Spread of Malware within an E-Commerce Network with Quarantine: A Dynamic Model

[#1]Biswarup Samanta, [#2]Samir Kumar Pandey
[#1]*Asst. Professor, Department of Computer Science, Jharkhand Rai University, Ranchi, Jharkhand, India.*
[#2]*Asst. Professor, Department of Mathematics, XIPT, Ranchi, Jharkhand, India.*

Abstract: *Small business e-commerce sites are very good target for cyber-attack. They do not have sufficient resources required to deal with the attack. The extensive use of e-commerce websites create new ways for both image and brands to be attacked. Security of e-commerce websites is essential for compliance with laws and regulations as well as gaining and maintaining the trust of stakeholders, partners and customers. Attacks on customer's sensitive information have the adverse effect of decreasing the customer's faith on online transactions, which happens in e-commerce network. In this paper, we propose a dynamic transmission model (S_p-I-Q-S_p) of malicious objects in the e-commerce network and study its dynamic behaviours. Numerical method is employed to solve and simulate the system of equations developed. In this context, we give the threshold for determining whether the virus dies out completely. Then, we study the existence of equilibria, and analyse their local asymptotic stability. Results of numerical simulations are obtained using MATLAB. Interpretation of the model yields interesting exposures.*

Keywords: *e-commerce; dynamic model; malware; local stability; equilibrium point.*

I. INTRODUCTION

E-Commerce has changed how firms do business and is now defining how firms do business [7].Nowadays, e-commerce network has become an important technology for the dissemination of information and communicating business related data from customer to business or vice-versa. We have different categories of e-commerce network like B2B, B2C, C2C, B2G, C2B, etc. A network consists of hosts and router nodes. Routers form the backbone of the network and the hosts are placed at the edges of the network. Network security consists of the provisions and policies adopted by the administrator of the network to prevent and monitor unauthorized access, misuse or modification, or denial of service for a computer in a network [8]. Attackers first target the host nodes and then they propagate throughout the entire network. Malware propagate via network communications in a similar way as a virus spreads among people. The activity of malware (virus/worms) throughout an e-commerce network can be captured by using epidemiological models for disease propagation [4-6]. Based on the Kermack and McKendrick S-I-R classical epidemic model [1-3], a dynamic mathematical model (Sp-I-Q- Sp) for malicious objects propagation is proposed in this paper.

II. MODELLING THE SYSTEM

Dynamic model for infectious diseases are mostly based on compartment structures that were initially proposed by Kermack and McKendrick [1-3] and later developed by other mathematicians. Our Sp-I-Q-Sp model consists of basically three types of nodes as a whole which are discussed as follows:

The total number of nodes (N) in our e-commerce network is divided into three classes (compartments) : Susceptible with Protection (Sp), Infected (I), Quarantine (Q). That is,

$$Sp + I + Q = N \quad \text{(i)}$$

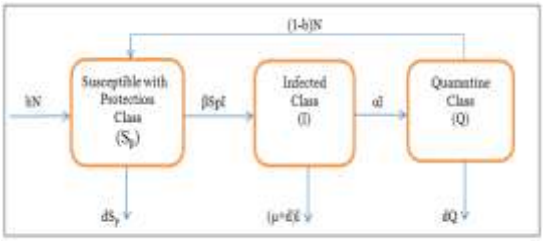
Susceptible with Protection (Sp) Class: This class includes those nodes of the network which are protected by the antivirus software and not yet infected with the malware or those susceptible to the malware.

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 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 with antivirus are added to the network it becomes the member of the S_p class. Initially all the nodes belong to the S_p class. If a node from S_p class is attacked by any virus or worms (due to obsolete antivirus), 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. This model also assumes that a node from I class may rescued by moving that node to the Q class. The nodes from the Q class are moved to the S_p 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 figure-1 below:

Different transmission rates of the nodes among different compartments (classes) in our proposed model are used to show the dynamism of the model are as follows: β: transmission rate of the nodes from S_p lass to I class; α: transmission rate of nodes from I class to Q class; b: birth rate of the S_p nodes in the network; d: natural death rate of the nodes in the network (i.e., crashing of nodes due to the reason other than the attack of malicious codes); μ: death rate of infectious nodes (I) in the network due to malware attack.

The corresponding system equations for the Internal Network of our proposed model are given in the following system (1) equation:

$$\frac{dS}{dt} = bN - \beta S_p I - dS_p$$
$$\frac{dI}{dt} = \beta S_p I - \alpha I - (\mu + d)I$$
$$\frac{dQ}{dt} = \alpha I - dQ$$

(1)

Equilibrium Points:

To calculate the equilibrium points for the proposed model, we set the right sides of the model equations of system (1) equal to zero, that is,

$$\frac{dS_p}{dt} = \frac{dI}{dt} = \frac{dQ}{dt} = 0$$

$$bN - \beta S_p I - dS_p = 0$$

(2)

$$\beta S_p I - \alpha I - (\mu + d)I = 0$$
$$\beta S_p - \alpha - (\mu + d) = 0$$
$$S_p^* = \frac{\alpha + \mu + d}{\beta} \quad (3)$$

$$\alpha I - dQ = 0 \quad (4)$$

III. Numerical Methods

Let U be used to represent the feasible region for the corresponding system (1) for the model given in the fig. 1. Hence we may write U as follows:

$$U = \{(S, I, Q) \in R^3 : S > 0, I \geq 0, Q \geq 0; S + I \leq 1, S + Q \leq 1, S + I + Q = 1\}$$

Putting the value of S_p in (2), we get the following:

$$bN - \beta \frac{\alpha + \mu + d}{\beta} I - d \frac{\alpha + \mu + d}{\beta} = 0$$
$$\Rightarrow -(\alpha + \mu + d)I = d \frac{\alpha + \mu + d}{\beta} - bN$$
$$I^* = \frac{bN}{\alpha + \mu + d} - \frac{d}{\beta} \quad (5)$$

Putting the value of I in (4), we get

$$\alpha\left(\frac{bN}{\alpha + \mu + d} - \frac{d}{\beta}\right) - dQ = 0$$
$$\Rightarrow Q^* = \left(\frac{bN}{\alpha + \mu + d} - \frac{d}{\beta}\right)\frac{\alpha}{d}$$

(6)

Jacobian Matrix for point $E_1 \equiv (S_p^*, I^*, Q^*)$

$$J_{E1} = \begin{bmatrix} -\beta I^* - d & -\beta S_p^* & 0 \\ \beta I^* & \beta S_p^* - (\alpha + \mu + d) & 0 \\ 0 & \alpha & -d \end{bmatrix}$$

Jacobian Matrix for point $E_0 \equiv (1,0,0)$

$$J_{E0} = \begin{bmatrix} -d & -\beta & 0 \\ 0 & \beta-(\alpha+\mu+d) & 0 \\ 0 & \alpha & -d \end{bmatrix}$$

A. *Calculation of Eigen value for J_{E1}:*

Characteristic equation for J_{E1} at $E_1 \equiv (S_p^*, I^*, Q^*)$:

$$(-d-\lambda)\{(-\beta I^* - d - \lambda)(\beta S_p^* - (\alpha+\mu+d) - \lambda) + \beta^2 I^* S_p^*\} = 0$$

Either

$$-d-\lambda = 0$$

$$\Rightarrow \lambda_1 = -d$$

Or,

$$(-\beta I^* - d - \lambda)(\beta S_p^* - (\alpha+\mu+d) - \lambda) + \beta^2 I^* S_p^* = 0$$

$$\Rightarrow \lambda^2 + (-\beta S_p^* + \alpha + \mu + d + \beta I^* + d)\lambda +$$

$$(-d\beta S_p^* + \alpha\beta I^* + d\alpha + \beta I^* \mu + d\mu + d\beta I^* + d^2) = 0$$

(7)

One Eigen value, λ_1 is negative and other two Eigen values may also found negative by solving the above equation (7) above.

B. *Calculation of Eigen value for J_{E0}:*

$E_0 \equiv (1,0,0)$

Characteristic equation for J_{E0} at:

$$(-d-\lambda)\{(-d-\lambda)(\beta-(\alpha+\mu+d)-\lambda)\} = 0$$

Either, $-d-\lambda = 0$

$$\Rightarrow \lambda_1 = -d$$

Or,

Either, $-d-\lambda = 0$

$$\Rightarrow \lambda_2 = -d$$

Or, $\beta-(\alpha+\mu+d)-\lambda = 0$

$$\Rightarrow \lambda_3 = \beta-(\alpha+\mu+d)$$

λ_3 Will be negative, if

$$\beta < \alpha+\mu+d$$

$$\Rightarrow \frac{\beta}{\alpha+\mu+d} < 1$$

$$\Rightarrow R_0 < 1$$

C. *Reproductive number (R_0):*

In epidemiology, the basic reproduction number of an infection is the mean number of secondary cases a typical single infected case will cause in a population with no immunity to the infection in the absence of interventions to control the infection. It is often denoted R0. This metric is useful because it helps to determine whether or not an infectious agent will spread through a population.

IV. Result and Analysis

In this section we will show the result of numerical simulations using MATLAB to support the dynamism and stability of our formulated model using graphs. Here we have analysed four cases as follows:

Case 1 Changes of Sp, I and Q over time when R_0 <1:

Here in this case we have plotted the different classes of nodes of our proposed model over time to show the dynamism and stability of the model when $R_0 < 1$, as shown in the figure 2 below:

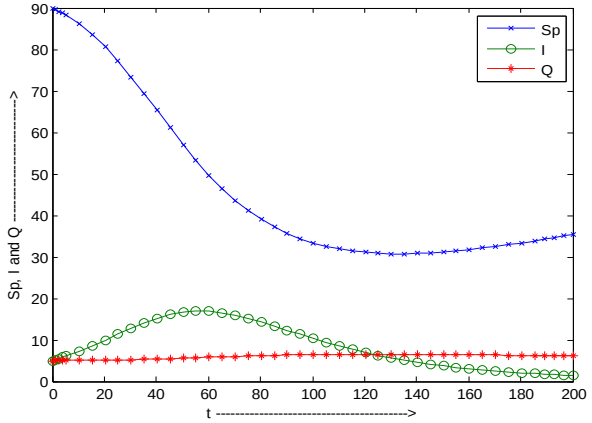


Fig. 2: Dynamism of Sp, I and Q over time (t=0-200; b=0.15;β=0.001; α=0.002; μ=0.05; d=0.00001)

We have done the said study for the initial condition, $\{S_p, I, Q\} = \{90, 5, 5\}$ for the time period 0-200 and at the value for all other transmission rates to satisfy the condition, $R_0 < 1$. The above graph shows the local stability of the system.

Case 2 I vs. Q:

Here in this case we have studied the behaviour of the nodes in Q with respect to the nodes in I for our equation system (1) for the time frame 0-200 and the dynamism is represented graphically in the following figure 3:

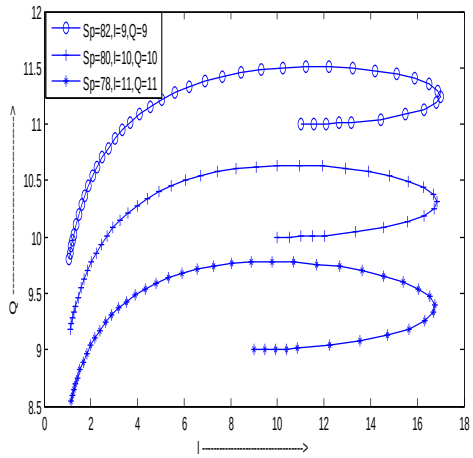


Fig. 3: Infected vs. Quarantine (t=0-200; b=0.15; β=0.001; α=0.002; μ=0.05; d=0.00001)

Here plotting is done for three different initial conditions, i.e. $\{S_p, I, Q\} = \{\{82, 9, 9\}; \{80, 10, 10\}; \{78, 11, 11\}\}$ and same value for b, μ, d, α and β for all the three cases. The graph in figure 3 shows that in the proposed system the number of infected nodes increases with slightly increase in quarantine nodes and then it shows the reverse behaviour. That indicates that although initially the system become unstable due to increase in infectious nodes in the systems but the low contact rate and transmission rate to quarantine class help the system to recover later by reducing the infectious nodes from the system.

Case 3 Sp vs. I:

The following figure 4 shows the changes of infected nodes over the changes of susceptible with protection nodes. The graph shows that the system become stable because the reduction of infected over time with increase in S_p class nodes.

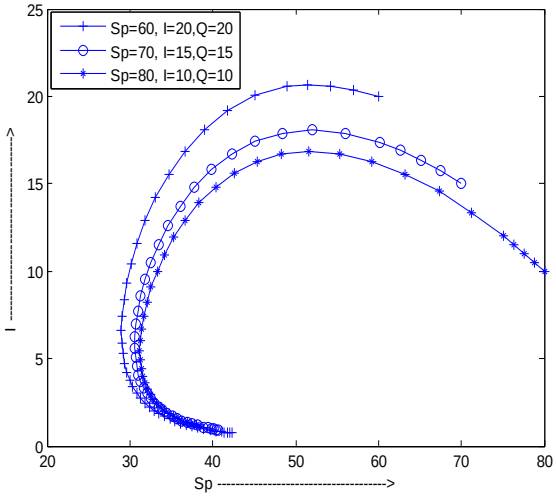


Fig. 4: Susceptible with Protection vs. Infected (t=0-200; b=0.15;β=0.001; α=0.002; μ=0.05; d=0.00001)

Case 4 Sp vs. Q:

The following figure 5 shows that as time increases, the number of Q nodes decreases and the nodes in S_p navigates and the system becomes stable when the number of nodes in S_p becomes 48.

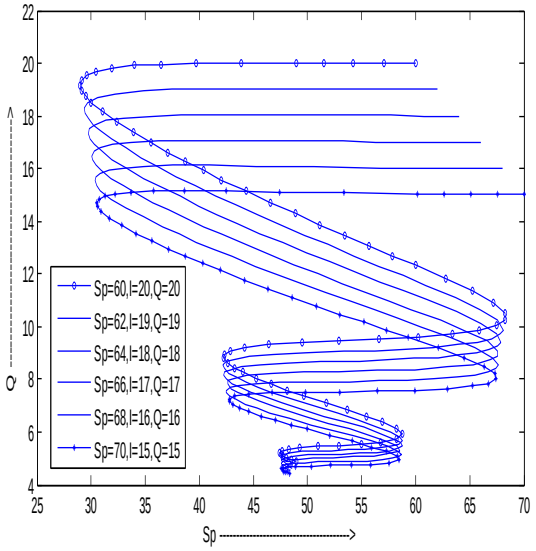


Fig. 5: Sp vs Q (t=0-1200; b=0.15;β=0.001; α=0.002; μ=0.05; d=0.00001)

V. CONCLUSION

Here in this paper we have proposed a dynamic mathematical model (Sp-I-Q- Sp) for malicious objects propagation. The behaviour of the nodes of different classes over time is also shown with the

help of diagrams. It shows that the quarantine is also a very good technique to make your system stable while $R_0 < 1$.

VI. LIMITATION

In this paper we have validated the local stability of our proposed model through graphs. One can find the global stability of our proposed model numerically and graphically also. We have also assumed that initially all the nodes will be introduced into S_p class with antivirus protection, but in the real life organization may introduce few nodes without antivirus protection also.

REFERENCES:

[1] W.O. Kermack, A.G. McKendrick, *Contributions of mathematical theory to epidemics*, Proc. R. Soc. Lond. Ser. A 115, 1927, 700-721.

[2] W.O. Kermack, A.G. McKendrick, *Contributions of mathematical theory to epidemics*, Proc. R. Soc. Lond. Ser. A 138, 1932, 55-83.

[3] W.O. Kermack, A.G. McKendrick, *Contributions of mathematical theory to epidemics*, Proc. R. Soc. Lond. Ser. A 141, 1933, 94-122.

[4] B.K. Mishra, S.K. Pandey, *Dynamic Model of worms with vertical transmission in computer network*, Appl. Math. Comput. 217 (21) (2011) 8438–8446, Elsevier.

[5] B.K. Mishra, S.K. Pandey, *Effect of antivirus software on infectious nodes in computer network: a mathematical model*, Phys. Lett. A 376 (2012) 2389–2393. Elsevier.

[6] Bimal Kumar Mishra, Navnit Jha, *Fixed period of temporary immunity after run of anti-malicious software on computer nodes*, Appl. Math. Comput. 190 (2), 2007, 1207-1212.

[7] Issa Najafi, *Identify Effective Factors for Improving E-Trust of E-Transactions in the Context of E-Commerce and E-Government;* International Journal of Computer Trends and Technology (IJCTT) – volume 17 Number 6 Nov 2014, 281-299.

[8] Rajesh R Chauhan, G S Praveen Kumar, *A Novel Approach to Detect Spam Worms Propagation with Monitoring the Footprinting*, International Journal of Computer Trends and Technology (IJCTT) – volume 6 number 3– Dec 2013, 143-149.