xi I - dI - \alpha I \quad (4)$$

$$dQ / dt = \alpha I - dQ - \mu Q \quad (5)$$

where, b is the birth rate (new nodes attached to the network), d is the natural death rate , i.e; destroying of the computers because of the reason other than the attack of virus or worms, γ is the rate of execution of antivirus software initially (i.e; from class S to class Sp), θ is the rate of transfers of computer nodes from class Sp to class S, β is the rate of contact from class S to class I, α is the rate of quarantine from class I to class Q, μ is the rate of susceptible after recovery from class Q to class S, σ is the fraction of computer nodes (not belonging to the above mentioned classes, viz; S, Sp, I, and Q) on which we execute antivirus software and directly introduced at the class Sp, λ is the rate by which the nodes from the class Sp are infected by the malware are transformed to class I, ξ is the death rate (destroying of computer nodes) due to the attack of malware and η is the rate by which infected computers are recovered by updated antivirus and transferred back to the Sp class, i.e; from class I to class Sp. Using equation (2), (3) and (4), we get the value of Q, S and Sp as follows:

$$Q = [\alpha / (d + \mu)] * I \quad (6)$$

$$S = [(\theta+d+\lambda)*1/\lambda*(\eta+\xi+d+\alpha)] / [(\gamma*1/I) + \{\beta (\theta+d+\lambda)*1/\lambda\}] \quad (7)$$

$$Sp = 1/\lambda [\eta+\xi+d+\alpha-\beta*[[(\theta+d+\lambda)*1/ \lambda*(\eta+\xi+d+\alpha)] / [(\gamma*1/I) +\{\beta(\theta+d+\lambda)*1/\lambda\}]]]*I \quad (8)$$

III. Analyzing the Stability of the Model

Our proposed model contains four classes of nodes, viz; Susceptible(S) - Susceptible with Protection (Sp) – Infected (I) - Quarantine (Q) to represent the propagation of worms in e- commerce network.

The figure (Figure 2) shows the dynamic behavior of different classes of nodes with respect to time. Initially the number of nodes in the S class decreases drastically due to its transfer into the Sp class by installing the antivirus software into it and then it maintain a stable number of nodes in it. The nodes in Sp and Q classes increase initially and then decreaseswith time.

Installation of updated antivirus may contribute to the increase of nodes in Sp classes. The figure shows the sudden increase of nodes in I class due to the non-identification of the presence of the malware in the network. Once the malware is identified and removed by the updated antivirus software, it contributes to the sharp decrease in the number ofnodes in I class.

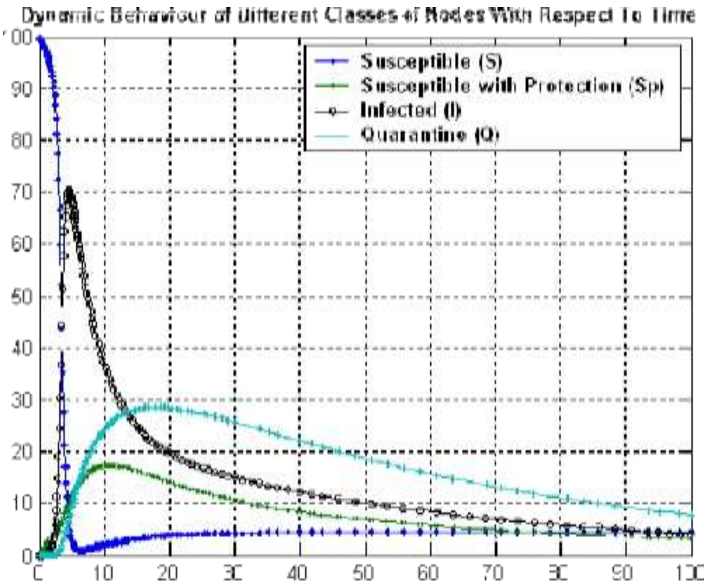

Fig. 2: Dynamic Behaviour of Different Classes of Nodes with Respect to Time when σ =0.09; μ =0.05; θ =0.07; β =0.03; γ =0.02; η=0.06; λ=0.04; ξ=0.03; α=0.08; b=0.07; d=0.01.

IV. CONCLUSION

Understanding the cyber threat is the first step in defending against it. There are many issues involved in securing the e-commerce network which is connected to the internet, e.g.; Malware infection, Being fraudulently represented as sender of phishing messages, Password sniffing, Denial of Service, etc. The spread of malware in the e-commerce network is epidemic in nature. We have developed an epidemic model for the spread of malware in e-commerce network where infected nodes are quarantined from the network. We have also used MATALB to simulate and analyze the behavior of different classes' of nodes among themselves and with respect to time to study the stability of the system. We observed that quarantining the highly infectious e-commerce nodes have positive contribution to the stability of the system. Continuous study of the system at different states of the e-commerce network may contribute to the stability of the system.

REFERENCES

1. B.K. Mishra, S.K. Pandey, Fuzzy epidemic model for the transmission of worms in computer network, Nonlinear Anal.: Real world Appl., 2010; 11: 4335–4341.
2. B.K. Mishra, S.K. Pandey, Effect of antivirus software on infectious nodes in computer network: a mathematical model, Phys. Lett. A, 2012; 376: 2389– 2393.
3. Erol Gelenbe, Varol Kaptan, YuWang, Biological metaphors for agent behaviour, in: Computer and Information SciencesISCIS, 19th International Symposium, in: Lecturer Notes in Computer Science, vol. 3280, Springer-Verlag, 2004; 667-675.
4. Samir Kumar Pandey, SS Prasad Shukla, A Kumar Yadav, D Singh Rajpoot, e-Epidemic Model on Covid-19: A Fuzzy Approach, Thirteenth International Conference on Contemporary Computing (IC3-2021), 2021; 328-332.
5. Pandey et al, Fourth wave Covid19 analyzing using mathematical seirs epidemic model & deep neural network, Multimedia Tools and Applications, 2023; 1-20.
6. 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.
7. Y.Wang, C.X.Wang, Modelling the effect of timing parameters on virus propagation, in: 2003 ACM Workshop on Rapid Malcode, ACM, 2003; 61-66.
8. W.O. Kermack, A.G. McKendrick, Contributions of mathematical theory to epidemics, Proc. Royal Soc. London – Series A., 1927; 115: 700–721.
9. W.O. Kermack, A.G. McKendrick, Contributions of mathematical theory to epidemics, Proc. Roy. Soc. London – Series A., 1932; 138: 55 – 83.
10. W.O. Kermack, A.G. McKendrick, Contributions of mathematical theory to epidemics, Proc. Royal Soc. London – Series A., 1933; 141: 94 – 122.
11. D.Moore, C.Shannon, G.M.Voelker, S. Savage, Internet quarantine: requirements for containing self C propagating code, in: Proceedings of IEEE INFOCOM, 2003; IEEE, 2003.
12. P. De, Y. Liu, S.K. Das, An epidemic theoretic

framework for evaluating broad-cast p protocols in wireless sensor networks, in: Proc. IEEE (Intl Conf. on Mobile Adhoc and sensor systems (MASS), (Pisa, Italy), Oct. 2007.

13. C.C. Zou, W. Gong, D. Towsley, Worm propagation modelling and analysis under dynamic quarantine defence, in: Proceedings of the ACM CCSWorkshop on Rapid Malcode, ACM, 2003; 51C60.
14. U Kumar, Samir K Pandey, Dynamic model on DDoS attack in computer network, Proceedings of the International Conference on Informatics and Analytics, 2016; 1-5.
15. Pandey et al, A Distributed Time Delay Model of Worms in Computer Network, Networking and Communication Engineering, 2011; 3(6): 441-447.
16. Pandey, SK; Omair, SM, e-Epidemic on the Computer Viruses in the Network, Eur. J. Adv. Eng. Technol, 2015; 2(9): 78-82.
17. Samir Kumar Pandey, B Samanta, Attacking Behaviour of Computer Worms on E-Commerce Network: A Dynamic Model, IJRASET, 2014.