



DYNAMIC MODEL ON THE SPREAD OF BOTS FOR AN E-COMMERCE NETWORK

Biswarup Samanta

Department of Computer Science & Engineering
Amity University Jharkhand, Rnachi, India

Samir Kumar Pandey

Department of Mathematics
XIPT, Ranchi, Jharkhand, India

Abstract— The primary goal of e-commerce network is to sell goods and services online. Increasing usages of e-commerce network increases the security loop holes in the network. Nodes of an e-commerce network can be easily compromised by various types of malware. The nature of the spread of malware among the nodes of an e-commerce network can be easily compared 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. Various types of malware are used to attack the network of an organization, but, here, in this paper we concentrate and formulate a dynamic model for the propagation of bots in an e-commerce network and study its dynamic behavior. After categorizing the nodes of the network, based on their interface to the Internet, we have proposed two sub-models to formulate the overall architecture of the model. A schematic compartmental model is designed to represent the propagation of bots within the network and then differential equation model is formulated to represent the dynamics of all the compartments, respectively. The proposed system is solved and the basic reproduction number is also calculated to analyze the stability of the system. At the end, we have shown the result of numerical simulations using MATLAB to support the dynamism of our proposed model.

Keywords— cyber-attack, malware, bots, dynamic model, e-commerce, stability

I. INTRODUCTION

E-commerce has presented a new way of doing business all over the world using Internet. It refers to a wide range of online business activities for products and services. It is a powerful tool for business transformation that allows companies to enhance their supply-chain operation, reach new markets, and improve services for customer as well as for providers [10]. Commercial activities over the Internet have been growing in an exponential manner over the last few years. As the world becomes more electronically connected, systems running on network become more vulnerable to cyber-attack and this has posted a serious challenge for information security. Web based attacks are considered to be the greatest threat to any business or state as it is related to the confidentiality, availability, and integrity of the data for the business and the state, respectively.

Major types of cyber-attacks on e-commerce network includes fraudulent-email, phishing, 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.

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. A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, known as "botnet". The term botnet comes from

robot network. The computers under the botnet are the collection of computers that are connected to the internet and have been compromised by a cracker, computer virus, bots or Trojan horse and can be used to perform malicious tasks of one sort or another under the control of a remote server known as "bot herder" or "bot master" or "command-and-control (C&C) server". In most of the cases the owner of the systems of botnet are unaware that their systems are being used in this way and hence, these computers are metaphorically compared to zombies. The zombie computers of the botnet, which are controlled by a C&C server, are used to forward transmissions, including spam, viruses or worms to other computers on the e-commerce network. Bots have all the advantages of worms, but are generally much more versatile in their infection vector, and are often modified within hours of publication of a new exploit [14].

II. MODELING THE SYSTEM

In this section we will develop a model on the attack and spread of bots among the nodes within an e-commerce network. Several mathematical models have been developed which give clear view of attacking behavior as well as the transmission of malicious codes in network [1-9]. A typical e-commerce network consists of various types of computers, viz.; workstations, servers, routers and other devices also. Server may be of different types, viz.; web server, database server, application server, mail server, etc. All the servers are internal to the network, i.e.; they are not directly connected to the outside world. Apart from the servers there are some other workstations which are internal to the network and forms the backbone of the network, i.e.; an attacker or a valid client can't directly interact with those nodes also. But there will be some other computers (external nodes) which are the interfaces to the backbone of that network, i.e.; an attacker or a valid client can directly connect to those computers with the help of the Internet. A

bot master or C&C server first target those interface nodes of that network and turn them to zombie computers with the help of bots and turn them to the part of its botnet. Now those zombies will be controlled by the bot master. The bot master, with the help of those zombies, can infect other computers of that network by transmitting bots throughout the network and can reach and infect the targeted server of that network to make the entire network to crash. This scenario can be represented schematically as shown in the following fig. 1.

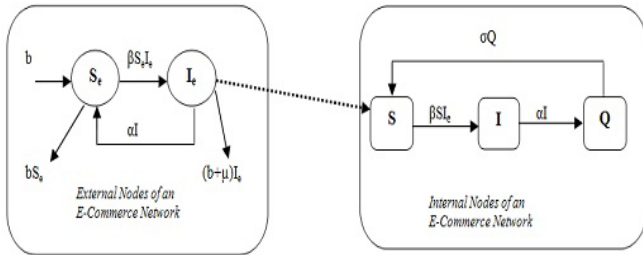


Fig. 1 Schematic representation of S-I-Q-S and S-I-S model.

Considering the above discussed scenario, we have created a schematic model consisting of two different, but interactive models. Before we proceed with the mathematical modeling of the above mentioned framework, we briefly discuss the basic assumption which will guide our formulation of equation system as follows.

Dynamic model for infectious diseases are mostly based on compartment structures that were initially proposed by Kermack and McKendrick [11-13] and later developed by other mathematicians. To formulate a dynamic model on the transmission of an epidemic disease, the entire population in a given region is often divided into several different groups or compartments. In this paper we apply “S-I-S” model for the population of the external computers which are directly connected to the Internet. Initially all the external nodes which are directly connected to the outside of the network through Internet are placed in “S” class. But, once a node of “S” class is infected by the bots sent from a “C&C server” to turn it into a zombie computer, that node is transferred into the “I” class. As the non-availability of the external node directly affect the services it provides to its client nodes, the nodes in the “I” class of our “S-I-S” model are repaired immediately with the help of antimalware software or any other means of repair and hence it is transferred back to the “S” class to resume its operation.

The population of the internal nodes of our e-commerce network is used to form the “S-I-Q-S” model. Initially all the internal nodes of our network are placed into the “S” class. The nodes of that “S” class may be affected by the zombies of the “S-I-S” model. Once, a node from “S” class is infected by the zombies of “S-I-S” model, it is transferred into the “I” class. The nodes of the “I” class are quarantined and transferred into “Q” class. The non-availability of the internal nodes may hamper the communication process within the network and hence the quarantine nodes are repaired immediately and transferred to the “S” class again to resume their operation. The entire population of the computers of our network is divided into the following five compartments:

- (i) Susceptible-External (S_e): represents the external nodes which are susceptible to direct attack from bots of an existing botnet.
- (ii) Infectious-External (I_e): represents the infected external nodes which are infectious and are capable of spreading the bots to other susceptible nodes.
- (iii) Susceptible-Internal(S): represents the internal nodes which are susceptible to the attack from the zombie computers of the botnet.
- (iv) Infectious-Internal (I): represents the infected internal nodes which are infectious and are capable of spreading the bots to other susceptible nodes.
- (v) Quarantine (Q): represents the internal nodes which are infected and separated.

The study of epidemic dynamics is an important theoretic approach to investigate the transmission dynamics of infectious diseases. It formulates mathematical models to describe the mechanism of disease transmissions and dynamics of infectious agents. Different transmission rates which are used to show the dynamism of our model are as follows: b : birth rate as well as death rate of the suspected external nodes; β : transmission rate coefficient; α : quarantine rate coefficient; σ : loss of immunity rate coefficient; μ : death rate of external nodes due to attack.

The corresponding model equations for Internal Nodes of an E-Commerce Network (S-I-Q-S) are given in the following system equation:

$$\left. \begin{aligned} \frac{dS}{dt} &= -\beta S I_e + \sigma Q, \\ \frac{dI}{dt} &= \beta S I_e - \alpha I, \\ \frac{dQ}{dt} &= \alpha I - \sigma Q. \end{aligned} \right\} \quad (1)$$

For the above system (1), we may assume the following equation,

$$\begin{aligned} S + I + Q &= 1 \\ \Rightarrow Q &= 1 - S - I. \end{aligned} \quad (a)$$

In the above equation (a), S, I and Q represents the fraction of the total nodes from susceptible, infectious and quarantine categories, respectively, present in the internal part of an e-commerce network of an organization.

The corresponding model equations for External Nodes of an E-Commerce Network are given in the following system equations:

$$\left. \begin{aligned} \frac{dS_e}{dt} &= b - bS_e - \beta S_e I_e + \sigma I_e, \\ \frac{dI_e}{dt} &= \beta S_e I_e - \alpha I_e - (b + \mu) I_e. \end{aligned} \right\} \quad (2)$$

For the above system (2), we may assume the following equation,

$$\begin{aligned} S_e + I_e &= 1 \\ \Rightarrow S_e &= 1 - I_e. \end{aligned} \quad (b)$$

In the above equation (b), S_e and I_e represents the fraction of the total nodes from susceptible and infectious

categories, respectively, present in the external part of an e-commerce network of an organization. By using the equations (a) and (b), respectively, we may simplify the above mentioned two systems equations, viz.; (1) and (2), into the following system equation:

$$\left. \begin{aligned} \frac{dS}{dt} &= -\beta SI_e + \sigma(1 - S - I), \\ \frac{dI}{dt} &= \beta SI_e - \alpha I, \\ \frac{dI_e}{dt} &= \beta(1 - I_e)I_e - \alpha I_e - (b + \mu)I_e. \end{aligned} \right\} \quad (3)$$

Let U be used to represent the feasible region for the corresponding system (3) for the model given in the fig.1. Hence we may write U as follows:
 $U = \{(S, I, I_e) \in R^3 : S > 0, I \geq 0, I_e \geq 0, S + I \leq 1, I_e \leq 1\}$.

III. SOLUTION AND BASIC REPRODUCTION NUMBER

In this section, we discuss about the solution of the system developed and find out the basic reproduction number, which helps us to analyze the stability of the system.

A. Solution of the System (Calculation of Equilibrium Points)

To calculate the equilibrium points for the proposed model, we set the right sides of the model equations of system (3) equal to zero, that is,

$$\frac{dS}{dt} = 0, \quad \frac{dI}{dt} = 0, \quad \frac{dI_e}{dt} = 0.$$

Using the above mentioned three equations, the trivial bots free equilibrium is obtained at point $E_1 \equiv (1, 0, 0)$ and the endemic equilibrium is found at point $E_2 \equiv (S^*, I^*, I_e^*)$, where,

$$\begin{aligned} S^* &= \frac{\alpha\sigma}{(\alpha + \sigma)(\beta - \alpha - b - \mu) + \sigma\alpha}, \\ I^* &= \frac{\sigma(\beta - \alpha - b - \mu)}{(\alpha - \sigma)(\beta - \alpha - b - \mu) + \sigma\alpha}, \\ I_e^* &= \frac{\beta - \alpha - b - \mu}{\beta}. \end{aligned}$$

B. Basic Reproduction Number

The basic reproduction number, also known as threshold number, is defined by the average number of secondary infections produced by one infected node of a network during the mean course of infection in completely susceptible nodes of the network. This is also simply known as reproductive number and is denoted by R_0 . The essential condition for an epidemic to occur is that the number of infected nodes should increase i.e. $\frac{dI}{dt} > 0$.

We get the following equation for the changes of infected nodes over time from system (1) as follows:

$$\frac{dI}{dt} = \beta SI_e - \alpha I. \quad (1.1)$$

By applying the above condition for an epidemic to occur on the above mentioned equation (1.1) we get

$$\begin{aligned} \frac{dI}{dt} &> 0 \\ \Rightarrow SI_e - \alpha I &> 0 \\ \Rightarrow \frac{\beta SI_e}{\alpha I} &> 1. \end{aligned}$$

The above condition is satisfied when $R_0 = \frac{\beta}{\alpha} > 1$, because

the transmissions to infectious nodes are greater than the transmission to quarantine node. Similarly from the system (2) we have the following equation

$$\frac{dI_e}{dt} = \beta S_e I_e - \alpha I_e - (b + \mu)I_e. \quad (2.1)$$

By applying the condition for an epidemic to occur on the above mentioned equation (2.1) we get,

$$\begin{aligned} \frac{dI_e}{dt} &> 0 \\ \Rightarrow \beta S_e I_e - \alpha I_e - (b + \mu)I_e &> 0 \\ \Rightarrow R_{0e} &= \frac{\beta}{\alpha + b + \mu}. \end{aligned}$$

IV. STABILITY OF THE SYSTEM

In this section we discuss the local stability at bots free equilibrium as well as at endemic equilibrium.

Theorem 1. *The malware free equilibrium E_1 of system (3) is locally asymptotically stable in U if $R_{0e} < 1$ and is unstable if $R_{0e} > 1$.*

Proof. Linearizing system (3) around the malware free equilibrium point $E_1 \equiv (1, 0, 0)$, we obtain the following Jacobian matrix

$$J_{E_1} = \begin{bmatrix} -\sigma & -\sigma & -\beta \\ 0 & -\alpha & \beta \\ 0 & 0 & \beta - (\alpha + b + \mu) \end{bmatrix}$$

To examine the local stability of the equilibria of system (3), for its Jacobian matrix J_{E_1} , we need to find out its eigenvalue. The characteristic equation for the above matrix (J_{E_1}) is given as follows:

$$(\beta - (\alpha + b + \mu) - \lambda)((-\sigma - \lambda)(-\alpha - \lambda)) = 0.$$

Hence the characteristic roots are $\lambda_1 = \beta - (\alpha + b + \mu), \lambda_2 = -\sigma, \lambda_3 = -\alpha$. As we know

that, σ and α are always positive, so the second (λ_2) and third (λ_3) Eigen values are negative.

Let us assume that the first Eigen value (λ_1) is also negative, i.e. $\beta - (\alpha + b + \mu) < 0$, which is equivalent to $R_{0e} < 1$ and that can be proved as follows:

$$\begin{aligned} &\beta - (\alpha + b + \mu) < 0 \\ \Rightarrow &\beta < (\alpha + b + \mu) \\ \Rightarrow &\frac{\beta}{\alpha + b + \mu} < 1 \\ \Rightarrow &R_{0e} < 1. \end{aligned}$$

Hence our assumption is true, that is the first Eigen value is also negative. Thus all the Eigen values of the Jacobian Matrix J_{E1} at the equilibrium $E_1 \equiv (1,0,0)$ are negative, and hence the malware free equilibrium is locally asymptotically stable, if $R_{0e} < 1$. On the other hand, if $\beta > (\alpha + b + \mu)$, then the first Eigen value (λ_1) is positive, i.e.

$$\begin{aligned} &\beta > (\alpha + b + \mu) \\ \Rightarrow &\frac{\beta}{\alpha + b + \mu} > 1 \\ \Rightarrow &R_{0e} > 1. \end{aligned}$$

Hence the equilibrium point $E_1 \equiv (1, 0, 0)$ becomes unstable, if $R_{0e} > 1$.

Theorem 2. *The endemic equilibrium E_2 of system (3) is locally asymptotically stable in U , if $R_{0e} > 1$.*

Proof. Following the same way as above Theorem 1, the system (3) is linearized at the endemic equilibrium point $E_2 \equiv (S^*, I^*, I_e^*)$ to obtain the following Jacobian matrix

$$J_{E2} = \begin{bmatrix} -\beta I_e^* - \sigma & -\sigma & -\beta S^* \\ \beta I_e^* & -\alpha & \beta S^* \\ 0 & 0 & -2\beta I_e^* + \beta - (\alpha + b + \mu) \end{bmatrix}$$

The characteristic equation for the above matrix (J_{E2}) is given as follows:

$$\{-2\beta I_e^* + \beta - (\alpha + b + \mu) - \lambda\} \{(\beta I_e^* + \sigma + \lambda)(\alpha + \lambda) + \sigma \beta I_e^*\} = 0$$

One of the Eigen values of the Jacobian Matrix J_{E2} at the equilibrium $E_2 \equiv (S^*, I^*, I_e^*)$ is found as follows:

$$\lambda_1 = -2\beta I_e^* + \beta - (\alpha + b + \mu).$$

Let us assume that $\lambda_1 < 0$, i.e.

$$-2\beta I_e^* + \beta - (\alpha + b + \mu) < 0.$$

After putting the value of I_e^* in the above equation, we get,

$$\begin{aligned} &-2\beta \frac{\beta - \alpha - b - \mu}{\beta} + \beta - (\alpha + b + \mu) < 0 \\ \Rightarrow &-2(\beta - \alpha - b - \mu) + \beta - (\alpha + b + \mu) < 0 \\ \Rightarrow &-\beta + (\alpha + b + \mu) < 0 \\ \Rightarrow &(\alpha + b + \mu) < \beta \\ \Rightarrow &\frac{\alpha + b + \mu}{\beta} < 1 \\ \Rightarrow &\frac{\beta}{\alpha + b + \mu} > 1. \end{aligned}$$

That is, $R_{0e} > 1$.

Hence the above assumption is true, i.e.; the first Eigen value $\lambda_1 = -2\beta I_e^* + \beta - (\alpha + b + \mu)$ is negative. The other two Eigen values (λ_2, λ_3) will be the roots of

$$(-2\beta I_e^* + \beta - (\alpha + b + \mu) - \lambda)((\beta I_e^* + \sigma + \lambda)(\alpha + \lambda) + \sigma \beta I_e^*) = 0$$

, which is the characteristic equation of J_{E2} . Since the sum of those two roots (λ_2, λ_3) is negative and the product of the roots is positive, therefore suggesting that both of its roots λ_2 and λ_3 are negative. So, all the three Eigen values of J_{E2} are negative when $R_{0e} > 1$. Hence the endemic equilibrium E_2 is locally asymptotically stable, if $R_{0e} > 1$.

V. SIMULATION AND DISCUSSION

In this section we will show the result of numerical simulations using MATLAB to support the dynamism of our formulated model.

A. Stability at Bots Free Equilibrium

The dynamic behavior of the entire population of system (3) is examined through simulation and the result is displayed in fig.2. The simulation is done for three different initial conditions, $(S, I, I_e) \equiv ((0.3,0.5,0.2), (0.5,0.3,0.2), (0.7,0.2,0.1))$ and we get the resultant data about the number of computer in different classes for all of the above three conditions as follows, $(S, I, I_e) \equiv ((1.000,0.000,0.000), (1.000,0.000,0.000), (1.000,0.000,0.000))$, i.e., final states are same for all the conditions and there are no infectious nodes present in the system when $R_{0e} < 1$. At this point the system is stable because all the bots are wiped out from the system and hence our proposed model is found to be asymptotically stable at $R_{0e} < 1$.

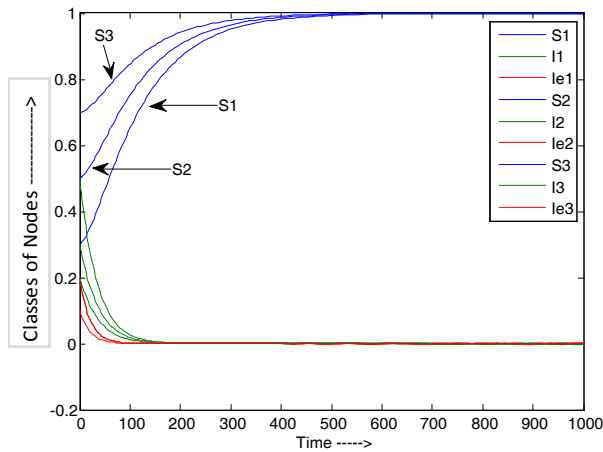


Fig. 2 Local stability for bots free equilibrium of system equation (3), when $R_{0e} < 1$ (when, $\beta=0.012$; $\alpha=0.010$; $b=0.020$; $\mu=0.010$).

B. Stability at Endemic Equilibrium

The stability of endemic equilibrium point is shown in fig. 2 for three different initial conditions same as fig. 2. Here also, we get the unique final states for all the given conditions as follows: $(S, I, I_e) \equiv ((0.0100, 0.2475, 0.9250), (0.0100, 0.2475, 0.9250), (0.0100, 0.2475, 0.9250))$. Hence the system is stable at this point, though the bots exists in the system. It is also found from the fig.3 that the system is asymptotically stable at this point when $R_{0e} > 1$.

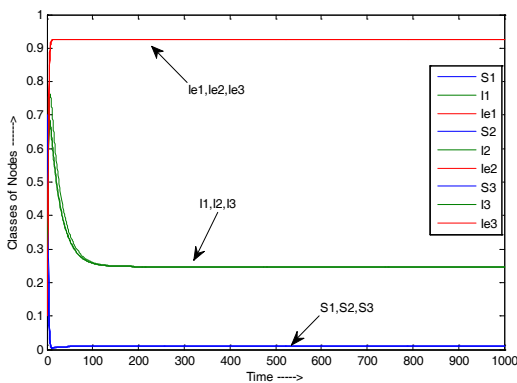


Fig. 3 Local stability for endemic equilibrium of system equation (3), when $R_{0e} > 1$ (when, $\beta=0.800$; $\alpha=0.030$; $b=0.020$; $\mu=0.010$)

C. Bots Free Equilibrium for System (1) & (2)

To observe the effect of increase in β on the dynamisms of the classes of nodes in system (1) & (2), we simulate the models using two different values of β (0.12, 0.92) for a given initial point $(S, I, Q, S_e, I_e) \equiv (0.4, 0.2, 0.1, 0.2, 0.1)$ and the given value of $(\sigma, \alpha, b, \mu) \equiv (0.01, 0.03, 0.02, 0.01)$ and we get two different set of values of $(S, I, Q, S_e, I_e) \equiv ((0.1667, 0.1333, 0.4000, 0.5000, 0.2000)$ and $(0.0149, 0.0173, 0.5138, 0.0652, 0.03739))$.

From our resultant data we can say that our proposed system become stable at $R_0 > 1$ due to the increase of quarantine nodes from Q_1 to Q_2 , where $Q_2 > Q_1$, as β is increased from 0.12 to 0.92. It is also observed from fig.4,

that the system is asymptotically stable at $R_0 > 1$, but bots till exists in the system.

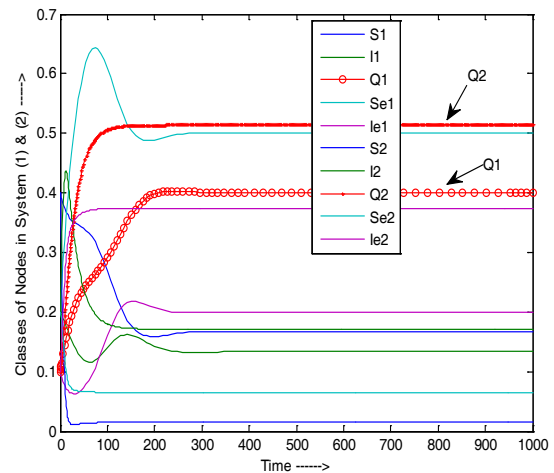


Fig. 4 Effect of increasing β on system dynamics at $R_0 > 1$.

D. Dynamics of Infectious-Internal (I) nodes while changing the value of β

Fig.5. shows the result of simulation for the evolution of I over time at initial point $(S, I, I_e) \equiv (0.7, 0.2, 0.1)$. We get the following five sets of values of $(S, I, I_e) \equiv ((0.0968, 0.2258, 0.5385), (0.0857, 0.2268, 0.5714), (0.0769, 0.2308, 0.6000), (0.0698, 0.2326, 0.6250), (0.0638, 0.2340, 0.6471))$, for five different values of $\beta = (0.13, 0.14, 0.15, 0.16, 0.17)$ and fixed value of $\sigma = 0.01, \alpha = b, \mu = 0.01$. It is found from fig. 5. , that the number of bots increases as β increases over time but the system becomes stable after a certain point of time and it proves that the endemic equilibrium is asymptotically stable at $R_{0e} > 1$.

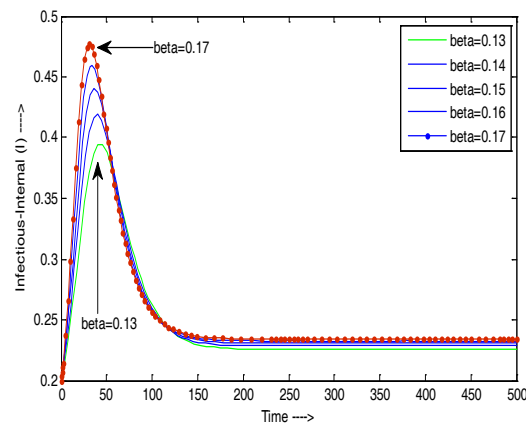


Fig. 5 Evolution of I over time, while β increases at $R_{0e} > 1$; ($\beta = 0.13/0.14/0.15/0.16/0.17, \sigma = 0.01, \alpha = b, \mu = 0.01$).

E. I VS Q by changing the values of β and α

The dynamisms of I vs. Q while changing the values of β and α to satisfy the following two conditions, i.e. $R_{0e} \leq 1$ and $R_{0e} > 1$, are shown in fig. 6 and the resultant data of the simulation are presented in Table 1.

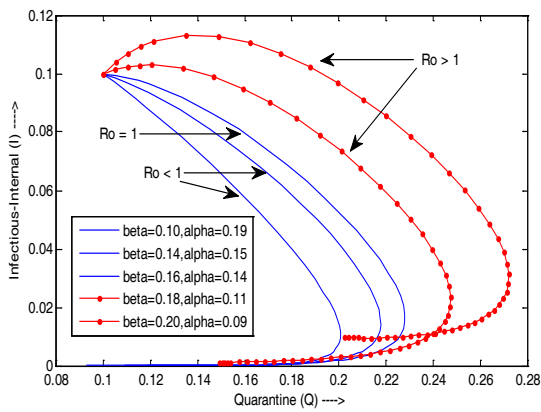


Fig. 6 Dynamics of I Vs Q when $R_{0e} > 1$ and $R_{0e} \leq 1$

It is found from the following Table 1, that there will be no bots in the system when $R_{0e} \leq 1$, which is a bots free equilibrium state and bots exists when $R_{0e} > 1$, i.e.; endemic equilibrium state. Fig. 6 also shows that the bots free equilibrium is asymptotically stable when $R_{0e} \leq 1$ and endemic equilibrium is also asymptotically stable when $R_{0e} > 1$.

TABLE 1. RESULT OF “I” vs. “Q” SIMULATION

σ	μ	b	α	β	R_{0e}	S	I	Q	Se	Ie
0.01	0.01	0.01	0.19	0.1	<1	0.5073	0	0.0927	0.6999	0
0.01	0.01	0.01	0.15	0.14	<1	0.4909	0	0.1091	0.6912	0
0.01	0.01	0.01	0.14	0.16	=1	0.4813	0	0.1187	0.6853	0
0.01	0.01	0.01	0.11	0.18	>1	0.4497	0.0012	0.1491	0.6619	0.0014
0.01	0.01	0.01	0.09	0.2	>1	0.3879	0.0099	0.2022	0.6023	0.0123

VI. CONCLUSION

In this paper, we have formulated an epidemic model to study the dynamics of the spread of bots in an e-commerce network through botnet. Categorizing the nodes of the networks based on their interface to the Internet, we have formulated two sub systems to represent the entire system for the propagation of bots. We have observed that if the basic reproduction number is less than unity, then the system is bots free and the bot free equilibrium is locally asymptotically stable. It is also found that when the reproduction number is greater than one, the system is also stable although bots persist in the system. During the analysis of the dynamism of the proposed model it is also found that the Infectious-Internal nodes are increased up to a certain peak over a period of time, but after a certain point of time it stabilizes. And while analyzing the dynamism of

Infectious nodes over the Quarantine nodes by increasing the infectivity contact rate, it is found that bots can exists in the system if $R_{0e} > 1$, but the system is bots free when $R_{0e} \leq 1$.

VII. REFERENCES

- [1] 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.
- [2] B.K. Mishra, S.K. Pandey, Fuzzy epidemic model for the transmission of worms in computer network, *Nonlinear Anal.: Real world Appl.* 11 (2010) 4335–4341.
- [3] 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.
- [4] B. Samanta, S. K. Pandey; Attacking Behaviour of Computer Worms on E-Commerce Network : A Dynamic Model; *IJRASET*; Vol. 2 Issue XII, Dec 2014.
- [5] Erol Gelenbe, Varol Kaptan, YuWang, Biological metaphors for agent behaviour, in: *Computer and Information Sciences ISCS 2004*, 19th International Symposium, in: *Lecturer Notes in Computer Science*, vol. 3280, Springer-Verlag, 2004, pp. 667-675.
- [6] 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.
- [7] Y.Wang, C.X.Wang, Modelling the effect of timing parameters on virus propagation, in: *2003 ACM Workshop on Rapid Malcode*, ACM, 2003, pp. 61-66.
- [8] S. Forest, S. Hofmeyr, A. Somayaji, T. Longstaff, Self-nonsel self discrimination in a computer, in: *Proceeding of IEEE Symposium on Computer Security and Privacy*, 1994, pp. 202-212.
- [9] Bimal K. Mishra, Navnit Jha, SEIQRS model for the transmission of malicious objects in computer network, *Appl. Math. Model.* 34 (2010) 710-715.
- [10] S. Yasin, K. Haseeb, R. Qureshi; “Cryptography Based E-Commerce Security: A Review”; *IJCSI*; Vol. 9, Issue 2, No 1, March 2012.
- [11] W.O. Kermack, A.G. McKendrick, Contributions of mathematical theory to epidemics, *Proc. R. Soc. Lond. Ser. A* 115, 1927, 700-721.
- [12] W.O. Kermack, A.G. McKendrick, Contributions of mathematical theory to epidemics, *Proc. R. Soc. Lond. Ser. A* 138, 1932, 55-83.
- [13] W.O. Kermack, A.G. McKendrick, Contributions of mathematical theory to epidemics, *Proc. R. Soc. Lond. Ser. A* 141, 1933, 94-122.
- [14] <http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html#8>