World Journal of Engineering Research and Technology

www.wjert.org

Impact Factor: 7.029 Coden USA: WJERA4

DYNAMIC MODEL ON ATTACKING BEHAVIOR OF DDOS IN E-COMMERCE NETWORK

***Samir Kumar Pandey**

ICFAI Tech School. The ICFAI University Jharkhand, Ranchi.

Article Received on 29/12/2025 **Article Revised on 19/01/2026** **Article Published on 01/02/2026**

***Corresponding Author**

Samir Kumar Pandey

ICFAI Tech School. The ICFAI University Jharkhand, Ranchi.

https://doi.org/10.5281/zenodo.18441201

How to cite this Article: Samir Kumar Pandey. (2026). Dynamic Model on Attacking Behavior of Ddos In E-Commerce Network. World Journal of Engineering Research and Technology, 12(2), 140–148.

ABSTRACT

The "information warfare" can hit and completely break down critical IT infrastructure of an organization or a country. Cybercrime has many types, but, in this paper we have focused on DDoS attack into an E-Commerce network to spread bots throughout the network. DDoS attack can be used to sabotage a service or as a cover for bots delivery. In this paper a dynamic SIS – SEIRS model is proposed to represent the propagation of bots in E-Commerce network through DDoS attack. A mathematical model is also formulated to represent the dynamism of the members of different compartments of the model. Numerical methods are employed to solve and simulate the system of equations developed. Results of numerical simulations are obtained using MATLAB.

KEYWORDS: E-Commerce; Computer Network; Cyber-Attack; Network Security; Dynamic Model; Epidemic Model; Bots; Botnet; Malware.

1. INTRODUCTION

The growth of Internet technology has thrown several challenges in the form of requirement of a suitable cyber defense mechanism to protect the valuable business information stored in e-commerce systems and for information in transit over network. Towards this goal, it is very much necessary to understand the types of attack in the network and develop mathematical

model to represent their behavior. In this paper we will be developing a mathematical model to understand DDoS attack while delivering bots within an e-commerce network.

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make computer resources of a network unavailable to its legitimate user. In a DDoS attack, an attacker may use your computer to launch DDoS attack to another computer of your network or others by using various tools, like, Trinoo, Tribe Flood Network (TFN), Stacheldraht, Shaft, MStream, etc. Botnet is the popular medium to launch DoS/DDoS attacks. The term "Botnet" is used to refer to a group of compromised computers (also known as zombie computers) under the control of hackers, running malwares under a common command and control infrastructure.[17] A bot is an automated program for doing some particular task, often over a 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]

2. Modeling the System

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] In this section of our paper we will develop a model on DDoS attack to spread of bots within an e-commerce network. DDoS attack paralyze Internet systems by overwhelming servers, network links, and network devices like, routers, firewalls, etc., with bogus traffic,[15] A network is composed of hosts and routers and it has an edge and a core. The hosts live at the edge, while the core consists of an interconnected mesh of routers,[16] Hosts are the interface between the organization's internal network and external internet. Hosts are the gateway of attacks to spread the bots into the network.

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. We have divided the entire e-commerce network into two sub networks, viz.; External Network which basically consists of host computers (SIS model) and Internal Network consists of the remaining nodes (SEIR model) of that network, which includes routers, servers and other devices attached to the network. We have represented the DDoS attack and spread of malware into the network schematically by using an interactive epidemic SIS-SEIRS model which consists of two sub models as shown below in the following figure-1.

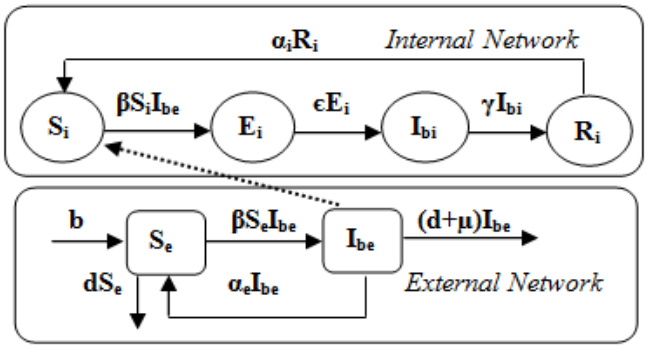

Fig. 1. Schematic presentation of S-I-S and S-E-I-R-S model.

Our entire SIS-SEIRS model consists of basically four types of nodes as a whole which are discussed as follows:

The fraction of Susceptible class nodes of the total population at any time in internal network and external network of the model are represented by Si and Se, respectively. The fraction of Exposed class nodes of the total population at any time in internal network of the model is represented by Ei. The fraction of Infectious class nodes of the total population at any time in internal network and external network of the model are represented by Ibi and Ibe, respectively. The fraction of Recovered class nodes of the total population at any time in internal network of the model is represented by Ri.

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 Susceptible class to Exposed class in internal network and Susceptible class to Infectious class in external network; ϵ: transmission rate of nodes from Exposed class to Infectious class in internal network; γ: rate of recovery in internal network, i.e., transmission rate of nodes from Infectious class to Recovered class in internal network; αi: transmission rate of nodes from Recovered class to Susceptible class in the internal network due loss of immunity (e.g., due to outdated version of antivirus); b: birth rate of the susceptible nodes in external network; d: natural death rate of susceptible nodes and infectious nodes in external network (i.e., crashing of nodes due to the reason other than the attack of malicious codes); μ: death rate of infectious nodes in external network due to DDoS attack; αe: rate of updated run of antivirus software which transfer the nodes from infectious class of external network to its susceptible class.

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

$$\begin{aligned}
\frac{dS_i}{dt} &= -\beta S_i I_{be} + \alpha_i R_i \\
\frac{dE_i}{dt} &= \beta S_i I_{be} - \varepsilon E_i \\
\frac{dI_{bi}}{dt} &= \varepsilon E_i - \gamma I_{bi} \\
\frac{dR_i}{dt} &= \gamma I_{bi} - \alpha_i R_i
\end{aligned} \tag{1}$$

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

$$\begin{aligned}
&S_i + E_i + I_{bi} + R_i = 1 \\
&\Rightarrow R_i = 1 - (S_i + E_i + I_{bi})
\end{aligned} \tag{a}$$

The corresponding system equations for the External Network of our proposed model are given in the following system (2) equation:

$$\begin{aligned}
\frac{dS_e}{dt} &= b - \beta S_e I_{be} - dS_e + \alpha_e I_{be} \\
\frac{dI_{be}}{dt} &= \beta S_e I_{be} - \alpha_e I_{be} - (d + \mu) I
\end{aligned} \tag{2}$$

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

$$S_e + I_{be} = 1 \Rightarrow S_e = 1 - I_{be} \tag{b}$$

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 (3) equation:

$$\begin{aligned}
\frac{dS_i}{dt} &= -\beta S_i I_{be} + \alpha_i (1 - (S_i + E_i + I_{bi})) \\
\frac{dE_i}{dt} &= \beta S_i I_{be} - \varepsilon E_i \\
\frac{dI_{bi}}{dt} &= \varepsilon E_i - \gamma I_{bi} \\
\frac{dI_{be}}{dt} &= \beta (1 - I_{be}) I_{be} - \alpha_e I_{be} - (d + \mu) I_{be}
\end{aligned} \tag{3}$$

Let Z be used to represent the feasible region for the corresponding system (3) for the model given in the fig. 1. Hence we may write Z as follows:

$$\begin{aligned}
Z = \{ &(S_i, E_i, I_{bi}, I_{be}) \in R^4 : S_i > 0, E_i \geq 0, I_{bi} \geq 0, I_{be} \geq 0, \\
&S_i + I_{bi} + I_{be} \leq 1, I_{bi} + I_{be} < 1 \}
\end{aligned}$$

3. Solution And Stability

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

A. 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,

$$\frac{dS_i}{dt}=0;\frac{dE_i}{dt}=0;\frac{dI_{bi}}{dt}=0;\frac{dI_{be}}{dt}=0$$

$$S_i^*=\frac{\varepsilon}{\beta-\alpha_e-d-\mu}.\alpha_i.\frac{1}{(\varepsilon+\frac{\alpha_i\varepsilon}{\beta-\alpha_e-d-\mu}+\alpha_i+\frac{\alpha_i\varepsilon}{\gamma})}$$

$$E_i^*=\alpha_i.\frac{1}{(\varepsilon+\frac{\alpha_i\varepsilon}{\beta-\alpha_e-d-\mu}+\alpha_i+\frac{\alpha_i\varepsilon}{\gamma})}$$

Using the above mentioned four equations, the trivial bots free equilibrium is obtained at point $E_1 \equiv \{1,0,0,0\}$ and the endemic equilibrium is found at point $E_2 \equiv \{S_i^*, E_i^*, I_{bi}^*, I_{be}^*\}$, where,

$$I_{bi}^*=\frac{\varepsilon}{\gamma}.\alpha_i.\frac{1}{(\varepsilon+\frac{\alpha_i\varepsilon}{\beta-\alpha_e-d-\mu}+\alpha_i+\frac{\alpha_i\varepsilon}{\gamma})}$$

$$I_{be}^*=\frac{\beta-\alpha_e-d-\mu}{\beta}$$

B. Basic Reproduction Number

Number of infected node should increase to become endemic, i.e.. For system (1)

$$\frac{dI}{dt}>0 \quad \frac{dI_{bi}}{dt}>0 \Rightarrow \varepsilon E_i-\gamma I_{bi}>0 \Rightarrow \frac{\varepsilon E_i}{\gamma I_{bi}}>1$$

For system (2)

$$\begin{aligned}&\beta S_e I_{be}-\alpha_e I_{be}-(d+\mu)I_{be}>0\\&\Rightarrow \beta S_e I_{be}-(\alpha_e+d+\mu)I_{be}>0\\&\Rightarrow \frac{\beta S_e}{(\alpha_e+d+\mu)}>1\end{aligned}$$

The above condition is satisfied, when the basic reproduction number, *C. Stability of The System*

$$R=\frac{\beta}{\alpha_e+d+\mu}>1$$

Theorem 1. *The malware free equilibrium E_1 of system (3) is locally asymptotically stable in Z if $R < 1$ and is unstable if $R > 1$.*

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

$$J_{E_1} = \begin{bmatrix} -\alpha_i & -\alpha_i & -\alpha_i & -\beta \\ 0 & -\varepsilon & 0 & \beta \\ 0 & \varepsilon & -\gamma & 0 \\ 0 & 0 & 0 & \beta-(\alpha_e+d+\mu) \end{bmatrix}$$

The characteristic equation for the above matrix (J_{E_1}) is given as follows:

So, either, $\{-(\beta-(\alpha_e+d+\mu)-\lambda)\}[-(\alpha_i+\lambda)\{(\varepsilon+\lambda)(\gamma+\lambda)\}]=0$

$$\{-(\beta-(\alpha_e+d+\mu)-\lambda)\}=0$$
$$\Rightarrow \lambda_1 = -(\alpha_e+d+\mu)+\beta \qquad (4)$$

From the above equation (4) it can be found that the value of λ_1 will be negative if the following holds:

$$\boldsymbol{\beta < \alpha_e + d + \mu}$$
$$\boldsymbol{\Rightarrow R < 1}$$

Or,

$$[-(\alpha_i+\lambda)\{(\varepsilon+\lambda)(\gamma+\lambda)\}]=0 \qquad (5)$$

From the above equation (5), we get the value of λ as follows:

$$\lambda_2 = -\alpha_i,\ \lambda_3 = -\varepsilon \text{ and } \lambda_4 = -\gamma$$

Hence all the Eigen values of the Jacobean matrix J_{E_1} at equilibrium point $E_1 \equiv \{1, 0, 0, 0\}$ are negative when $R < 1$. So, it is proved that our proposed system is stable at equilibrium point $E_1 \equiv \{1, 0, 0, 0\}$ when $R < 1$.

But, when $R > 1$, we get

$$\frac{\beta}{\alpha_e+d+\mu} > 1 \Rightarrow \beta > \alpha_e + d + \mu$$

Now given the above condition, i.e. $\beta > \alpha_e + d + \mu$, it can be easily found from the equation (9) that, the value of λ_1 becomes positive; hence our system becomes unstable. So, it is also proved that our proposed system becomes unstable at equilibrium point $E_1 \equiv \{1, 0, 0, 0\}$ when $R > 1$.

Theorem 2. *The endemic equilibrium E_2\of system (3) is locally asymptotically stable in Z if* $R > 1$.

Proof. Linearizing system (3) around the endemic equilibrium point $E_2 \equiv \{S_i^*, E_i^*, I_{bi}^*, I_{be}^*\}$, we obtain the following Jacobean matrix J_{E_2} :

$$J_{E_2} = \begin{bmatrix} -\beta I_{be} - \alpha_i & -\alpha_i & -\alpha_i & -\beta S_i \\ \beta I_{be} & -\varepsilon & 0 & \beta S_i \\ 0 & \varepsilon & -\gamma & 0 \\ 0 & 0 & 0 & \beta - 2\beta I_{be} - (\alpha_e + d + \mu) \end{bmatrix}$$

From the characteristic equation for the above matrix (J_{E2}) we get: Either,

$$\begin{aligned} &-\beta + 2\beta I_{be} + (\alpha_e + d + \mu) + \lambda = 0 \\ &\Rightarrow \lambda_1 = -\beta(2I_{be} + 1) - (\alpha_e + d + \mu) \end{aligned} \qquad (6)$$

From the above equation (6), it is found that the value of λ_1 is negative. Or,

$$\begin{aligned} &-\varepsilon(0 + \beta I_{be}\alpha_i) - (\gamma + \lambda)[(\beta I_{be} + \alpha_i + \lambda)(\varepsilon + \lambda) \\ &+ \alpha_i \beta I_{be}] = 0 \\ &\Rightarrow \lambda^3 + \lambda^2(\beta I_{be} + \alpha_i + \varepsilon + \gamma) + \\ &\lambda\{\varepsilon(\beta I_{be} + \alpha_i) + \alpha_i \beta I_{be} + \gamma(\beta I_{be} + \alpha_i + \varepsilon)\} + \\ &\{\gamma\varepsilon(\beta I_{be} + \alpha_i) + \gamma\alpha_i \beta I_{be} + \beta I_{be}\alpha_i\varepsilon\} = 0 \end{aligned} \qquad (7)$$

Let λ_2, λ_3, and λ_4 are the roots of the above equation (7). From the theory of equation, it is found that the value of λ_2, λ_3 and λ_4 is negative. And from equation (6) above, it is already proved that the first Eigen value λ_1 of J_{E2} is negative. So, all the four Eigen values viz., λ_1, λ_2, λ_3 and λ_4 of J_{E2} are negative when $R > 1$. Hence the endemic equilibrium at E_2 is locally asymptotically stable if $\boldsymbol{R > 1}$.

4. CONCLUSION

In this paper we have designed an interactive epidemic SIS-SEIRS model which consists of two interactive sub models to represent the DDoS attack and spread of bots into an e-commerce network. It is mathematically proved that the proposed system is asymptotically

stable at malware free equilibrium point if the reproduction number is less than one and unstable if the reproduction number is greater than 1. It is also proved mathematically that the proposed model is asymptotically stable at endemic equilibrium point if the reproduction number is greater than one. It is also shown graphically that the stability of the model is due to the absence of malware in the system when the reproduction number is less than one. The comparison between Si vs. Ibi shows that when β is increased by a fixed value (0.01), it decreases the value of Si and increases the value of Ibi and hence make the system more infectious. And the rate of increase in I_{bi} is more than the decrease of S_i. The limitation of our proposed model is that, it does not allow inclusion of new node in internal network.

REFERENCES

1. B.K. Mishra, S.K. Pandey, Dynamic Model of worms with vertical transmission in computer network, Appl. Math. Comput., 2011; 217(21): 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., 2010; 11: 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., 2012; 376: 2389–2393. Elsevier.
4. Biswarup 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 SciencesISCIS 2004, 19th International Symposium, in: Lecturer Notes in Computer Science, vol. 3280, Springer-Verlag, 2004; 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., 2005; 1(1): 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; 61-66.
8. S. 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.
9. Bimal K. Mishra, Navnit Jha, SEIQRS model for the transmission of malicious objects in computer network, Appl. Math. Model., 2010; 34.
10. S. Yasin, K. Haseeb, R. Qureshi; "Cryptography Based E-Commerce Security: A Review"; IJCSI; 1, March 2012; 9(2).

11. W.O. Kermack, A.G. McKendrick, Contributions of mathematical theory to epidemics, Proc. R. Soc. Lond. Ser. A., 1927; 115: 700-721.
12. W.O. Kermack, A.G. McKendrick, Contributions of mathematical theory to epidemics, Proc. R. Soc. Lond. Ser. A., 1932; 138: 55-83.
13. W.O. Kermack, A.G. McKendrick, Contributions of mathematical theory to epidemics, Proc. R. Soc. Lond. Ser. A, 1933; 141: 94-122.
14. http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html#8
15. http://www.cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/prod_white_paper0900aecd8011e927.html
16. D. N. Shah, "Mark Stamp's Information Security Principles and Practices", 2014 Ed., Wiley India Pvt. Ltd, 341–342.
17. N. Godbole, S. Belapure, "Cyber Security-Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", 2015 Ed., Wiley India Pvt. Ltd., 14.