ISSN 1749-3889 (print), 1749-3897 (online)
International Journal of Nonlinear Science
Vol.17(2014) No.2,pp.145-153

Mathematical Model on Attack by Malicious Objects Leading to Cyber War

Bimal Kumar Mishra *, Apeksha Prajapati
Department of Applied Mathematics, Birla Institute of Technology, Mesra, Ranchi, India - 835215
(Received 10 May 2012, accepted 10 April 2013)

Abstract: With an increasing global reliance on technology, from managing national electrical grids to ordering supplies for troops, the security of cyber world become an important issue worldwide. In this paper, an e-epidemic $SEI_1I_2R_1R_2$ (Susceptible-Exposed-Infectious class-1 (I_1) - Infectious class-2 (I_2) - Removed class (R_1) - Recovered class (R_2)) model for the transmission of malicious codes in a computer network is developed to have a better understanding of removed class on Cyber war. An analysis of the basic reproduction number has been made and the global stability of an attack-free state is established. Furthermore, initial simulation results show the system behavior, stability analysis for attack-free state, impact of removed class in the network for minimizing the infection and the positive impact of increasing security measures on malicious codes propagation in computer network. Efficiency of antivirus software and crashing of the nodes due to attack is critically analyzed. Cyber war against computer networks are an important research area because of the security strategies.

Keywords: Cyber war; Global stability; Epidemic Model; Virus; Computer network

1 Introduction

In today's world, the internet is considered to be one of the most useful tools for people to communicate, find information and to buy goods and services. Most computers are connected to each other in some way. They usually share the same operating system software and communicate with all other computers using the standard set of TCP/IP protocols. The major way of attack in cyber world, is cyber war. Cyber war is a form of war which takes places on computers and the Internet, through electronic means rather than physical ones. This has spawned a new generation of criminals. These cyber criminals develop programs or software called malicious codes that invades the government computers as well as personal computer and starts gathering information such as financial or personal details. The Internet is the primary medium used by attackers to commit computer crimes. Virus's attacks are considered by network experts the highest security risk on computer network. Computers virus are built to propagate without warning or user interaction, causing an increase in traffic service requests that will eventually lead to Cyber attack. With this paper, we discuss the attacking behavior of malicious objects that weakens the IT security infrastructure within organizations. With the rapid spread of Internet technologies and applications, the number of those seeking to break into the systems is also increasing - usually to gain fame, money, or to damage the target's reputation. The major attacks are the Denial of Service attack (DoS) and the distributed version (DDoS). This paper gives the idea about how these attacks work technically, and discuss ways to prevent them in the network. The fundamental technique behind a DoS attack is to make the target system busy. In a computer server, when a network packet is being received, all components (right from the network interface card or NIC to the application running under the OS) are participating to ensure successful delivery of that packet. The NIC must monitor the Ethernet frames meant for it, align data and pass it to the network card driver, which then adds its own intelligence and passes it to the OS, which takes it to the application. Each component involved can exhibit some form of vulnerability, and DoS attacks are devised to exploit one or more of these, to penetrate into the system. The TCP/IP protocol uses a handshake between the sender and the receiver. Figure 1 shows how a

*Corresponding author. *E-mail address*: drbimalmishra@gmail.com

IJNS.2014.04.15/797

healthy TCP handshake takes place, and how a SYN flood attack compares with it. When the sender wants to communicate, it sends a SYN packet with its own IP address as the source, and the receiver's IP address as the destination. The receiver responds with a SYN-ACK packet. The sender confirms this by sending an ACK packet. Now, sender and receiver have a guarantee that they can communicate with each other. The sender then starts sending the actual data in small chunks, and for each data packet received, the receiver sends an ACK back. When the sender sends the final data chunk, it sends a FIN signal, which is acknowledged by the receiver by sending a FIN-ACK back. If a particular port is not supposed to respond to the request, the receiver responds with an RST packet, which means it is rejecting that request. The TCP/IP stack software has to deal with complex communication, which does take some CPU and memory resources. Adding to this, many handshakes are happening on a server for different source and destination addresses and for various TCP ports. All IP-based protocols such as ICMP ping, telnet, FTP, etc, actually piggyback on this framework to do their job, each working on a different dedicated socket or port. At the application layers, the OS and the application receiving or transmitting data allocate internal memory buffers and a software process to keep track of what is being sent or received. The OS partially does this job itself, and leaves the rest to the network driver and protocol stack. Each process consumes some CPU time and memory resources. A DoS attack exploits this situation, by tweaking TCP packets to make the server respond to malicious, fabricated network requests. TCP packets can be forged, or modified to disrupt the basic handshake process, in order to create unexpected network responses. This ultimately results in exhausting all the server resources, which when overwhelmed, stops responding.

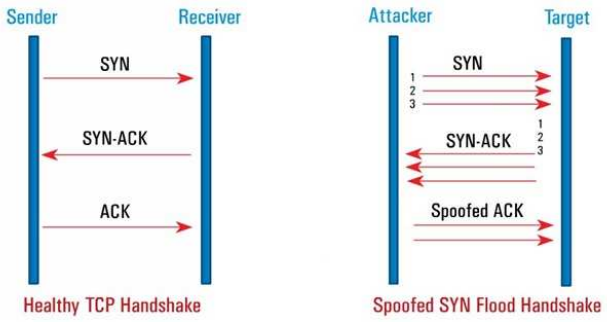

Figure 1: TCP Handshake and Spoofed SYN Handshake

The similarity between the spread of a biological virus and computer virus propagation encourages researchers to adopt an epidemic model to the network environment [1]. Recently, more research attention has been paid to the combination of virus propagation model and antivirus countermeasures to study the dominance of virus and worms, e.g., virus immunization [2] [3] [4]. Kshetri discussed the pattern of global cyber war, cyber crime and their way of attack [5]. Enough literature on the different models in epidemiology [6] [7] [8] is available which are used to develop e-epidemic models, starting with the work of Kermack and McKendrick classical epidemic model [9–11]. Forrest et al. developed mathematical models on the vaccinations of virus in email networks [12]. Epidemic models like SIS (Susceptible-Infectious-Susceptible)[13] and SEIRS (Susceptible-Exposed-Infectious-Recovered-Susceptible) [14] were developed to understand the spreading behavior of malicious objects in computer network. Dynamical models for the behavior of transmission of malicious objects and the effect of quarantine nodes in the computer network were developed depending on network parameters [15, 16]. Attention has also been paid to develop models on worm [17] and infection dynamics in the network [18]. A key concept in these studies is the basic reproduction number R_0 [14][19] which denotes the expected number of secondary infective caused by a single primary infective. The paper by Mishra and Pandey, describes an epidemic model susceptible - exposed - infectious - susceptible with vaccination (SEIS-V) of worms in a computer network. An explicit formula has been derived for reproductive number R_0. Analysis of efficient antivirus software is also performed [20]. Brautbar, Michael and Draief initiate the study of adversarial infection strategies. Necessary and sufficient conditions is also identified in terms of network structure and edge infection probabilities such that the adversarial process can infect more nodes than the stochastic process [21]. Propagation modeling of worms has become an attractive research field in recent years since it facilitates worm prediction, detection, analysis and prevention etc. Chen et al.

proposed a novel ternary-matrix-based model to describe the propagation trend of active P2P worms. This model can adapt to different scenes by changing the related parameters, particularly this model is general for different kinds of time lags and P2P topologies [22]. In this paper, Fan et al. proposed a virus model based on the application platform of Facebook which describes virus propagation through emails and compare the behaviors of virus spreading in Facebook and email network [23]. Presently, P2P worm poses a serious threat to the Internet infrastructure. As it spreads extremely fast and is hard to be detected in early stage. Chen et al. proposed a Four-factors Propagation Model (FPM) for passive P2P worms. This paper describes four critical factors-addresses hiding, configuration diversity, online/offline behaviors and download duration into consideration. It also gives an idea about the differential equations of FPM [24]. In this paper, Wang et al. studied MMS viruses and its spreading behavior. The results also show that at given sufficient time, sophisticated viruses may infect a large fraction of susceptible phones without being detected and it also describes the way of better understanding on how one could prevent the spread of mobile-phone viruses [25].

2 The Epidemic Model

We assume the network being divided into different sub networks and the total nodes (N) in the network are susceptible towards the attack by cyber criminals. The attacker attacks the n (n<N) number of nodes in the sub network making them highly infectious and the users are unable to open a specific website. These n numbers of nodes are placed in infectious class I_1. We also assume that when the infectious nodes are flooding the most and the effect of antivirus software is almost negligible in that same node, they are permanently removed from the network say k (<n) as their recovery is feeble. The remaining (n-k) infectious nodes are capable enough to transmit the virus to the nodes of another sub network making the proportion of nodes infectious and we say it I_2 class. Antivirus software is run at specific time interval to recover the nodes in I_2 class. We assume the crashing of nodes due to hardware/software termed as natural death and attack of malicious objects termed as death due to attack. A simple classical epidemic malicious objects transmission model on cyber war illustrates the dynamics of direct transmission of malicious codes among susceptible, exposed, infected class-1, infected class-2, removed class and recovered class in the computer network. I_1 and I_2 represent the Infectious class-1 and infectious class-2 respectively. R_1 and R_2 denote the Removed class and Recovered class respectively. Nodes are removed permanently from Infectious class-1 to minimize the infection in the network. b is the inclusion rate of new nodes for susceptible class . μ is the death rate due to attack, δ is the natural crashing rate of the nodes in the network, β is infectivity contact rate, τ is the infectious rate in exposed class, ρ is the infectious rate in infectious class-1, α is the removal rate in infectious class-1 and γ is the recovery rate in infectious class-2. The system of differential equation illustrates the rate of change of different classes which is depicted in figure 2 is given as.

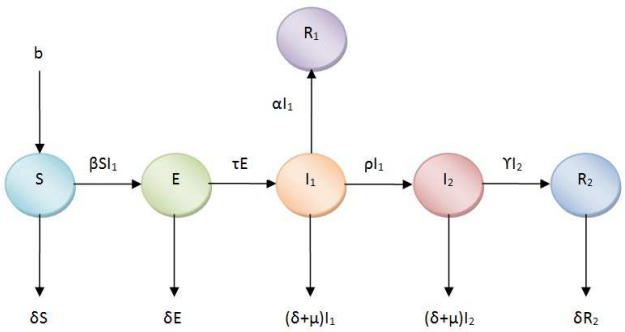

Figure 2: Schematic diagram for the flow of malicious objects in computer network

$$\begin{aligned}
\frac{dS}{dt} &= b - \beta S I_1 - \delta S \\
\frac{dE}{dt} &= \beta S I_1 - (\tau + \delta) E \\
\frac{dI_1}{dt} &= \tau E - (\rho + \mu + \delta + \alpha) I_1 \\
\frac{dI_2}{dt} &= \rho I_1 - (\delta + \mu + \gamma) I_2 \\
\frac{dR_1}{dt} &= \alpha I_1 \\
\frac{dR_2}{dt} &= \gamma I_2 - \delta R_2
\end{aligned} \tag{1}$$

3 The reproduction number and equilibrium points

The basic reproduction number can be obtained by calculating V and F, where V and F are given as

$$V = \begin{pmatrix} \delta + \tau & 0 & 0 \\ -\tau & \delta + \mu + \rho + \alpha & 0 \\ 0 & -\rho & \delta + \mu + \gamma \end{pmatrix}, F = \begin{pmatrix} 0 & \beta & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

The basic reproduction number is defined as the dominant Eigen value of FV^{-1}

$$R_0 = \frac{\tau\beta}{(\delta+\tau)(\delta+\mu+\alpha+\rho)}$$

The first four equations of (1) are independent of $R_1$and R_2 so we can consider the reduced model as

$$\begin{aligned}
\frac{dS}{dt} &= b - \beta S I_1 - \delta S \\
\frac{dE}{dt} &= \beta S I_1 - (\tau + \delta) E \\
\frac{dI_1}{dt} &= \beta S I_1 - (\mu + \rho + \delta + \alpha) I_1 \\
\frac{dI_2}{dt} &= \rho I_1 - (\delta + \mu + \gamma) I_2
\end{aligned} \tag{2}$$

For equilibrium points we must have

$$\tfrac{dS}{dt} = 0; \tfrac{dE}{dt} = 0; \tfrac{dI_1}{dt} = 0; \tfrac{dI_2}{dt} = 0$$

System (2) has attack-free equilibrium point $E_0 = (\frac{b}{\delta}, 0, 0, 0)$ and endemic equilibrium at

$$E^* = \begin{pmatrix} \frac{1}{R_0} & \frac{(bR_0-\delta)}{R_0(\delta+\tau)} & \frac{(bR_0-\delta)}{\beta} & \frac{\rho}{\delta+\mu+\gamma} \end{pmatrix}$$

4 Global stability of the attack-free equilibrium point

Lemma 1 *Assume that a bounded real valued function $f : [0, \infty) \to R$ be twice differentiable with bounded second derivative. Let $k \to \infty$ and $f(t_k)$ converges to f^∞ or f_∞ then $\lim_{t\to\infty} f'(t_k) = 0$, where $f_\infty = \lim_{t\to\infty} inf_{\theta\geq t} f(\theta)$, $f^\infty = \lim_{t\to\infty} \sup_{\theta\geq t} f(\theta)$.*

Theorem 2 *If $R_0 < 1$ then the attack - free equilibrium is globally asymptotically stable.*

Proof. Jacobian matrix of the system (2)

$$J = \begin{pmatrix} \beta I_1 - \delta & 0 & -\beta S & 0 \\ \beta I_1 & -\delta - \tau & -\beta S & 0 \\ 0 & -\tau & -\delta - \mu - \rho - \alpha & 0 \\ 0 & 0 & \rho & -\delta - \mu - \gamma \end{pmatrix}$$

Jacobian of the system (2) for attack free state is given as

$$J = \begin{pmatrix} -\delta & 0 & 0 & 0 \\ 0 & -\delta - \tau & 0 & 0 \\ 0 & -\tau & -\delta - \mu - \rho - \alpha & 0 \\ 0 & 0 & \rho & -\delta - \mu - \gamma \end{pmatrix}$$

Eigen values are $-\delta, -\delta - \tau, -\delta - \mu - \rho - \alpha, -\delta - \mu - \gamma$.

From the first equation of system (2) we have

$$\frac{dS}{dt} < b - \delta S$$

A solution of the equation

$$\frac{dX}{dt} = b - \delta X$$

is super solution of $S(t)$. Since $X \to \frac{b}{\delta}$ as $t \to \infty$, then for a given $\epsilon > 0$ there exists a t_0 such that Thus $S^{\infty} \leq X(t) \leq (\frac{b}{\delta} + \epsilon)$ for all $t > t_0$ $\epsilon \to \infty$ then $S^{\infty} \leq \frac{b}{\delta}$

Second equation of (2) reduces to

$$\frac{dE}{dt} = \beta I_1 (\frac{b}{\delta} + \epsilon) - (\delta + \tau) E \tag{3}$$

Now taking third and fourth equation of (2) with (3)

$$\begin{pmatrix} \dot{E} \\ \dot{I_1} \\ \dot{I_2} \end{pmatrix} \leq P \begin{pmatrix} E \\ I_1 \\ I_2 \end{pmatrix} \tag{4}$$

where $P = \begin{pmatrix} -(\delta + \tau) & (\frac{b}{\delta} + 1) & 0 \\ \tau & (-\delta + \mu + \rho + \alpha) & 0 \\ 0 & \rho & (\delta + \mu + \gamma) \end{pmatrix}$, $M \in R^+$, such that $M \geq \max\{(\delta - \tau), (\delta - \mu - \rho - \alpha), (\delta + \mu + \gamma)\}$. Thus $P + MI_{3\times 3}$ is a strictly positive matrix if $\omega_1, \omega_2, \omega_3$ are the eigen values of P then $\omega_1 + M, \omega_2 + M, \omega_3 + M$ are eigen value of $P + MI_{3\times 3}$. Thus from Perron-Frobenius theorem ,[26] $P + MI_{3\times 3}$ has a simple positive eigen value equal to dominant eigen value and corresponding eigen vector $e > 0$, which implies that $\omega_1, \omega_2, \omega_3$ are real . If $\omega_1 + M$ is the dominant eigen value of $P + MI_{3\times 3}$, then $\omega_1 > \omega_2$ and $eP = e^{\omega_1}$. Obviously ω_2, ω_3 are the roots of the equation.

$$\lambda^2 + (2\delta + \mu + \tau + \alpha + \rho)\lambda + (\delta + \tau)(\mu + \rho + \delta + \alpha) - (\frac{b}{\delta} + \epsilon)\beta\tau = 0 \tag{5}$$

Since $R_0 < 1$ for $\epsilon > 0$, sufficiently small, we have

$$(\delta + \tau)(\mu + \rho + \delta + \alpha) - (\tfrac{b}{\delta} + \epsilon)\beta\tau > 0$$

Therefore, the coefficients of the quadratic equation (5) are positive. Thus $\omega_1, \omega_2, \omega_3$ all are negative, from equation (4), for $t \geq t_0$, $\frac{d}{dt}(e(E(t), I_1, I_2)) \leq \omega_1(e(E(t), I_1, I_2))$.

Integrating above equation we have $0 \leq e(E(t), I_1, I_2) \leq e(E(t), I_1, I_2)e^{(t-t_1)\omega_1}$ for $t \geq t_1 \geq t_0$.

Since $\omega_1 < 0, e(E(t), I_1, I_2) \to 0$ as $t \to \infty$. Using $e > 0$, we have $E(t), I_1, I_2 \to (0, 0, 0)$ as $t \to \infty$. By Lemma 1 we choose a sequence$t_n \to \infty, S_n \to 0(n \to \infty)$ such that $S(S_n) \to S^{\infty}$ $S(t_n) \to S_{\infty}$, $\dot{S}(S_n) \to 0$ and $\dot{S}(t_n) \to 0$. Since,$E(t), I_1, I_2 \to 0$ for $t \to \infty$
Thus from the first equation of (2) we have $\lim_{n\to\infty} S(t) = \frac{b}{\delta}$.
Hence, by incorporating lemma 1, the attack-free equilibrium E_0, is globally asymptotically stable, if $R_0 < 1$.
■

5 Relevance of the Developed Mathematical Model in Real Network

Cyber war against computer networks are an important research area because of the security strategies. In particular, an understanding of malicious objects transmission in a cyber war scenario allows us to improve predictions of the distribution of infection and the early growth of infection (attack). The relationship between epidemiology and virus transmission in computer networks goes further; because the knowledge of model can be used as part of cyber defense. The study of computer malicious objects propagation in computer network and how they relate to the propagation of infection in a computer network is an essential tool to understanding malware spread and, therefore, can be used to develop better preventive tools. For example, we can predict the impact of malicious objects attack in a computer network which may lead to cyber war and thus maintaining the various parameters we can reduce the spread of malicious objects.

6 Conclusion

In this paper we propose a malicious codes propagation model an $e - SEI_1I_2R_1R_2$ epidemic model taking consideration of removed class in a computer network. Our main contribution thus involves local and global stability of attack free equilibrium state. The initial parameter values (Table 1) were chosen to suit a real cyber war scenario. Runge-Kutta Fehlberg method of order 4 and 5 were employed to solve and simulate the system of equations (1). The behavior of the system with respect to time is analyzed which can be observed from figure 3. From figure 4, we observe the behavior of the infectious class-1 with respect to time for different parameters. Figure 5-8, shows the global stability of the attack free state of the system for different parameters. The behavior of Recovered class with time is also observed from figure 9 for different parameters. The rate of recovery is very high when updated version of antivirus software is run into the nodes. So we recommend the software organization to maintain these parameters for antivirus software. Figure 10, shows the deviation of removed class with time. It has been shown that as the number of secondary infection which arises from primary infection is greater than one, then epidemic starts (that is, attack were able to pervade), and the attack endemic would die out when $R_0 < 1$.

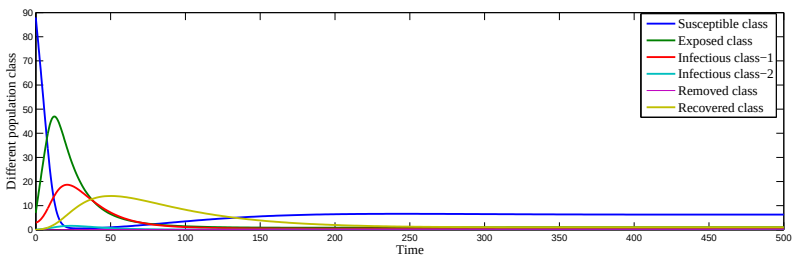

Figure 3: Dynamical behavior of the system with respect to time; where $\alpha = 0.002; \beta = 0.02; \gamma = 0.4; \delta = 0.02; b = 0.2, \mu = 0.03; \rho = 0.04; \tau = 0.02$

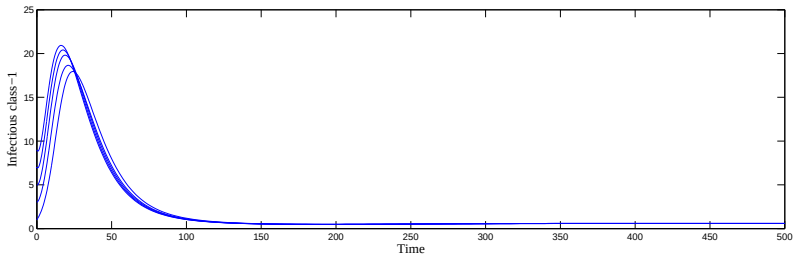

Figure 4: Dynamical behavior of the Infectious class-1 with respect to time; where $\alpha = 0.002, 0.045, 0.025; \beta = 0.02; \gamma = 0.4, 0.35, 0.25; \delta = 0.02; \mu = 0.03; \rho = 0.04, 0.03; \tau = 0.02, 0.035, 0.04; b = 0.2$

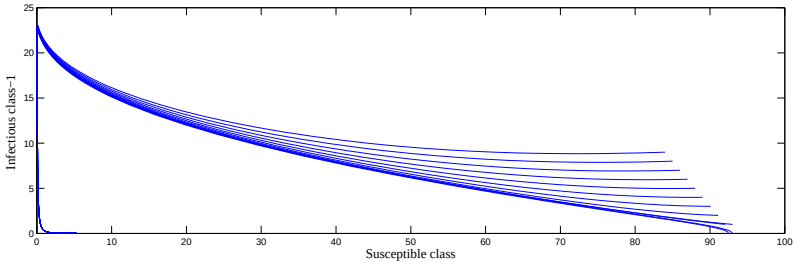

Figure 5: Dynamical behavior of the Susceptible class with respect to Infectious class-1; where $\alpha = 0.002, 0.045, 0.025; \beta = 0.02; \gamma = 0.4, 0.35, 0.25; \delta = 0.01; \mu = 0.03; \rho = 0.04, 0.03; \tau = 0.02, 0.035, 0.04; b = 0.05; E_0 = (\frac{b}{\delta}, 0, 0, 0) = (5, 0)$

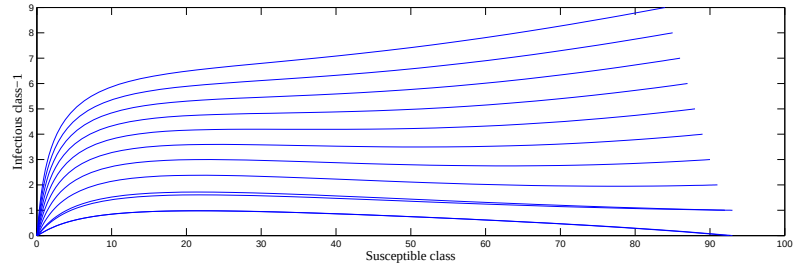

Figure 6: Dynamical behavior of the Susceptible class with respect to Infectious class-1; where $\alpha = 0.002; 0.045\beta = 0.02; \gamma = 0.4; \delta = 0.2; \mu = 0.03; \rho = 0.04, 0.03; \tau = 0.02; b = 0.02; E_0 = (.2, 0)$

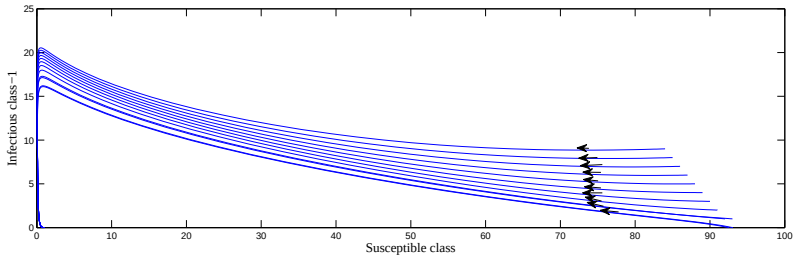

Figure 7: Dynamical behavior of the Susceptible class with respect to Infection class-1; where $\alpha = 0.002, 0.045, 0.025; \beta = 0.02; \gamma = 0.4, 0.35, 0.25; \delta = 0.05; \mu = 0.03; \rho = 0.04, 0.03; \tau = 0.02, 0.035, 0.04; b = 0.05; E_0 = (1, 0)$

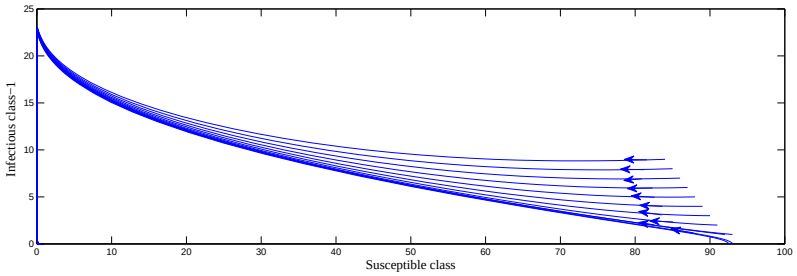

Figure 8: Dynamical behavior of the Susceptible class with respect to Infection class-1; where $\alpha = 0.002, 0.045, 0.025; \beta = 0.02; \gamma = 0.4, 0.35, 0.25; \delta = 0.1; \mu = 0.03; \rho = 0.04, 0.03; \tau = 0.02, 0.035, 0.04; b = 0.01; E_0 = (0.1, 0)$

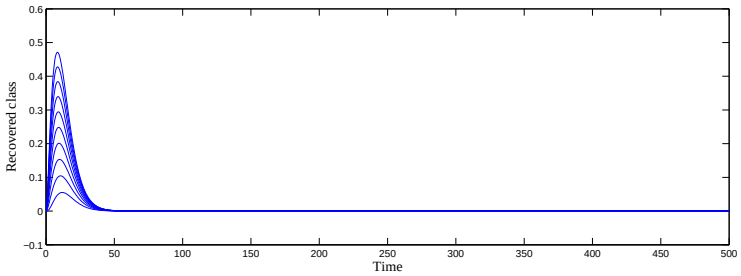

Figure 9: Dynamical behavior of the Recovered class with respect to time; where $\alpha = 0.002, 0.045, 0.025; \beta = 0.02; \gamma = 0.4, 0.35, 0.25; \delta = .02; \mu = 0.03; \rho = 0.04, 0.03; \tau = 0.02, 0.035, 0.04; b = 0.2$

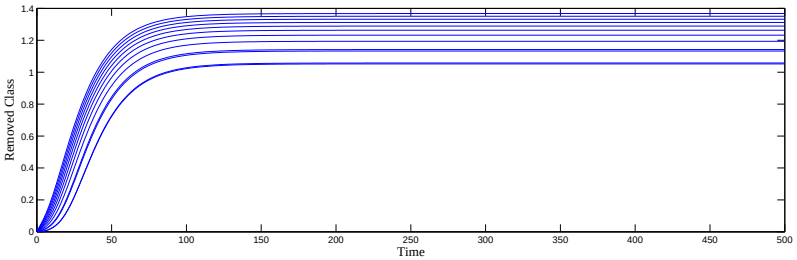

Figure 10: Dynamical behavior of the Removed class with respect to time; where $\alpha = 0.002, 0.045, 0.025; \beta = 0.02; \gamma = 0.4, 0.35, 0.25; \delta = 0.02; \mu = 0.03; \rho = 0.04, 0.03; \tau = 0.035, 0.04; b = 0.2$

Table 1: Initial values

Notation	values
$S(0)$	95
$E(0)$	3
$I_1(0)$	2
$I_2(0)$	0
$R_1(0)$	0
$R_2(0)$	0
α	0.002, 0.045, 0.025
β	0.02
γ	0.4, 0.35, 0.25
δ	0.02
μ	0.03
ρ	0.04, 0.03
τ	0.02, 0.035, 0.04
b	0.2

References

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

[2] B. K. Mishra , N. Jha. Fixed period of temporary immunity after run of anti-malicious software on computer nodes. *Applied Mathematics and Computation*, 190(2)(2007):1207-1212.

[3] J. O. Kephart. A biologically inspired immune system for computers. *In Artificial Life IV: proceedings of the fourth international workshop on the synthesis and simulation of living systems*, (1994):130-139.

[4] S. Data,H. Wang. The effectiveness of vaccinations on the spread of email-borne computer viruses. *In Electrical and Computer Engineering ,Canadian Conference on IEEE*, (2005):219-223.

[5] N. Kshetri. Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*, 11(4)(2005):541-562.

[6] J. O. Kephart, S. R. White , D. M. Chess. Computers and epidemiology. *Spectrum, IEEE*, 5(30)(1993):20-26.

[7] J. R. C. Piqueira , V. O. Araujo. A modified epidemiological model for computer viruses. *Applied Mathematics and Computation*, 213(2)(2009):355-360.

[8] G. Li , J. Zhen. Global stability of an sei epidemic model with general contact rate. *Chaos, Solitons & Fractals*, 23(3)(2005):997-1004.

[9] W. Kermack , A. McKendrick. Contributions to the mathematical theory of epidemics i. *Proceedings of the Royal Society of London. Series A*,115(1927):700-721.

[10] W. O. Kermack , A. G. McKendrick. Contributions to the mathematical theory of epidemics. ii. the problem of endemicity. *Proceedings of the Royal society of London. Series A*,138(834)(1932):55-83.

[11] W. Kermack , A. McKendrick. Contributions to the mathematical theory of epidemics .iii. further studies of the problem of endemicity. *Proceedings of the Royal Society of London. Series A*, 141(843)(1933):94-122.

[12] M. E. Newman, S. Forrest , J. Balthrop. Email networks and the spread of computer viruses. *Physical Review E*, 66(3)(2002):035101.

[13] J. Kim, S. Radhakrishnan , J. Jang. Cost optimization in sis model of worm infection. *ETRI journal*, 28(5)(2006):692-695.

[14] B. K. Mishra , N. Jha. Seiqrs model for the transmission of malicious objects in computer network. *Applied Mathematical Modelling*, 34(3)(2010):710-715.

[15] T. M. Chen , N. Jamil. Effectiveness of quarantine in worm epidemics. *Cost optimization in sis model of worm infectionIn Communications, ICC'06. IEEE* ,5(2006)2142-2147.

[16] X. Han , Q. Tan. Dynamical behavior of computer virus on internet. *Applied Mathematics and Computation*, 217(6)(2010):2520-2526.

[17] C. C. Zou, W. Gong , D. Towsley. Worm propagation modeling and analysis under dynamic quarantine defense. *In Proceedings of the 2003 ACM workshop on Rapid malcode*,(2003):51-60.

[18] R. M. May , A. L. Lloyd. Infection dynamics on scale-free networks. *Physical Review E*, 64(6)(2001):066112.

[19] M. Draief, A. Ganesh , L. Massoulié. Thresholds for virus spread on networks. *In Proceedings of the 1st international conference on Performance evaluation methodolgies and tools*,(51)2006.

[20] B. K. Mishra , S. K. Pandey. Dynamic model of worm propagation in computer network. *Applied Mathematical Modelling*, 2013.

[21] M. Brautbar, M. Draief , S. Khanna. On the power of adversarial infections in networks. *In Algorithms and Models for the Web Graph,Springer*, (2013):44-55.

[22] T. Chen . Propagation modeling of active p2p worms based on ternary matrix. *Journal of Network and Computer Applications*, 2013.

[23] W. Fan , K.-H. Yeung. Virus propagation modeling in facebook. *In The Influence of Technology on Social Network Analysis and Mining,Springer*, (2013):185-199.

[24] T. Chen, X.-s. Zhang , Y. Wu. Fpm: Four-factors propagation model for passive p2p worms. *Future Generation Computer Systems*, 2013.

[25] P.Wang . Understanding the spread of malicious mobile-phone programs and their damage potential. *International Journal of Information Security*, (2013):1-10.

[26] J. K. Hale.Ordinary Differential Equations. *Robert E. Krieger Publishing , Huntington, Beijing*,1980.