IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

NUMERICAL MODEL FOR CYBER ATTACK IN CYBERSPACE

Debrupa Pal

Assistant Professor, Narula Institute of Technology, Kolkata, India

Abstract: This research emphasizes to establish an e-VEIRS (vulnerable, exhibited, infected, restored) widespread computer network model to examine the spread of malicious program in a computer network and deduce the estimated threshold requirement to explore the balance and stability of the model. The author has simulated the outputs of several parameters applied in the model and Runge-Kutta Fehlberg fourth-fifth order method is applied to obtain the solution of equations developed. They have examined the stability of the level of crime to reach equilibrium and discovered the crucial value of the threshold to determine if the contagious free equilibrium is asymptotically stable on a global scale and endemic equilibrium is asymptotically stable. on a local scale. Simulation output applying MATLAB comply with the actual situations.

Keyword: Computer Network, widespread Model, asymptotically stable at global level, asymptotically stable at local level, boundary value

I. INTRODUCTION

The progression of society with the utilization of software and hardware has developed a new kind of offense in all territories termed cyber-attacks that are a new type of crime in the 21st century across the world. Therefore, judicial inquiry is the main theme for investigation in the current situation for various research communities and academia. Advancements in communication systems have made computers more crucial in our daily lives. Diverse models of specialized models broadened people's dependence on computers. With the development of the internet and other correspondence systems, few evil individuals vary in their additional expenses for committing an offense by different technical means. The connection between the computer network and its communication channels transmits infection and prevents the network from performing its due function, causing enormous loss to society. Therefore, the unlimited number of prevailing malicious codes and their emergence are essential risk factors for everybody and large sectors. Malicious objects such as computer viruses or worms and Trojan horses spread through a process in a computer network, similar to the way the plague spreads to the public. Diseases that can be transmitted through vectors when controlling public health are analogous to virtual viruses that can spread in interactive computer systems. Hence, in reference to the resemblance, a model such as SEIR has been selected and applied to examine the behavior of malicious objects across networks.

The spread of malicious codes in a computer network is universal in nature, and various epidemiologic models for the spreading of the disease have been investigated by several researchers [1-3]. The dynamical models for the transfer of malicious objects were created based on the conventional SIR model proposed by [4] and suggested the estimates for temporal developments of affected nodes based on network metrics that took facets of the network under consideration [1] [5] [6]. This methodology was also implemented to e-mail circulation techniques [7] and modification by applying the hypothesis of epidemiologic threshold [8] [9] [10] of SIR models generated the guidebooks for infection expectancy. [11] modeled virus reproduction by applying improved SEI (susceptible-exposed-infected) model. In recent times, the association of antivirus counteracts to review the predominance of virus and virus extension models like virus immunization has turned into a fast-growing field of research for supplying alternative solutions [12-18].

Significant attempts have been made by several research workers to realize the impact of vicious behavior on contamination dynamics. Though such attempts have not always found a way into numerical models. Hence by approving the law of virus propagation over the network and model analysis besides the features of a computer virus, I have evolved an acceptable computer virus propagation model. Depending on the proposed model, I will be capable of acquiring an estimate from the effectiveness of various immunization techniques without presuming a class of affected agents at the outset and depending on a particular epidemiological model for the propagation of epidemics. It also furnishes the means for human conduct to contamination dynamics by having notified individuals seeking to purchase the anti-malware software and decrease the vulnerability of their system. This model displays the balance and constancy condition qualitative wise and quantitative wise.

II. NUMERICAL MODEL AND ASSUMPTIONS

Let the total computer nodes CN (t) partitioned into four bunches each containing either vulnerable (V) or infected (I) with an infectious malicious object. Whenever the malicious objects incorporate into the network, the nodes become vulnerable (V) and after a specific time delay the nodes become infected (F) and then become infectious (I). After the nodes become infectious, anti-malicious software is executed that supports the nodes to recover (R) temporally from the attack and produce transient immunity to the nodes in the network.

The circulation of malicious objects in the computer network is shown in Fig 1.

$$\frac{dV}{dt} = A - \beta VI - dV + \varepsilon R$$

$$\frac{dF}{dt} = \beta VI - dF + \alpha F \qquad (1)$$

$$\frac{dI}{dt} = \alpha F - (d + \delta)I - \gamma I$$

$$\frac{dR}{dt} = \gamma I - dR - \varepsilon R$$

where CN(t)= V(t)+F(t)+I(t)+R(t)

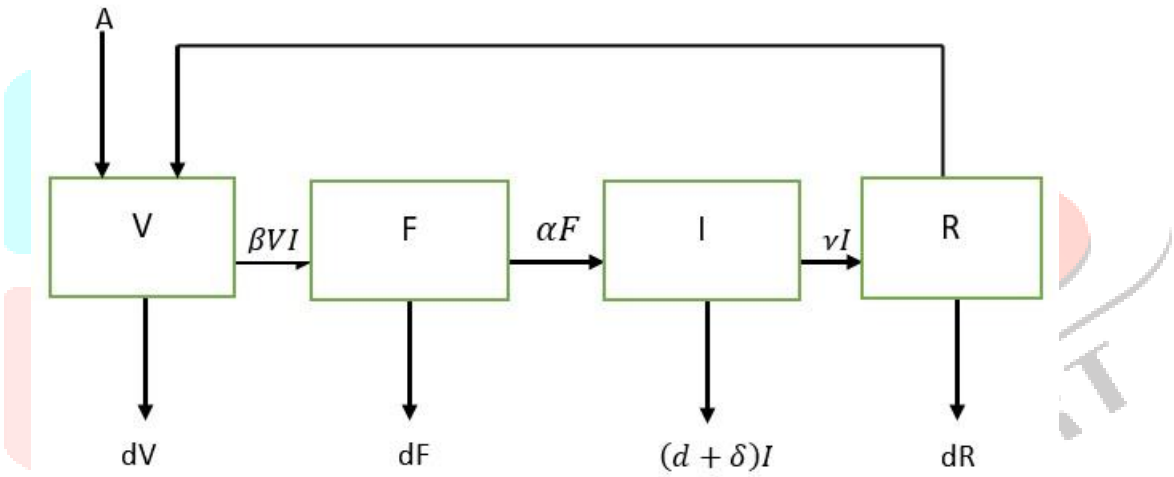

Figure 1: Malicious objects in computer

Adding all the equations from (1)

$$\frac{dCN(t)}{dt} = A - dCN(t) - \partial I$$

From the previous equation, it can be observed that, without worms I=0.

$N \to \frac{A}{d}$ Thus; $K_1 = \left[(V, F, I): V \geq 0, F \geq 0, I \geq 0 V + F + I \leq \frac{A}{d}\right]$ is a completely invariant area for the model.

III. EQULIBRIUM AND STABILITY ANALYSIS

Virus free equilibrium is $(\frac{A}{d}, 0, 0, 0)$, while endemic equilibrium is

V^*= (d+$\delta + \gamma$) $(d + \alpha)/\alpha\beta$

$F^* = (d + \delta + \gamma)/[d/\beta - A\alpha/(d + \alpha\, d + \delta + \gamma) + \alpha\varepsilon\gamma I/(d + \varepsilon\, d + \alpha\, d + \delta + \gamma)]$

$I^* = [d(d + \delta + \gamma)(d + \alpha)/\alpha\beta - A][\alpha(d + \epsilon)/(d + \delta + \gamma)(d + \alpha)\,(d + \epsilon) + \alpha\varepsilon\gamma]$

$R^* = \gamma I/(d + \varepsilon)$

IV. FOUNDATION OF PRODUCTION NUMBER

By applying next generation matrix method, let the RN0 be elementary reproduction number known as the average number of secondary infections, in other words an individual viral computer can produce an entirely vulnerable class throughout its life cycle.

$$\begin{pmatrix} F' \\ I' \end{pmatrix} = \begin{pmatrix} 0 & \beta V \\ 0 & 0 \end{pmatrix} \begin{pmatrix} F \\ I \end{pmatrix} - \begin{pmatrix} \alpha + d & 0 \\ -\alpha & (d + \delta + \gamma) \end{pmatrix} \begin{pmatrix} F \\ I \end{pmatrix}$$

E=$\begin{pmatrix} 0 & \beta V \\ 0 & 0 \end{pmatrix}$ and M= $\begin{pmatrix} \alpha + d & 0 \\ -\alpha & (d + \delta + \gamma) \end{pmatrix}$

$$M^{-1} = \begin{pmatrix} \frac{1}{(\alpha + d)} & 0 \\ \frac{\alpha}{(\alpha + d)(d + \delta + \gamma)} & \frac{1}{(d + \delta + \gamma)} \end{pmatrix}$$

Hence

$$EM^{-1} = \begin{pmatrix} \frac{\beta \alpha V_0}{(\alpha + d)(d + \delta + \gamma)} & \frac{\beta V_0}{(d + \delta + \gamma)} \\ 0 & 0 \end{pmatrix}$$

The spectral radius of the above-mentioned matrix is $\alpha\beta\ V_0/(\alpha + d)(d + \delta + \gamma)$

Hence elementary reproduction number is

$RN0 = \alpha\beta\ V_0/(\alpha + d)(d + \delta + \gamma)$

Two equilibrium point given by this model are

Virus free equilibrium $K_0 = \left(\frac{A}{d}, 0, 0\right)$

Endemic equilibrium $K^* = (V^*, F^*, I^*, RN^*)$

V. STABILITY ANALYSIS

Linearization of the model given by equation 1 is

$$K^* = \begin{pmatrix} -(\beta I + d) & 0 & -\beta V & \epsilon \\ \beta I & -(d + \alpha) & \beta V & 0 \\ 0 & 0 & -(d + \delta + \gamma) & 0 \\ 0 & 0 & 0 & -(d + \epsilon) \end{pmatrix}$$

Linearization of the model given by equation 1 at virus free equilibrium is

$$K^* = \begin{pmatrix} -d & 0 & -\beta \frac{A}{d} & \epsilon \\ 0 & -(d + \alpha) & \beta \frac{A}{d} & 0 \\ 0 & 0 & -(d + \delta + \gamma) & 0 \\ 0 & 0 & 0 & -(d + \epsilon) \end{pmatrix} \quad (2)$$

Eigen values of matrix 2 are $-d, -(d + \alpha), -(d + \delta + \gamma), -(d + \epsilon)$. Hence the model given by equation 1 are at virus free equilibrium. Hence K is asymptotically consistent locally.

At endemic equilibrium the linearization of the model given by equation 1

$$K^* = \begin{pmatrix} -(\beta I^* + d) & 0 & -\beta V^* & \epsilon \\ \beta I^* & -(d + \alpha) & \beta V^* & 0 \\ 0 & 0 & -(d + \delta + \gamma) & 0 \\ 0 & 0 & 0 & -(d + \epsilon) \end{pmatrix} \quad (3)$$

Eigen values of matrix 3 are $-(\beta I^* + d), -(d + \alpha), -(d + \delta + \gamma), -(d + \epsilon)$. As all Eigen value of matrix 3 is negative, Hence K is asymptotically consistent locally at endemic equilibrium.

Table 1. Routing table of each node

Symbol	Description	Baseline Value
N	Overall number under consideration	10000
V	Number of vulnerable at time t	V (0) 8900
E	Total number in exhibited class	E (0) 1000
I	Number of infected at time t	I (0) 100
A	Total number of new born	70
R	Total number of healed people with immunity at time t	R (0) =0
α	Rate of node from E to I class	0.7
β	Rate of contact	.0001
γ	Rate of node from I to R class	.08
ϵ	Rate of node from V to R class	.05
d	Natural death of a file	.2
δ	Death of the node due to disease	.2
RN_0	Preliminary reproduction number in case of endemic	1.390625
RN_0	Preliminary reproduction number for disease free case	0.0546875

VI. MODEL FRAMEWORK AND INITIAL VALUES

Table 1 represents the routing details of each node.

VII. DISCUSSION OF THE RESULTS

The suggested model consists of exposed classes besides vulnerable, infected, and recovered. I have utilized a volatile population malicious object transmission model in a computer network with persistent latency and immune time. The equilibrium of the model is derived and accordingly, graphs are plotted for analyzing the stability.

Runge-Kutta Fehlberg fourth-fifth order method is applied for solving the system of equations (1) and the performance of the vulnerable, exposed, infectious, and recovery nodes with reference to time is noted as represented in Fig 2. From Fig 2, it is observed that the system is asymptotically stable.

The elementary reproduction number RN0 is procured and has been recognized as a threshold parameter. If RN0 < 1 >1, a distinct endemic equilibrium F* exists and is locally asymptotically stable. It indicates that the longer the exposure duration of the system, the less probability is that it will turn into endemic in the long period. Essential information about this model is that the most associated nodes are at maximum risk of an attack. The reproduction number is calculated from the model by utilizing the spectral radius of the generation matrix by translating it into the estimated threshold condition. The stability of the model is expressed on the basis of reproduction number.

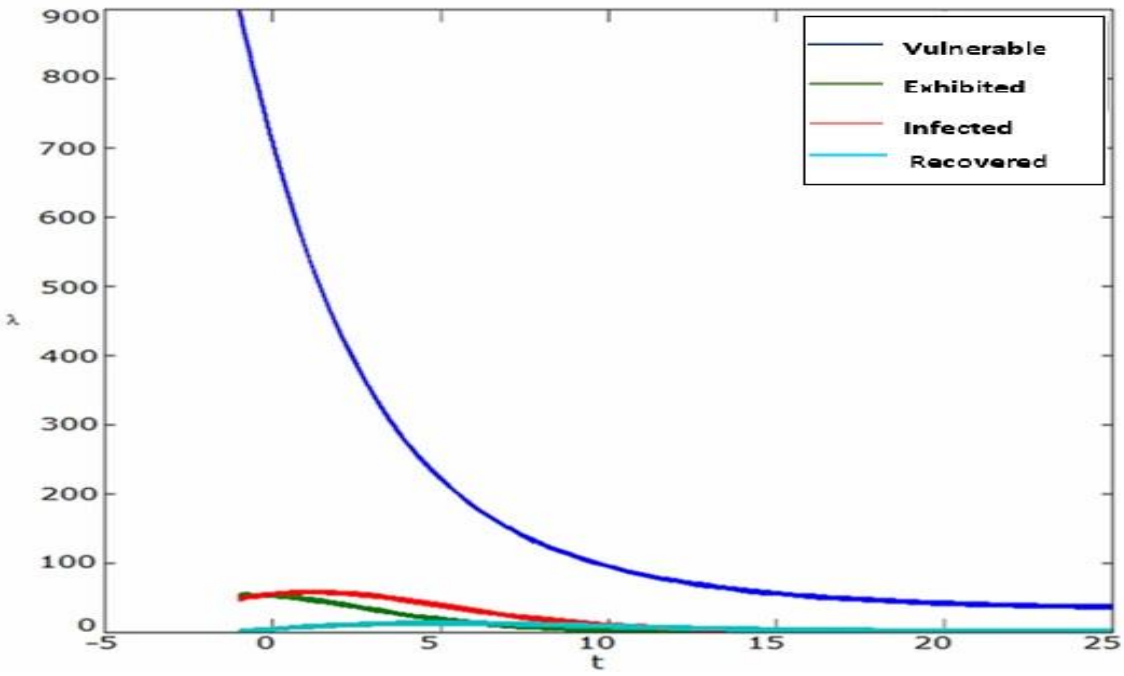

Figure 2: Presence of malicious object in computer network

VIII. CONCLUSION

On the basis of the suggested model, I have provided a general approach for immunity of the network. The suggested strategy can efficiently employ the consequence of locally disseminating awareness for the prevention of infection spreading across the network. It can be observed that in the conceptualization of the model, I have not presumed the immunity after the first infection of the machine and permitted the recovering machine to be vulnerable to future infections again. I stated that computer viruses can be nearly simulated biological viruses. The intercommunication between the parameters is examined and the possibility of the model is established by investigating their mathematical features. Worldwide stability of the endemic equilibrium for the epidemic prototype has been determined. Hence this model is a beneficial tool for controlling the propagation of computer viruses and helps to understand the dynamics of computer viruses.

REFERENCES

[1] Mishra, B. K., & Saini, D. K. (2007). SEIRS epidemic model with delay for transmission of malicious objects in computer network. Applied mathematics and computation, 188(2), 1476-1482.

[2] Mishra, B. K., & Nayak, P. K. (2009). Epidemic model for active infectious nodes in computer sub-networks. International Journal of Signal Control and Engineering Applications, 2, 56-60.

[3] Zhu, Q., Yang, X., Yang, L. X., & Zhang, X. (2013). A mixing propagation model of computer viruses and countermeasures. Nonlinear Dynamics, 73(3), 1433-1441.

[4] Zou, C. C., Gao, L., Gong, W., & Towsley, D. (2003, October). Monitoring and early warning for internet worms. In Proceedings of the 10th ACM conference on Computer and communications security (pp. 190-199).

[5] Kermack, W. O., & McKendrick, A. G. (1932). Contributions to the mathematical theory of epidemics. II.—The problem of endemicity. Proceedings of the Royal Society of London. Series A, containing papers of a mathematical and physical character, 138(834), 55-83.

[6] Kumar Nayak, P., Mishra, D., & Ram, S. (2016). Dynamic e-epidemic model for active infectious nodes in computer network. Journal of Statistics and Management Systems, 19(2), 247-257.

[7] Piqueira, J. R., Navarro, B. F., & Monteiro, L. H. A. (2005). Epidemiological models applied to viruses in computer networks. Journal of Computer Science, 1(1), 31-34.

[8] Mishra, B. K., & Saini, D. K. (2007). SEIRS epidemic model with delay for transmission of malicious objects in computer network. Applied mathematics and computation, 188(2), 1476-1482.

[9] Draief, M., Ganesh, A., & Massoulié, L. (2006, October). Thresholds for virus spread on networks. In Proceedings of the 1st international conference on Performance evaluation methodologies and tools (pp. 51-es).

[10] Gan, C., Yang, X., Zhu, Q., Jin, J., & He, L. (2013). The spread of computer virus under the effect of external computers. Nonlinear Dynamics, 73(3), 1615-1620.

[11] Thommes, R. W., & Coates, M. J. (2005, December). Modeling virus propagation in peer-to-peer networks. In 2005 5th International Conference on Information Communications & Signal Processing (pp. 981-985). IEEE.

[12] Fečkan, M. (2011). Chaos in Ordinary Differential Equations. In Bifurcation and Chaos in Discontinuous and Continuous Systems (pp. 87-165). Springer, Berlin, Heidelberg.

[13] Kephart, J. O., White, S. R., & Chess, D. M. (1993). Epidemiology of computer viruses. IEEE SPECTRUM, 30(5), 20-20.

[14] Chen, T. M., & Jamil, N. (2006, June). Effectiveness of quarantine in worm epidemics. In 2006 IEEE International Conference on Communications (Vol. 5, pp. 2142-2147). IEEE.

[15] Yang, L. X., Yang, X., Zhu, Q., & Wen, L. (2013). A computer virus model with graded cure rates. Nonlinear Analysis: Real World Applications, 14(1), 414-422.

[16] Yuan, H., & Chen, G. (2008). Network virus-epidemic model with the point-to-group information propagation. Applied Mathematics and Computation, 206(1), 357-367.

[17] Zhu, Q., Yang, X., Yang, L. X., & Zhang, C. (2012). Optimal control of computer virus under a delayed model. Applied Mathematics and Computation, 218(23), 11613-11619.

[18] Zhu, Q., Yang, X., Yang, L. X., & Zhang, X. (2013). A mixing propagation model of computer viruses and countermeasures. Nonlinear Dynamics, 73(3), 1433-1441.