Available at
http://pvamu.edu/aam
Appl. Appl. Math.
ISSN: 1932-9466

Applications and Applied Mathematics:
An International Journal
(AAM)

Vol. 8, Issue 2 (December 2013), pp. 684 – 700

Spread of Malicious Objects in Computer Network: A Fuzzy Approach

Bimal Kumar Mishra and Apeksha Prajapati
Department of Applied Mathematics
Birla Institute of Technology
Mesra, Ranchi, India – 835 215
drbimalmishra@gmail.com, prajapatiapeksha@gmail.com

Received: October 5, 2011; Accepted: February 12, 2013

Abstract

We propose an e-epidemic fuzzy SEIQRS (Susceptible-Exposed-Infectious-Quarantine-Recovered-Susceptible) model for the transmission of malicious codes in a computer network. We have simulated the result for various parameters and analyzed the stability of the model. The efficiency of antivirus software and crashing of the nodes due to attack of malicious code is analyzed. Furthermore, initial simulation results illustrate the behavior of different classes for minimizing the infection in a computer network. It also reflects the positive impact of anti-virus software on malicious code propagation in a computer network. The basic reproduction number R_0^f and its formulation is also discussed.

Keywords: Fuzzy Mathematics; Global stability; Epidemic Model; Malicious code; Fuzzy Basic Reproduction number

AMS-MSC 2010 No: 92D30, 34A07, 34D23

1. Introduction

There is no doubt that the Internet is a wondrous creation. The entire world is rapidly becoming obsessed with it. 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. Everywhere we look we are bound to see something related to the Internet. The Internet is indeed spectacular but as the saying goes, "Behind every silver lining there is a cloud". There are several problems associated

with the Internet. All financial dealings are made over the Internet. It is estimated that billions or even trillions of dollars are being exchanged online every day. This has spawned a new generation of criminals. These cyber criminals develop programs or software called malicious codes that invade our personal computers and start gathering information such as our financial or personal details. We can stop these crimes from happening by simply installing the best Internet security software available.

Epidemic systems in particular, those dealing with infectious diseases, have strong non-linearities and should be treated in a different way. These non-linearities are due to the fact that the force of epidemic of an infectious agent, among other things, depends on the fraction of susceptible nodes and fraction of infectious nodes. Both susceptibility and infectiousness are intrinsically fuzzy concepts as suggested by Mishra and Pandey (2010) and therefore, ideal subjects for fuzzy logic analysis. The mathematical models of transmission of malicious object in a computer network are always subject to inaccuracies related to the nature of the state variables involved, parameters and initial conditions.

In this paper we extend the SIRS model studied by Mishra and Pandey (2010), by introducing two new compartments, viz. Exposed and Quarantine classes and analyze the effect. In this model we have used fuzzy logic, which helps us to explain the transmission of malicious code more accurately. Recently, more research attention has been paid towards modeling the combined propagation of malicious codes and also anti-virus countermeasures to control the dominance of malicious codes. Examples include virus immunization studied by Mishra and Jha (2007), Pastor-Satorras and Vespignani (2002), Kephart (1995) and quarantine as a control measure which has been dealt by Mishra et al. (2009), Chen and Jamil (2006) and also by Kephart et al. (1993).

More work has also been done on the spread and vaccination of virus in email networks by Han and Tan (2010), Newman et al. (2002) and by Datta and Wang (2005) as well. Thresholds for virus propagation in the network have also been calculated, for instance by Draief et al. (2008).

There is an ample amount of literature on different models in epidemiology including the work of Kephart et al. (1993), Keeling and Eames (2005), Li and Zhen (2004) and Kermack and McKendrick (1927). Most of these models use the work of Kermack and McKendrick (1927, 1932, 1933) as basis where they studied the SIR classical epidemic model.

The similarity between the spread of a biological virus and malicious code propagation encourages researchers to adopt epidemic models like SIS (Susceptible-Infectious-Susceptible), SEIRS (Susceptible-Exposed-Infectious-Recovered-Susceptible), SEIQRS (Susceptible-Exposed-Infectious-Quarantined-Recovered-Susceptible) and SEIQAmS (Susceptible-Exposed-Infectious-Quarantined-Anti Malicious Software treated-Susceptible) in modeling computer viruses and worms, as has been done by Mishra and Jha (2010), Mishra and Saini (2007), Han and Tan (2010), Kim et al. (2006), Picqueria (2009), Williamson and Laeveillae (2003) and Jones (2007).

Dynamical models for malicious objects propagation were proposed, providing estimations for temporal evolutions of nodes depending on network parameters by May and Lloyd (2001) and

later by Zou et al. (2003). A key concept in almost all of these studies is the basic reproduction number R_0, which has been elaborately discussed by Mishra and Jha (2007, 2010) and also by Mishra and Saini (2007). It basically denotes the expected number of secondary infections caused by a single primary infective. If $R_0 > 1$, the infection spreads to some sizeable fraction of the entire population and if $R_0 < 1$, then the infection eventually becomes zero.

2. Formulation of Fuzzy SEIQRS Model

2.1. The Simple SEIQRS Model

A simple classical e-epidemic SEIQRS model illustrates the dynamics of direct transmission of malicious codes among susceptible, exposed, infected, quarantined and recovered classes of nodes in the computer network. We have assumed that there is neither vital dynamics nor crashing of nodes due to other reason in the network. The flow of malicious codes in a computer network is depicted in Figure 1.

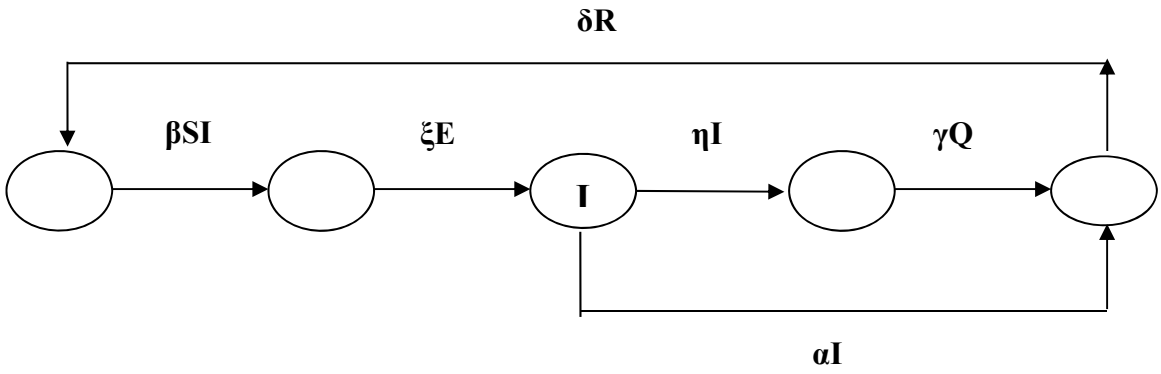

Figure 1. The flow of malicious codes in different classes in a computer network

The system of ordinary differential equations representing this model is given as follows:

$$\left.\begin{aligned} \frac{dS}{dt} &= -\beta SI + \delta R, \\ \frac{dE}{dt} &= \beta SI - \xi E, \\ \frac{dI}{dt} &= \xi E - (\eta + \alpha) I, \\ \frac{dQ}{dt} &= \eta I - \gamma Q, \\ \frac{dR}{dt} &= \gamma Q + \alpha I - \delta R, \end{aligned}\right\} \qquad \text{(A)}$$

where

$$S + E + I + Q + R = 1.$$

In this model constant population is divided into different classes based on the status of nodes. *S* is the class of proportional susceptible nodes. *E* is the class of proportional exposed nodes, which contains those nodes that are infectious but are still not able to transmit malicious codes to other nodes. *I* is the class of proportional infectious nodes while *Q* is the class of proportional quarantined nodes. The nodes which are highly infectious are quarantined from the network. *R* is the class of proportional recovered nodes. β is the infectivity contact rate, ξ is the rate at which exposed population becomes infectious, γ is the recovery rate in quarantine class, α is the recovery rate in infectious class, η is the rate of quarantine and δ is the rate of loss of immunity of the nodes. We now consider an expansion of the SEIQRS dynamic model incorporating heterogeneities, taking into account that nodes with different amount of malicious code contribute differently to the malicious code transmission.

2.2. The Fuzzy SEIQRS Model

All concepts of susceptibility, exposed, infectivity, quarantine and recovery are uncertain in the sense that there are different degrees in susceptibility, exposed, infectivity, quarantine and recovery among the nodes in a computer network. Such difference can arise, for example, when we consider nodes in a computer network with their different degrees of resistance to an attack. In this way, we could think of more realistic models which consider these different degrees of susceptibility, exposed, infectivity, quarantine and recovery of the nodes. Focusing on incorporating the population heterogeneity in the model, we consider the epidemic parameters as fuzzy numbers.

To convert a simple SEIQRS model into fuzzy SEIQRS model, we assume that the population heterogeneity is given by the infected node's malicious code load or intensity of malicious code. Thus, the higher the malicious code load, the higher will be the chance of its transmission. So, we assume $\beta = \beta(x)$ to be the chance of malicious code transmission between a susceptible and exposed node with an amount of malicious code x. Here, it may be possible that some values of β are more possible than others and that turns β into a membership function of a fuzzy number. Then to get the membership function β, we suppose that when the amount of malicious code in a node is relatively low, the chance of its transmission is negligible and then there is a minimum amount of malicious code x_{min} for the transmission. Now, for some amount of malicious code x_M, the chance of transmission is maximum and equal to one. However, we assume that the amount of malicious code in a node is always limited by x_{max} based on the assumption of Mishra and Pandey (2010). Hence, we define the membership function β (x) (depicted in Figure 2) as,

$$\beta(x) = \begin{cases} 0, & x < x_{min,} \\ \frac{x - x_{min}}{x_M - x_{min}}, & x_{min} < x < x_{M,} \\ 1, & x_M < x < x_{max}. \end{cases}$$

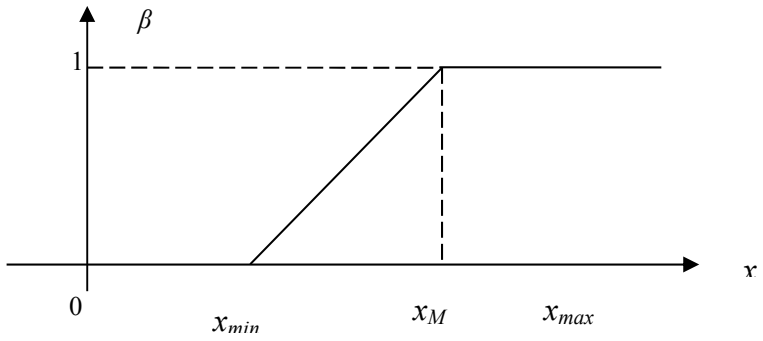

Figure 2. Fuzzy coefficient of malicious code transmission $\beta = \beta(x)$

The infectious rate $\xi = \xi(x)$ is also a function of malicious code load x. Moreover, it is an increasing function of x because higher the exposed nodes in the network, higher will be the chance of infection. So, the function $\xi(x)$ can be defined as follows (depicted in Figure 3):

$$\xi(x) = \frac{1-\xi_0}{x_{max}} x + \xi_0,$$

where $\xi_0 > 0$ is the lowest exposed rate.

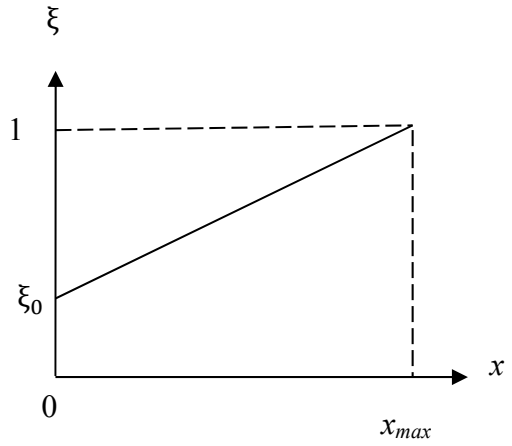

Figure 3. Fuzzy coefficient of exposed class ξ = ξ(x)

The node's quarantine rate $\eta = \eta(x)$ is also a function of malicious code load x. The nodes which transmit malicious codes most are more likely to be quarantined and so η is an increasing function of x. It may be defined as follows (depicted in Figure 4):

$$\eta(x) = \frac{1-\eta_0}{x_{max}} x + \eta_0,$$

where $\eta_0 > 0$ is the lowest Quarantine rate.

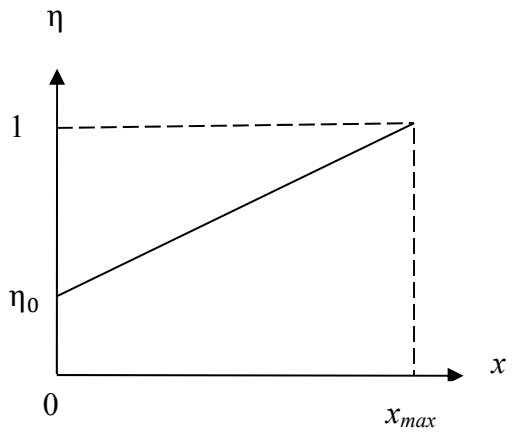

Figure 4. Fuzzy coefficient of infection $\eta = \eta(x)$

The recovery rate from infectious class $\alpha = \alpha(x)$ is also a function of malicious code load *x*. Higher the infection in the nodes, the chance of recovery will be less. So, α is a decreasing function of *x* as defined below (depicted in Figure 5):

$$\alpha(x) = \frac{\alpha_0 - 1}{x_{max}} x + 1,$$

where $\alpha_0 > 0$ is the lowest recovery rate in infectious class.

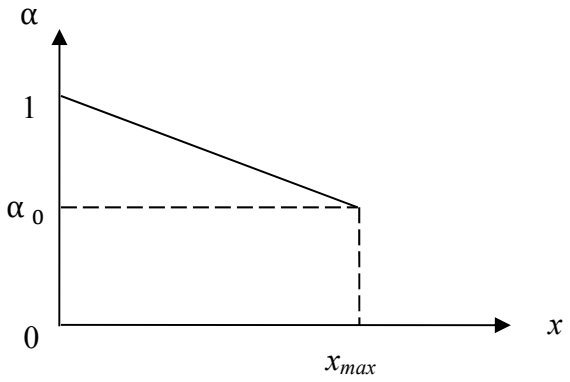

Figure 5. Fuzzy recovery rate in Infectious class $\alpha = \alpha(x)$

The node's recovery rate $\gamma = \gamma(x)$ from the quarantined class is function of malicious code load *x*. Higher the quarantined nodes in the network, higher will be the chance of recovery. So, γ is an increasing function of *x* and which may be defined as follows (depicted in Figure 6):

$$\gamma(x) = \frac{1-\gamma_0}{x_{max}} x + \gamma_0,$$

where $\gamma_0 > 0$ is the lowest recovery rate in quarantine class.

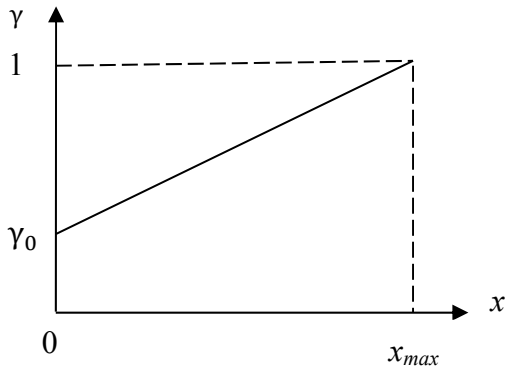

Figure 6. Fuzzy recovery rate in Quarantined class η = η(x)

The recovered node's loss of immunity rate $\delta = \delta(x)$ is also a function of malicious code load *x*. Higher the recovered nodes in the network, higher will be the chance to become susceptible. So, δ is increasing function of *x*, which may be defined as follows and it is depicted in Figure 7.

$$\delta(x) = \frac{1-\delta_0}{x_{max}} x + \delta_0,$$

where $\delta_0 > 0$ is the lowest susceptible rate.

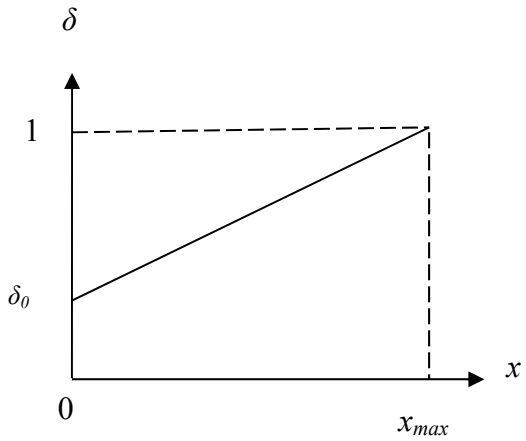

Figure 7. Fuzzy rate of loss of immunity $\delta = \delta(x)$

3. Solution and Equilibrium Points

Equilibrium points are the points where the variables do not change with time. In order to know about the evolution of infected nodes we study the stability of equilibrium points.
System of equations (A) reduces to

$$\left.\begin{aligned}\frac{dS}{dt} &= -\beta SI + \delta\big(1-(S+E+I+Q)\big),\\ \frac{dE}{dt} &= \beta SI - \xi E,\\ \frac{dI}{dt} &= \xi E - (\eta+\alpha)I,\\ \frac{dQ}{dt} &= \eta I - \gamma Q.\end{aligned}\right\} \quad \text{(B)}$$

For equilibrium points we have

$$\frac{dS}{dt}=0,\ \frac{dE}{dt}=0,\ \frac{dI}{dt}=0,\ \frac{dQ}{dt}=0.$$

Then, straightforward calculations show that the Endemic Equilibrium point is

$$(S^*,E^*,I^*,Q^*)=\left(\frac{\eta+\alpha}{\beta},\frac{(\eta+\alpha)\gamma\delta}{\beta}\frac{p}{q},\frac{\gamma\xi\delta p}{\beta q},\frac{\eta\xi\delta p}{\beta q}\right),$$

where

$$p=\beta-(\eta+\alpha)$$

and

$$q=(\eta+\alpha)(\gamma\delta+\xi\gamma)+\xi\delta(\gamma+\eta).$$

Malicious code free equilibrium point is $(\delta,0,0,0)$.

Now, by using fuzziness, i.e., by considering

$$\alpha=\alpha(x),\ \beta=\beta(x),\ \gamma=\gamma(x),\ \xi=\xi(x),\ \eta=\eta(x) \text{ and } \delta=\delta(x),$$

we have endemic equilibrium at

$$\left(\frac{l(x)}{\beta(x)},\frac{l(x)m(x)p(x)}{q(x)},\frac{l(x)m(x)\xi(x)p(x)}{q(x)},\frac{\eta(x)\xi(x)\delta(x)p(x)}{\beta(x)q(x)}\right),$$

where

$$l(x)=\eta(x)+\alpha(x),\ m(x)=\frac{\gamma(x)\delta(x)}{\beta(x)},\ p(x)=\beta(x)-\big(\eta(x)+\alpha(x)\big)$$

and

$$q(x)=\big(\eta(x)+\alpha(x)\big)\big(\gamma(x)\delta(x)+\gamma(x)\xi(x)\big)+\xi(x)\delta(x)\big(\gamma(x)+\eta(x)\big).$$

Malicious code free equilibrium point at $(\delta(x),0,0,0)$.

It is easy to check that the set

$$\Sigma = \{(S, E, I, Q, R) \in {R_5}^+ : S + E + I + Q + R = 1\}$$

is positively invariant for (A) and its global attractor is contained in Σ.

$$D = \{(S, E, I, Q) \in {R_4}^+ : S + E + I + Q \leq 1\}$$

is a positive invariant set of (B).

Now we assume that the amounts of malicious code differ in different nodes of the computer network, i.e., x can be seen as a fuzzy number with triangular shape according to following membership function:

$$\varphi(x) = \begin{cases} 1 - \frac{|x - \bar{x}|}{\theta} \; if \; x \in [\bar{x} - \theta, \bar{x} + \theta] \\ 0 \qquad\quad if \; x \notin [\bar{x} - \theta, \bar{x} + \theta], \end{cases}$$

where the parameter $\bar{x}$ is a central value and θ gives the dispersion of each one of the fuzzy sets assumed by x. For a fixed $\bar{x}$, $\varphi(x)$ is a linguistic variable and it has linguistic meaning such as low, medium, high and so on.

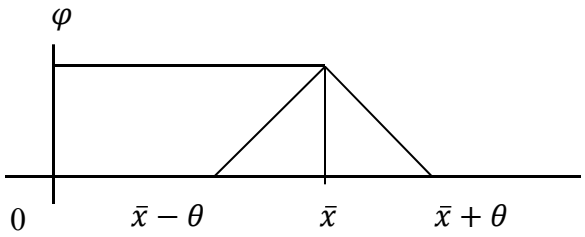

Figure 8. Membership function of the variable x

4. The Basic Reproduction Number (R_0)

The basic reproduction number is defined as the expected number of secondary cases that would arise from the introduction of a single primary infectious case into a fully susceptible population. We know that, in classical SEIQRS model the basic reproduction number (R_0) can be obtained by calculating the matrices V and F (Mishra and Jha, 2010), where R_0 is defined as the dominant Eigen value of FV^{-1} (Jones 2007). V and F represent transition matrix and infection matrix respectively. They are given as,

$$V = \begin{bmatrix} \xi & 0 & 0 \\ -\xi & \eta + \alpha & 0 \\ 0 & -\eta & \gamma \end{bmatrix}, \qquad F = \begin{bmatrix} 0 & \beta & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

and so,

$$FV^{1}=\begin{bmatrix} 0 & \frac{\beta}{\xi} & 0 \\ 0 & \frac{\beta}{\eta+\alpha} & 0 \\ 0 & \frac{-\eta\beta}{\alpha(\eta+\alpha)} & 0 \end{bmatrix}.$$

Hence $R_0 = \frac{\beta}{\eta+\alpha}$, which means that the malicious codes will not spread in the network if $\frac{\beta}{\eta+\alpha} < 1$ and it will attack the network if $\frac{\beta}{\eta+\alpha} > 1$. Now, due to fuzziness, $\beta = \beta(x)$, $\alpha = \alpha(x)$ and $\eta = \eta(x)$ and so we can write, $R_0(x) = \frac{\beta(x)}{\eta(x)+\alpha(x)}$. By this discussion, in order to control the transmission of malicious codes, we can impose $max\ \{R_0(x)\} < 1$. But this can be an extreme assumption. So, perhaps, it is better to adopt an average value of $R_0(x)$. For a given triangular fuzzy number $\varphi(x)$, we define the fuzzy basic reproduction number by,

$$R_0{}^f = \frac{1}{\alpha_0} FEV[\alpha_0 R_0(x)],$$

where FEV is the *fuzzy expected value* and $\alpha_0 > 0$ is the lowest recovery rate in infectious class.

Here, $R_0(x)$ can be greater than one but $\alpha_0 R_0(x) \leq 1$, so that $R_0{}^f$ is well-defined. Here, $R_0{}^f$ can be taken as the average number of secondary cases of infected nodes introduced into a susceptible class. So, to define $FEV\ [\alpha_0 R_0(x)]$, we take a fuzzy measure μ by using probability measure as:

$$\mu\ (A) = sup_{x\epsilon A}\sigma(x);\ A \subset R.$$

It means that the infectivity of a group is the one presented by the node in a computer network belonging to the group with maximal infectivity. Now, in the sense of $R_0{}^f$ we assume that the amount of malicious code x in the network has a linguistic meaning classified as *low*, *medium* and *high*. Then the fuzzy sets are given by the membership function $\varphi\ (x)$ for the three different cases:

(i) *low*, if $\bar{x} + \theta < x_{min}$,

(ii) *medium*, if $\bar{x} - \theta > x_{min}$ and $\bar{x} + \theta \leq x_M$,

(iii) *high*, if $\bar{x} - \theta > x_M$.

5. Comparison between R_0 and $R_0{}^f$

Here, we analyze the above three cases as discussed in the previous section, for the amount of malicious code load. Now for any of the three cases, we have

$$\frac{\beta(\bar{x})}{\eta(\bar{x})+\alpha(\bar{x})} < \frac{1}{\alpha_0} FEV[\alpha_0 R_0(x)] < \frac{\beta(\bar{x}+\theta)}{\eta(\bar{x}+\theta+\alpha(\bar{x}+\theta)}.$$

That is,

$$R_0(\bar{x}) < R_0{}^f < R_0(\bar{x}+\theta).$$

Since

$$R_0(x) = \frac{\beta(x)}{\eta(x)+\alpha(x)}$$

is crescent and continuous, by intermediate value theorem there exists only one x' with

$$\bar{x} < x' < \bar{x} + \theta, \text{ such that, } R_0{}^f = R_0(x') > R_0(\bar{x}).$$

This means that, there is an amount of malicious code $'$, where R_0 (classical) and $R_0{}^f$ (fuzzy) coincide. Also, the medium value of the number of secondary cases ($R_0{}^f$) is higher than the number of secondary cases due to the medium amount of malicious code $R_0(\bar{x})$.

6. Global Stability of the Malicious Code-Free Equilibrium

Lemma 1.

If $R_0 < 1$ the malicious code-free equilibrium is globally asymptotically stable. (Mishra et al. (2009)).

Lemma 2.

Let $f_\infty = \lim_{t\to\infty} inf_{\theta\geq t}\ f(\theta), f^\infty = \lim_{t\to\infty} sup_{\theta\geq t}\ f(\theta)$. 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 $\lim_{t\to\infty} f'(t_k) = 0$ (Mishra *et al.* (2009)).

Theorem 1.

If $R_0 < 1$ then the malicious code-free equilibrium is globally asymptotically stable.

Proof:

In this section we prove the local and global stability of the system using its Jacobian and by the Perron-Frobenius theorem.

Jacobian matrix of the system (B) for malicious code free state ($I = 0$) is given as,

$$\begin{bmatrix} -\delta & -\delta & -\delta & -\delta \\ 0 & -\delta & 0 & 0 \\ 0 & \xi & -\eta-\alpha & 0 \\ 0 & 0 & \eta & -\gamma \end{bmatrix}.$$

The characteristic equation of this matrix is

$$(\delta+\lambda)^2(\gamma+\lambda)(\eta+\alpha+\lambda) = 0.$$

The eigenvalues are $-\delta, -\delta, -\gamma, (-\gamma-\alpha)$.

All eigenvalues are negative so the system is locally asymptotically stable.

Now from the first equation of (B) we have

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

A solution of the equation $\frac{dX}{dt} = \delta - \delta X$ is super solution of $S(t)$.

Since $x \to 1$ as $t \to \infty$, then for a given $\varepsilon > 0$ there exists a t_0 such that

$$S(t) \le X(t) \le 1 + \varepsilon \; for \; all \; t \ge t_0.$$

Thus,

$$S^{\infty} \le X(t) \le 1 + \varepsilon.$$

Let $\varepsilon \to 0$ then $S^{\infty} \le 1$.

Second equation of (B) reduces to

$$\frac{dE}{dt} = \beta(1+\varepsilon)I - \xi E. \tag{1}$$

Now taking third and fourth equation of (B) with (1)

$$\begin{bmatrix} \dot{E} \\ \dot{I} \\ \dot{Q} \end{bmatrix} \le P \begin{bmatrix} E \\ I \\ Q \end{bmatrix},$$

where

$$P = \begin{bmatrix} -\xi & (\varepsilon+1)\beta & 0 \\ \xi & -(\eta+\alpha) & 0 \\ 0 & \eta & -\gamma \end{bmatrix}. \tag{2}$$

Let $M \in R^+$, such that $M \geq max\,(\xi, (\eta + \alpha), \gamma)$. Thus, $P + M\,I_{3\times3}$ is a positive matrix if ω_1, ω_2 and ω_3 are the eigenvalues of P then $\omega_1 + M$, $\omega_2 + M$, $\omega_3 + M$ are eigenvalues of $P + M\,I_{3\times3}$. Thus, from the Perron- Frobenius theorem $P + M\,I_{3x3}$ has a simple positive eigenvalue equal to dominant eigenvalue and corresponding eigenvector $e > 0$, which implies that $\omega_1, \omega_2, \omega_3$ are real (Hale (1980), Olesky et al. (2009) and Abed and Szyld (2010)). If $\omega_1 + M$ is the dominant eigenvalue of $P + MI_{3\times3}$ then $\omega_1 > \omega_2$ and $eP = e^{\omega_1}$. Obviously, ω_1 and ω_2 are the roots of the equation,

$$\lambda^2 + (\eta + \alpha + \xi)\lambda + \big((\eta + \alpha)\xi - (1 + \varepsilon)\beta\xi\big) = 0. \tag{3}$$

Since $R_0 < 1$ for $\varepsilon > 0$ which is sufficiently small, we have

$$\big((\eta + \alpha)\xi - (1 + \varepsilon)\beta\xi\big) > 0.$$

Therefore, the coefficients of the quadratic equation (3) are positive. Thus, $\omega_1, \omega_2, \omega_3$ are all negative. So from equation (2) for $t \geq t_0$ we have

$$\frac{d}{dt}(e[E(t), I(t), Q(t)]) \leq \omega_1 . e[E(t), I(t), Q(t)].$$

Integrating the above inequality we have

$$0 \leq e.[E(t), I(t), Q(t)] \leq e.[E(t), I(t), Q(t)]e^{\omega_1(t-t_1)} \text{ for } t \geq t_1 \geq t_0.$$

Since $\omega_1 < 0$, $e.[E(t), I(t), Q(t)] \to 0\ as\ t \to \infty$. Using $e > 0$, we have $E(t), I(t), Q(t) \to (0,0,0)\ as\ t \to \infty$. By lemma 2, we choose a sequence $t_n \to \infty$ and $S_n \to \infty (n \to \infty)$ such that,

$$S(S_n) \to S^{\infty},\ S(t_n) \to S_{\infty},\ \dot{S}(S_n) \to 0 \text{ and } \dot{S}(t_n) \to 0.$$

Since $E(t), I(t), Q(t) \to 0$, for $t \to \infty$. Thus, from the first equation of (B), we have

$$\lim_{n\to\infty} S(t) = \delta.$$

Hence, by incorporating lemma1, the malicious code-free equilibrium is globally asymptotically stable if $R_0 < 1$.

Now we try to investigate the local stability of the endemic equilibrium. The characteristic equation of endemic equilibrium is $\lambda^4 + c_1\lambda^3 + c_2\lambda^2 + c_3\lambda + c_4 = 0$, where c_1, c_2, c_3 and c_4 are positive constants. When the model (A) is linearized about the endemic equilibrium point and Routh – Hurwitz theorem is applied to the roots of the characteristic equation, it is found that all the roots have negative real parts. Hence the endemic equilibrium point is locally asymptotically stable.

7. Conclusion

The use of fuzzy theory in this work allowed us to study the SEIQRS model with heterogeneity within the compartment. Due to the latent time between the susceptible and the infectious state, the e-SEIQRS epidemic model is more suitable for modeling a malicious code attack in a computer network.

In this section, we simulated the system of equations developed, analyzed the stability of the proposed model and observed the effects of the anti-virus. The initial parameter values were chosen in such a way that it better suit a real malicious code attack scenario. In numerical simulations the total number of nodes was taken as 10,000, all of which were initially susceptible to attack. The rate of infection in exposed state is taken as 0.05. To measure the impact of the malicious code attack in a real network environment the recovery rate has been taken to be 0.02 in infectious class and 0.025 in quarantine class. Figure 9 shows the system behavior when initial values of exposed and infectious nodes were set respectively at E(0) = 100 and I(0) = 0. Figure 10 shows the behavior of recovered nodes versus time. Figure 11 represents the behavior of recovered nodes versus quarantine nodes. The simulated results show that, for the chosen numbers of quarantined nodes and for the given value of parameters, recovery of nodes is very high. So it is recommended to the software organization to maintain the value of the parameters for anti-virus software.

Numerical methods are employed to solve and simulate the system of equations. Mathematically, we developed the reproduction number using the set of differential equations for the SEIQRS model. The simulation results which is supported by the theoretical approach show that all malicious codes were able to pervade if the reproduction rate is less than one.

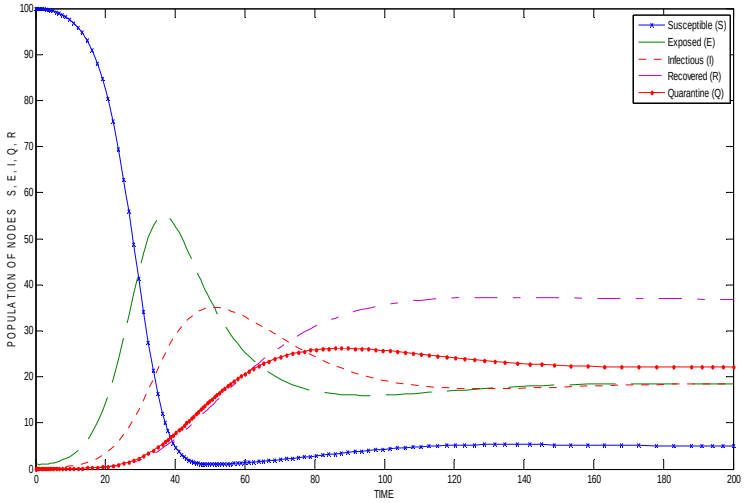

Figure 9. Numerical simulation of the system $(R_0 < 1)$

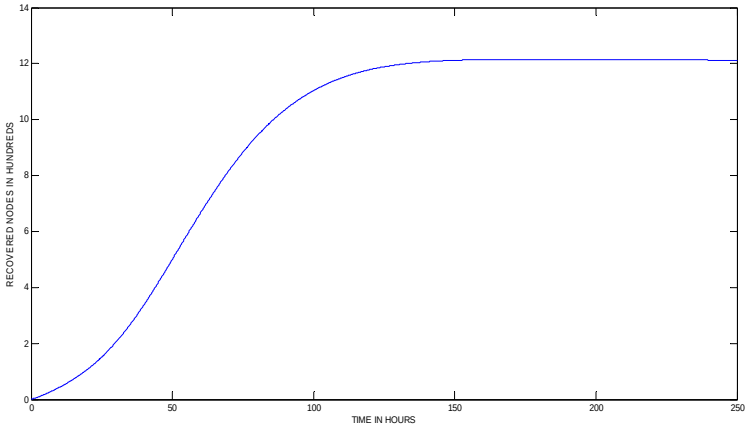

Figure 10. Effect of recovered nodes with time $(R_0 < 1)$

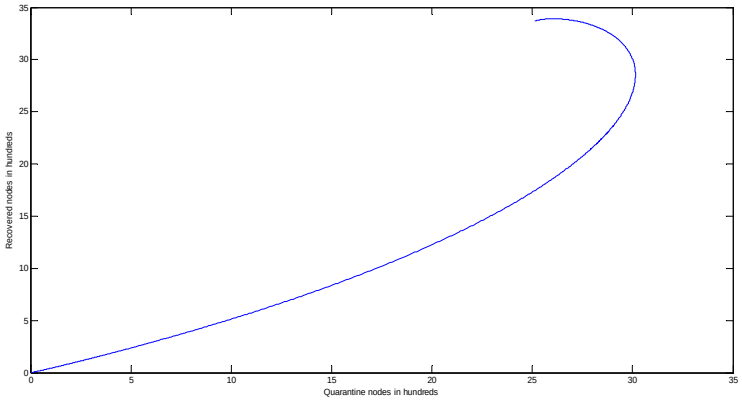

Figure 11. Quarantine class versus Recovered class ($R_0 < 1$)

Table 1: Notation and parametric values used for simulating the model

Notation	Explanation	Initial value
S(t)	Number of susceptible nodes at time t	$S(0) = 9{,}900$
E(t)	Number of exposed nodes at time t	$E(0) = 100$
I(t)	Number of infected nodes at time t	$I(0) = 0$
Q(t)	Number of quarantine nodes at time t	$Q(t) = 0$
R(t)	Number of recovered nodes at time t	$R(t) = 0$
β	Infectivity contact rate	$\beta = 0.01$
ξ	Rate of infection	$\xi = 0.05$
γ	Recovery rate in quarantine class	$\gamma = 0.025$
α	Recovery rate in infectious class	$\alpha = 0.02$
δ	Rate of susceptible in recovered class	$\delta = 0.025$
η	Rate of quarantine	$\eta = 0.03$

REFERENCES

Chen, T. and Jamil, N. (2006). Effectiveness of quarantine in worm epidemic, IEEE International Conference on Communications, IEEE, pp. 2142-2147.

Draief, M., Ganesh, A. and Massouili, L. (2008). Thresholds for virus spread on network, Annals of Applied Probability, Vol. 18, No. 2, pp. 359 – 369.

Datta, S. and Wang, H. (2005). The effectiveness of vaccinations on the spread of email-borne computer virus, IEEE CCECE/CCGEL, IEEE, pp. 219–223.

Elhashash, Abed and Szyld, Daniel B. (2010). Perron-Frobenius Properties of General Matrices. Report 07-01-10. http://www.math.temple.edu/~szyld

Hale, J. K. (1980). Ordinary Differential Equations, (Second Edition), R. E. Krieger Publishing Company, Basel.

Han, Xie and Tan, Qiulin (2010). Dynamical behavior of computer virus on Internet, Applied Mathematics and Computation, Vol. 217, No. 6, pp. 2520–2526.

Jones, James Holland (2007). Notes on R_0, Department of Anthropological Sciences Stanford University.

Keeling, M. J. and Eames, K.T.D. (2005). Network and epidemic models, Journal of Royal Society Interface, Vol. 2, No. 4, pp. 295 – 307.

Kephart, J.O., White, S.R. and Chess, D.M. (1993). Computers and Epidemiology, IEEE Spectrum, pp. 20 – 26.

Kephart, J.O. (1995). A biologically inspired immune system for computers, Proceeding of International Joint Conference on Artificial Intelligence.

Kermack, W. O. and McKendrick, A. G. (1927). A contribution to the mathematical theory of epidemics, Proceedings of the Royal Society, London A, Vol. 115, pp. 700–721.

Kermack, W.O. and McKendrick, A.G. (1932). Contributions of mathematical theory to epidemics, Proceedings of the Royal Society, London A, Vol. 138, pp. 55–83.

Kermack, W.O. and McKendrick, A.G. (1933). Contributions of mathematical theory to epidemics, Proceedings of the Royal Society, London A, Vol. 141, pp. 94–122.

www.math.wsu.edu/math/faculty/tsat/AIM/eventually.pdf.

Kim, J., Radhakrishana, S. and Jang, J. (2006). Cost Optimization in SIS Model of Worm Infection, ETRI Journal, Vol. 28, No. 5, pp. 692-695.

Li, G. and Zhen, J. (2004). Global stability of an SEI epidemic model with general contact rate, Chaos, Solitons and Fractals, Vol. 23, pp. 997–1004.

May, R.M. and Lloyd, A. L. (2001). Infection dynamics on scale-free networks, Physical Review E 64, 066112.

Mishra, Bimal Kumar and Saini, D. K. (2007). SEIRS epidemic model with delay for transmission of malicious objects in computer network, Applied Mathematics and Computation, Vol. 188, No. 2, pp. 1476–1482.

Mishra, Bimal Kumar and Jha, Navnit (2007). Fixed period of temporary immunity after run of anti-malicious software on computer nodes, Applied Mathematics and Computation, Vol. 190, pp. 1207– 1212.

Mishra, Bimal Kumar, Nayak, Prashant Kumar and Jha, Navnit (2009). Effect of Quarantine nodes in SEIQAmS model for the transmission of malicious objects in computer network, International Journal of Mathematical Modelling, Simulation and Applications, Vol. 2, No. 1, pp. 101-112.

Mishra, Bimal Kumar and Jha, Navnit (2010). SEIQRS model for the transmission of malicious objects in computer network, Applied Mathematical Modelling, Vol. 34, pp. 710–715.

Mishra, Bimal Kumar and Pandey, Samir Kumar (2010). Fuzzy epidemic model for the transmission of worms in Computer network, Nonlinear Analysis: Real World Applications, Vol. 11, No. 5, pp. 4335–4341.

Newman, M.E.J., Forrest, S. and Balthrop, J. (2002). Email networks and the spread of computer virus, Physical Review E, Vol. 66, 035101–1–035101–4.

Olesky, D. D., Tsatsomeros, M. J. and van den Driessche, P. (2009). A Generalization of M-Matrices based on eventually nonnegative matrices, Electronic Journal of Linear Algebra, Vol. 18, pp. 339-351.

Pastor-Satorras, R. and Vespignani, A. (2002). Epidemics and immunization in scale-free networks, Handbook of Graphs and Network: From the Genome to the Internet, Wiley-VCH, Berlin.

Picqueria, J. R. C. (2009). A modified epidemiological model for computer viruses, Applied Mathematics and Computation, Vol. 213, No. 2, pp. 355–360.

Williamson, Ma M. and Laeveillae, J. (2003). An Epidemiological Model of Virus Spread and cleanup. http://www.hpl.hp.com/techreports

Yuan, Hua and Chen, G. (2008). Network virus epidemic model with the point – to – group information propagation, Applied Mathematics and Computation, Vol. 206, No.1, pp. 357–367.

Zou, C. C., Gong, W. and Towsley, D. (2003). Worm propagation modeling and analysis underdynamic quarantine defense, Proceeding of the ACM CCS Workshop on Rapid Malcode, ACM, pp. 51–60.