

Worm Propagation with Differential Infectivity under Quarantine Control Strategy

Sounak Paul* and Bimal Kumar Mishra

*Dept. of Computer Sc. & Engineering
Birla Institute of Technology,
Mesra, Ranchi, India
Dept. of Applied Mathematics
Birla Institute of Technology,
Mesra, Ranchi, India*

Abstract

Malwares have sharp resemblance with the biological pathogens in terms of propagation. Biological pathogens spread from one living being to another in very short span of time. Similarly malwares also propagate rapidly from one host to another host and one network to another network, in order to spread infection in major scale. This spread can be epidemic if control strategies are not called in time. In order to timely intervene, study of epidemic behavior is very important. In this paper we develop SIII2Q1Q2R1R2 model of worm propagation under quarantine control strategy. We have considered different infective, quarantined and recovered (or removed) group in our model. The motivation of such model came from the study of propagation dynamics of HIV. Our worm propagation and its quarantined based defense is based on staged-progression (SP) hypothesis of HIV. We have studied in this paper the stability of worm free equilibrium condition and analyzed the epidemic state condition in terms of reproduction number. When reproduction number is greater than one the worm propagation become epidemic. If it is less than one then infection diminishes. Extensive analysis and simulation has been done to validate our system. Simulation result shows that effective quarantine strategy helps in controlling the epidemic outbreak of worms in networks.

Keywords: *malware, defense, propagation, quarantine, epidemic, stability, equilibrium, network*

1. Introduction

Malware attacks are still a major source of network threats. These automated programs are responsible for several malicious activities in network. These malicious activities include extended bandwidth consumption, creating performance bottleneck, corrupting computing resources, causing denial of service attack. These malicious programs could propagate very fast using e-mail attachment, instant message; file sharing, Internet relay chat *etc.* Early intervention is required to stop them from propagating and infecting other machines at very high rate to prevent an epidemic condition. Quarantine [1-6], is one among many available defenses which slow down the worm propagation rate.

Quarantine concept came from the age old practice of isolating the infectious individuals from healthy, yet susceptible population to prevent infection from spreading at an epidemic rate. Although it is practically not possible to isolate the entire subset of infectious population, the basic goal of quarantine is to curtail the speed of propagation by

* Corresponding Author. The author is presently deputed at BIT International Centre, Muscat, Sultanate of Oman (Waljat-College-of-Applied-Sciences)

isolating a subset of infectious population from susceptible population. Worms and other malware such as virus, Trojan *etc.* also propagate in computer network in similar way as of biological pathogens as described by many researchers. These malwares are automated program that replicate in order to spread themselves from one host to another host in the network. Within a very short span of time infection becomes epidemic, unless appropriate control strategy comes at rescue from such situation. Therefore it is very important to control the worm propagation, such that the manual and automated countermeasures can reduce the rate of infection. Quarantine is a defense strategy that is not sufficient by itself. It is complemented by other control strategies such as antivirus treatment, patching, filtering the malicious traffic using host level as well as network level firewalls, Intrusion detection system (IDS and Intrusion prevention system (IPS). These defense mechanisms help in removing the vulnerabilities and cure the infection. Quarantine slows down the rate of infection and thereby provides time to other control strategies to disinfect the infected host within the network. It also helps in buying time to apply the control strategies, thereby reducing the probability of vulnerable host to be infected by both external and internal host. Quarantine helps in reducing the damage in the network by preventing the outbreak as epidemic.

In this paper we develop SII2Q1Q2R1R2 model of worm propagation under quarantine control strategy. We have considered different infective, quarantined and recovered (or removed) group in our model. The motivation of such model came from the study of propagation dynamics of HIV. The study of HIV and AIDS shows that the disease can spread in two ways. First, depending on infectivity the infective population can be divided in several different groups. Infective individuals will remain in that group until they develop AIDS. This hypothesis is known as differential infectivity (DI) hypothesis [7-8]. Another hypothesis of HIV propagation is staged-progression (SP) [7], where the infective population will pass through different stages of infection. The primary infective group may acquire secondary infection and so on. This is because infected individual loose immunity and thus prone to any other secondary infection thereafter. Our worm propagation and its quarantined based defense is based on staged-progression (SP) hypothesis of HIV.

2. Related Work

One of the early theoretical model of worm propagation was proposed by Fred and Cohen [9]. The mathematical theory of epidemiology [10-12] concerning propagation of infectious disease is well established. Computer worms spread in network much like infectious diseases. Epidemiological theory can correctly represent the spreading behavior of worms and network limitations associated with it. Extensive research has been done in modeling the spreading of malware in computer and other networks. Kephart and White proposed a classical epidemiological model [13] of computer virus by drawing analogy between computer virus and biological virus. This model was later used in [14] to explore the propagation dynamics of Code Red worm [15]. Zou *et. al.*, further refined these models to consider effect of human countermeasures such as scanning with anti-virus, installing and updating patches and filtering with firewalls. They proposed a two-factor model in [4]. Weaver *et. al.*, [16] also improved the propagation model in [14] and [5] to fit with observed Code-Red propagation data. Many of the above mentioned models are actually based on Karmack-McKendrick classical epidemic model and [12] [17]. In classical simple epidemic model (also known as S-I model) [10-11], all hosts in network can take one of only two states: Susceptible (S) and Infectious (I). In classical general epidemic model (also known as SIR model) an additional state, Removed/Recovered (R) is introduced [17]. Classical simple epidemic model is simplest worm epidemic model and inspired many researchers to adopt this model to develop propagation dynamics of many bandwidth limited TCP worms such as Code Red [17], Slammer [18] *etc.*

Chen *et. al.*, presented a sophisticated Analytical Active Worm Propagation (AAWP) epidemic model [19] for characterizing random scanning worms. AAWP is based on deterministic approximation and discrete times. This model provides some countermeasures by monitoring connections in unused address space. Kesidis *et. al.*, adopted simple deterministic equations used by Kermack-McKendrick to correctly describe the spreading behavior of TCP worms, Slammer and Witty. This model also captures the scanning activity and limitation of their spread in networks. Worm propagation in network has been described by many other epidemic models [20-25] using different state transitions and different parametric conditions.

The worm propagation can be described using both deterministic as well as stochastic model. Deterministic models are further classified as continuous time and discrete time models. The deterministic models are based on homogeneous assumptions. *i.e.*, every host in network has equal probability of infecting any other vulnerable hosts. The models are not constrained by network topology. Continuous time propagation models are represented by set of differential equations whereas discrete time models are represented by set of difference equations.

Mishra and Saini [26] developed a different mathematical model to study the propagation behavior of the worms in computer system. These models help in finding probability of a system to be infected. They are useful in developing optimal defense solution against malware. Yan and Liu [27] studied SEIR worm propagation model. This model considers permanent recovery from infection state after some countermeasure applied on it. However in computer epidemiology, the condition is not realistic. Host can never achieve permanent immunity.

To overcome this constraint Mishra and Saini proposed SIRS model [28] that consider fixed period temporary immunity of the recovered hosts and SEIR model [29] that considers constant latent and immune periods. Worm free condition is discussed. Epidemic state threshold parameter- reproduction number has been evaluated. However the papers do not investigate the global stability of worm free equilibrium state. Fei *et. al.*, proposed a three layer worm model (TLWM) [29], to study the effect of network address translator (NAT), in propagation speed of worms. In this work the authors have extended the simple classical model and two factor model discussed above. Analysis and simulation study shows that NAT is effective in slowing the propagation speed of worms in Internet.

Kondakci presented a stochastic worm propagation model [30] using Markovian process to analyze epidemic states of computer system. This model helps to study the dynamics of state transition during worm propagation to estimate infection probability and rate of recoverability of infected hosts. Karma *et. al.*, [31] investigated the effects of DNS delays on worm propagation in IPV6 networks. Toutonji *et. al.*, proposed VEISV model [32] to study the effectiveness of human countermeasure on worm spreading behavior. They have studied various conditions of reproduction number on epidemic control. Global as well as local stability of worm free equilibrium has been discussed in this paper. Simulation result and analysis shows positive impact of countermeasure on worm propagation. Yao *et. al.*, described a worm propagation model [33] with time delay in quarantine. Local and global stability analysis has been discussed. Hopf bifurcation condition is derived to study the worm elimination condition.

3. Formulation of the Model

We propose $SI_1I_2Q_1Q_2R_1R_2$ model to study the worm propagation dynamics under quarantine defense strategy. We have considered variation in infectiousness and quarantine in our model. We assume that the total nodes K are divided into following states: S (Susceptible), E (Exposed), I_1 (Primary infected), I_2 (Secondary infected), Q_1 (Quarantine of I_1), Q_2 (Quarantine of I_2), R_1 (Removed) and R_2 (Recovered). A host can be

at any one of these eight states at any point of time. Susceptible host become Exposed when a worm code is transferred into it. Mere transfer of a malware does not make the host infectious. The worm code may take some time (latent period) before it gets activated in a host, to start the malicious activities in it. Once the worm code is activated the host becomes infected. It may start showing its malicious behavior at this stage. The worm code may also get replicated to infect other hosts in the network. In this model we have considered differential infectiousness I_1 (Primary infection) and I_2 (added secondary infection). Exposed nodes first enter into subgroup I_1 and then gradually progressed into I_2 , when other infection gets added into previously infected subgroup. Both infectious groups may be quarantined till they are recovered. Q_1 represents quarantine of I_1 . Q_2 represents quarantine of I_2 . The necessity of different quarantine group is due to difference in infectiousness, and therefore variation in treatment. We assumed that different infectious nodes are isolated in different group, and separate control strategies on them are applied for their cure. R_1 is the removed population from I_1 . R_2 is the recovered population from I_2 .

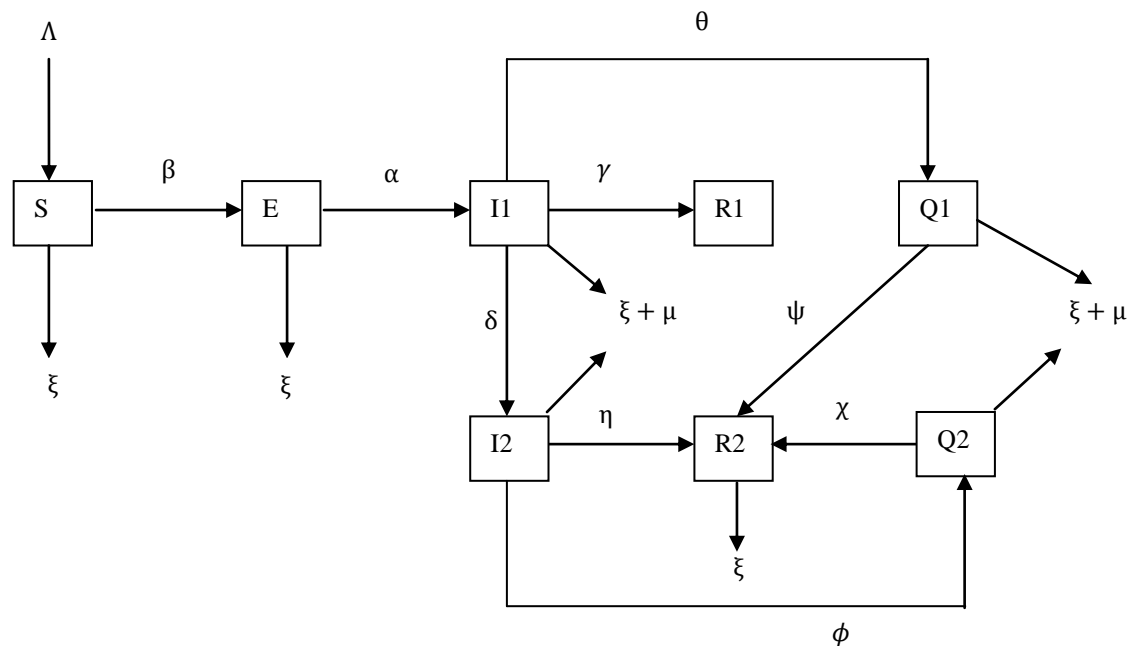


Figure 1. Model State Transition Diagram

Figure 1 shows the state transition of our model. This model is formulated with the assumption that total nodes in the network are relatively stable, and there are replacement possibilities against dead nodes. Let $S(t)$, $E(t)$, $I_1(t)$, $I_2(t)$, $Q_1(t)$, $Q_2(t)$, $R_1(t)$ and $R_2(t)$ denote the number of nodes in states S , E , I_1 , I_2 , Q_1 , Q_2 , R_1 , R_2 at time t , we have the total number of nodes:

$$S(t) + E(t) + I_1(t) + I_2(t) + Q_1(t) + Q_2(t) + R_1(t) + R_2(t) = K(t) \quad (1)$$

The system of differential equations for this model depicted in Figure 1 is given by:

$$\begin{aligned} \frac{dS}{dt} &= \Lambda - \beta SI_1 - \xi S \\ \frac{dE}{dt} &= \beta SI_1 - (\xi + \alpha)E \\ \frac{dI_1}{dt} &= \alpha E - (\xi + \mu + \delta + \gamma + \theta)I_1 \end{aligned}$$

$$\begin{aligned} \frac{dI_2}{dt} &= \delta I_1 - (\xi + \mu + \eta + \phi)I_2 \\ \frac{dQ_1}{dt} &= \theta I_1 - (\xi + \mu + \psi)Q_1 \end{aligned} \quad (2)$$

$$\frac{dQ_2}{dt} = \phi I_2 - (\xi + \mu + \chi)Q_2$$

$$\frac{dR_1}{dt} = \gamma I_1$$

$$\frac{dR_2}{dt} = \eta I_2 + \psi Q_1 + \chi Q_2 - \xi R_2$$

Where Λ denote the inclusion of new nodes in the system *i.e.*, birth coefficient of the nodes, ξ is the coefficient of natural death, *i.e.*, permanent filature of the node due to software or hardware fault, μ is the death rate due to severe attack, β is the infectivity contact rate, α is the coefficient of transmission from E to I_1 , γ denote the coefficient of removal of nodes from I_1 , δ is the coefficient of transmission from I_1 to I_2 , η is the coefficient of recovery from I_2 , θ is the rate of transmission from I_1 to Q_1 , χ is the coefficient of recovery from Q_2 , ψ is the rate of cure from Q_1 into R_2 .

4. Worm Free Equilibrium

Here we will analyze equilibrium and stability of our model; we compute the basic reproduction number for the worm control or worm eradication. By the equation (1) and the system of equations (2),

we get,

$$\frac{dK}{dt} = \Lambda - \xi(K - R_1) - \mu(I_1 + I_2 + Q_1 + Q_2) \quad (3)$$

The equation (3) is referred as equation of total population. Therefore, $K \rightarrow \frac{\Lambda}{\xi}$ as $t \rightarrow \infty$. This shows that, the feasible region $U = \{(S, E, I_1, I_2, Q_1, Q_2, R_1, R_2) : S, E, I_1, I_2, Q_1, Q_2, R_1, R_2 \geq 0, S + E + I_1 + I_2 + Q_1 + Q_2 + R_1 + R_2 \leq \frac{\Lambda}{\xi}\}$ is a positive invariant set for the model. In the absence of infection, the model has a unique disease - free equilibrium $P_0 (\frac{\Lambda}{\xi}, 0, 0, 0, 0, 0, 0, 0)$ and an endemic equilibrium point $P^* (S^*, E^*, I_1^*, I_2^*, Q_1^*, Q_2^*, R_1^*, R_2^*)$, where these points can be obtained by taking all the equations of system (4.2) equal to zero, given by, $S^* = \frac{1}{R_0}$, $E^* = \frac{(\xi + \mu + \delta + \gamma + \theta)(\Lambda R_0 - \xi)}{\alpha \beta}$, $I_1^* = \frac{(\Lambda R_0 - \xi)}{\beta}$, $I_2^* = \frac{\delta(\Lambda R_0 - \xi)}{\beta(\xi + \mu + \eta + \phi)}$, $Q_1^* = \frac{\theta(\Lambda R_0 - \xi)}{\beta(\xi + \mu + \psi)}$, $Q_2^* = \frac{\phi \delta(\Lambda R_0 - \xi)}{\beta(\xi + \mu + \chi)(\xi + \mu + \eta + \phi)}$, R_1^* (any constant) and $R_2^* = \frac{(\Lambda R_0 - \xi)}{\beta \xi} \left[\frac{\eta \delta}{(\xi + \mu + \eta + \phi)} + \frac{\psi \theta}{(\xi + \mu + \psi)} + \frac{\chi \phi \delta}{(\xi + \mu + \chi)(\xi + \mu + \eta + \phi)} \right]$, where, R_0 is the basic reproduction number defined in next section.

5. Basic Reproduction Number (R_0)

To compute basic reproduction number, R_0 , we consider the following equations of infected classes of the population as,

$$\frac{dE}{dt} = \beta S I_1 - (\xi + \alpha)E$$

$$\frac{dI_1}{dt} = \alpha E - (\xi + \mu + \delta + \gamma + \theta)I_1$$

$$\begin{aligned} \frac{dI_2}{dt} &= \delta I_1 - (\xi + \mu + \eta + \phi)I_2 \\ \frac{dQ_1}{dt} &= \theta I_1 - (\xi + \mu + \psi)Q_1 \\ \frac{dQ_2}{dt} &= \phi I_2 - (\xi + \mu + \chi)Q_2 \end{aligned} \tag{4}$$

By linearizing system (4), we get,

$$\begin{bmatrix} \dot{E} \\ \dot{I}_1 \\ \dot{I}_2 \\ \dot{Q}_1 \\ \dot{Q}_2 \end{bmatrix} = (F - V) \begin{bmatrix} E \\ I_1 \\ I_2 \\ Q_1 \\ Q_2 \end{bmatrix}, \text{ where, F and V can be expressed as,}$$

$$F = \begin{bmatrix} 0 & \beta & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ and}$$

$$V = \begin{bmatrix} (\xi + \alpha) & 0 & 0 & 0 & 0 \\ -\alpha & (\xi + \mu + \delta + \gamma + \theta) & 0 & 0 & 0 \\ 0 & -\delta & (\xi + \mu + \eta + \phi) & 0 & 0 \\ 0 & -\theta & 0 & (\xi + \mu + \psi) & 0 \\ 0 & 0 & -\phi & 0 & (\xi + \mu + \chi) \end{bmatrix}$$

Then, R_0 can be given by the dominant eigenvalue of $F V^{-1}$. That is,

$$R_0 = \frac{\beta\alpha}{(\xi + \alpha)(\xi + \mu + \delta + \gamma + \theta)}$$

6. Stability of the System

To evaluate the stability of worm free equilibrium, we take the Jacobian matrix of the system (4.2), that is,

$$J = \begin{bmatrix} -\xi & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -(\xi + \alpha) & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha & -(\xi + \mu + \delta + \gamma + \theta) & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \delta & -(\xi + \mu + \eta + \phi) & 0 & 0 & 0 & 0 \\ 0 & 0 & \theta & 0 & -(\xi + \mu + \psi) & 0 & 0 & 0 \\ 0 & 0 & 0 & \phi & 0 & -(\xi + \mu + \chi) & 0 & 0 \\ 0 & 0 & \gamma & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \eta & \psi & \chi & 0 & -\xi \end{bmatrix}$$

Obviously, the eigen values are, $-\xi$, $-(\xi + \alpha)$, $-(\xi + \mu + \delta + \gamma + \theta)$, $-(\xi + \mu + \eta + \phi)$, $-(\xi + \mu + \psi)$, $-(\xi + \mu + \chi)$, 0 , $-\xi$. Since all eigenvalues are less than or equal to zero, hence the system is locally asymptotically stable.

Lemma 1: If $R_0 < 1$, the disease – free equilibrium P_0 is locally asymptotically stable. If $R_0 = 1$, P_0 is stable and if $R_0 > 1$, P_0 is unstable.

Lemma 2: Assume that a bounded real valued function $f: [0, \infty] \rightarrow R$ be twice differentiable with bounded second derivative. Let $k \rightarrow \infty$ and $f(t_k)$ converges to f^∞ or f_∞ . Then,

$$\lim_{k \rightarrow \infty} f'(t_k) = 0$$

Theorem 1: If $R_0 < 1$, then the worm free equilibrium is globally asymptotically stable.

Proof: In the above discussion, we have obtained that the unique worm free equilibrium P_0 of the system (2) is locally asymptotically stable, if $R_0 < 1$. From the first equation of the system (2), we have,

$$\frac{dS}{dt} \leq \Lambda - dS$$

Let us take an equation, $\frac{dX}{dt} \leq \Lambda - dX$ which one solution is a super solution of $S(t)$.

Since $X \rightarrow \Lambda/\xi$ as $t \rightarrow \infty$, then for a given $\varepsilon > 0$, \exists a t_0 , such that, $S(t) \leq X(t) \leq \Lambda/\xi + \varepsilon$. Since ε is very small, so, $S^\infty \leq \Lambda/\xi$

Similarly, the second equation of the system (2) can be expressed as,

$$\dot{E}(t) \leq \beta I_1 (\Lambda/\xi + \varepsilon) - (\xi + \alpha)E, \text{ for, } t > t_0.$$

Using this and 2nd to 6th equations of the system (2), we have,

$$\begin{pmatrix} \dot{E} \\ \dot{I}_1 \\ \dot{I}_2 \\ \dot{Q}_1 \\ \dot{Q}_2 \end{pmatrix} \leq P \begin{pmatrix} E \\ I_1 \\ I_2 \\ Q_1 \\ Q_2 \end{pmatrix}, \quad \text{where,}$$

$$P = \begin{bmatrix} -(\xi + \alpha) & \beta \left(\frac{\Lambda}{\xi} + \varepsilon \right) & 0 & 0 & 0 \\ \alpha & -(\xi + \mu + \delta + \gamma + \theta) & 0 & 0 & 0 \\ 0 & \delta & -(\xi + \mu + \eta + \phi) & 0 & 0 \\ 0 & \theta & 0 & -(\xi + \mu + \psi) & 0 \\ 0 & 0 & \phi & 0 & -(\xi + \mu + \chi) \end{bmatrix}$$

(5)

Let $M \in R^+$, such that, $M > \max \{(\xi + \alpha), (\xi + \mu + \delta + \gamma + \theta), (\xi + \mu + \eta + \phi), (\xi + \mu + \psi), (\xi + \mu + \chi)\}$. Thus, $MI_{5 \times 5}$ is a strictly positive matrix. If λ_i ($i = 1, 2, 3, 4, 5$) are the eigenvalues of P , then, $M + \lambda_i$ ($i = 1, 2, 3, 4, 5$) are the eigenvalues of $(MI_{5 \times 5} + P)$ Thus from the Perron – Frobenius theorem, $(MI_{5 \times 5} + P)$ has a simple,

positive eigenvalue equal to dominant eigenvalue and corresponding eigenvector $e > 0$, which implies that, λ_i are real. If $(\lambda_1 + M)$ is the dominant eigenvalue of $(MI_{5 \times 5} + P)$, then $\lambda_1 > \lambda_i$ ($i = 2, 3, 4, 5$) and

$$e P = e \lambda_1. \text{ Obviously, } \lambda_i \text{ (} i = 1, 2, 3, 4, 5 \text{) are the roots of the equation,}$$

$$\lambda^5 - (\sum \lambda_1) \lambda^4 + (\sum \lambda_1 \lambda_2) \lambda^3 - (\sum \lambda_1 \lambda_2 \lambda_3) \lambda^2 + (\sum \lambda_1 \lambda_2 \lambda_3 \lambda_4) \lambda - (\lambda_1 \lambda_2 \lambda_3 \lambda_4 \lambda_5) = 0$$

Since $R_0 < 1$, for $\varepsilon > 0$ (sufficiently small), so the coefficients of the above equation are positive. Thus λ_i ($i = 1, 2, 3, 4, 5$) are negative. So, from equation (5), for $t \geq t_0$,

$$\frac{d}{dt} (e[E(t), I_1(t), I_2(t), Q_1(t), Q_2(t)]) \leq \lambda_1 e[E(t), I_1(t), I_2(t), Q_1(t), Q_2(t)]$$

Integrating the above inequality, we get,

$$0 \leq e[E(t), I_1(t), I_2(t), Q_1(t), Q_2(t)] \leq e[E(t_1), I_1(t_1), I_2(t_1), Q_1(t_1), Q_2(t_1)] e^{\lambda_1(t-t_1)}, \text{ for } t \geq t_1 \geq t_0.$$

Since, $\lambda_1 < 0$, $e[E(t_1), I_1(t_1), I_2(t_1), Q_1(t_1), Q_2(t_1)] \rightarrow 0$ as $t \rightarrow \infty$

Using $e > 0$, $e[E(t), I_1(t), I_2(t), Q_1(t), Q_2(t)] \rightarrow [0]$ as $t \rightarrow \infty$.

By lemma 2, we choose a sequence $t_n \rightarrow \infty$, $s_n \rightarrow \infty$ ($n \rightarrow \infty$), such that,

$$S(s_n) \rightarrow S^\infty, S(t_n) \rightarrow S_\infty, \dot{S}(s_n) \rightarrow 0, \dot{S}(t_n) \rightarrow 0.$$

Since, $E(t), I_1(t), I_2(t) \rightarrow Q_1(t), Q_2(t) \rightarrow 0$ as $t \rightarrow \infty$, so, from the first equation of system (2), we get, $\lim_{t \rightarrow \infty} S(t) = \frac{\Lambda}{\xi}$.

Hence by using lemma 1, the disease – free equilibrium P_0 is globally asymptotically stable, if $R_0 < 1$.

We now try to investigate the local stability of the endemic equilibrium point P^* ($S^*, E^*, I_1^*, I_2^*, Q_1^*, Q_2^*, R_1^*, R_2^*$). When the system (2) is linearized about the equilibrium P^* and Routh – Hurwitz theorem is applied to the roots of the characteristic equation, all the roots have negative real part. Hence P^* is locally asymptotically stable.

We have the following important result:

If $R_0 > 1$, then the system (2) has unique endemic equilibrium P^* which is locally asymptotically stable.

7. Results and Discussion

In this section we develop the experimental setup to study the dynamics of worm propagation in network under quarantine control strategy. As we mentioned before, quarantine itself is not sufficient defense measure. It slows down the infection, allowing other human countermeasures to take action on the infection.

It is difficult to use real world worm traffic traces. Traffic traces for some of very popular worms such as Code-Red-I, Code-Red-II, Slammer, Sapphire are also not in public domain. Working with sampled traces is not suitable to correctly study the worm propagation behavior under different circumstances. Few malware traces available in CAIDA (www.caida.org) does not come with legitimate traffic, as they were filtered, when the traces made available. Therefore we have to rely on simulation with different parametric values. Simulation result with different set of parameter gives an insight to the worm propagation behavior, which are helpful in designing an optimal solution for worm defense.

We solve the system of equations using Runge-Kutta-Fehlberg fourth-fifth order numerical methods and the system is simulated under parametric condition mentioned in corresponding figure. Figure 2 shows the dynamic behavior of different states with time. The behavior of S, E, I₁, I₂, Q₁, Q₂, R₁, R₂ is depicted in this figure. We observe this propagation behavior is with $R_0 < 1$. And the system is asymptotically stable. This is the result of quarantine and other security measures applied during defense. Figure 3 and Figure 4 shows, as the number of infectious nodes increases, the number of quarantine is also to be increased, in order to achieve worm free equilibrium and global stability of disease free equilibrium. When the quarantine reaches some threshold, the infection diminishes. This provides the other countermeasures time to prevent the epidemic outbreak of a worm. Figure 5 and figure 6 shows that dynamics of recovered nodes against quarantined node. Quarantine obviously increases recovery. But an optimum quarantine is required to get its maximum benefit. Figure 7 clearly shows that when the number of infectious node increases, recovery becoming difficult, as the infection spread from one host to another host. Figure 8 shows the dynamics of Infectious, quarantined and recovered nodes when $R_0 < 1$. Figure 9 shows recovery improves when both quarantine 1 and quarantine 2 group increases. This result is obvious; as such situation provides other countermeasures to get on infectious nodes to remove the worms.

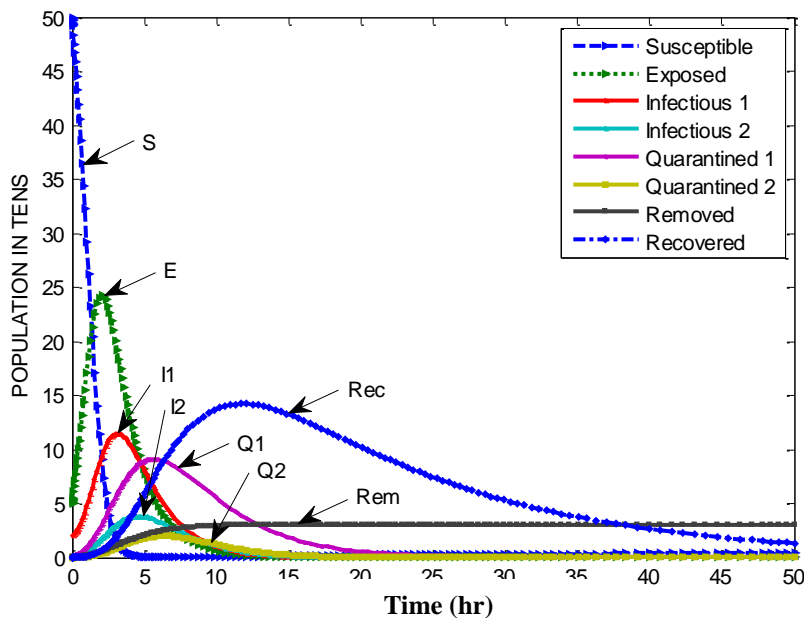


Figure 2. Propagation Behavior of Different Classes of Nodes with Parametric Values, $\Lambda=0.03$, $\xi=0.07$, $\beta=0.15$, $\theta=0.35$, $\mu=0.03$, $\gamma=0.05$, $\alpha=0.45$, $\phi=0.35$, $\psi=0.15$, $\delta=0.25$, $\eta=0.15$, $\chi=0.45$

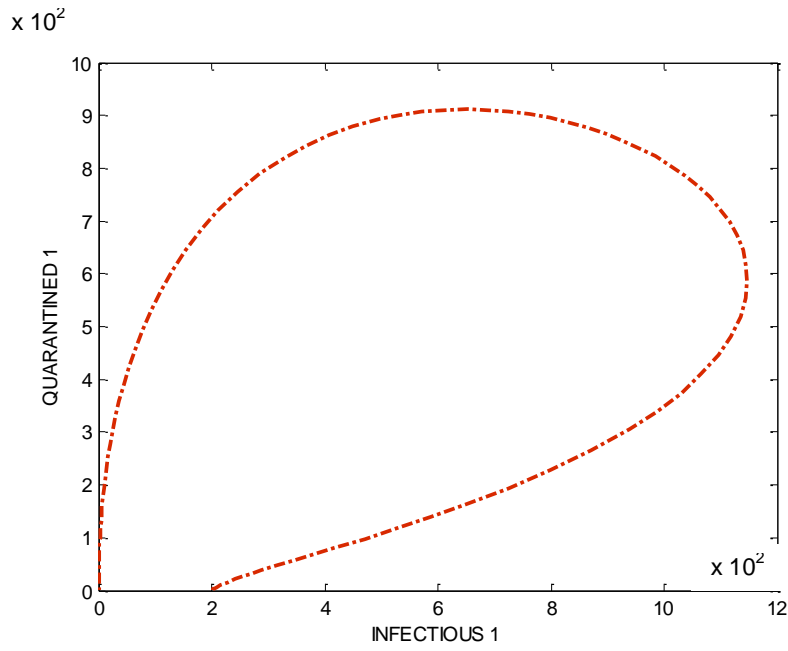


Figure 3. Effect of Q_1 with Respect to I_1 with Parametric Values, $\Lambda=0.03$, $\xi=0.07$, $\beta=0.15$, $\theta=0.35$, $\mu=0.03$, $\gamma=0.05$, $\alpha=0.45$, $\phi=0.35$, $\psi=0.15$, $\delta=0.25$, $\eta=0.15$, $\chi=0.45$

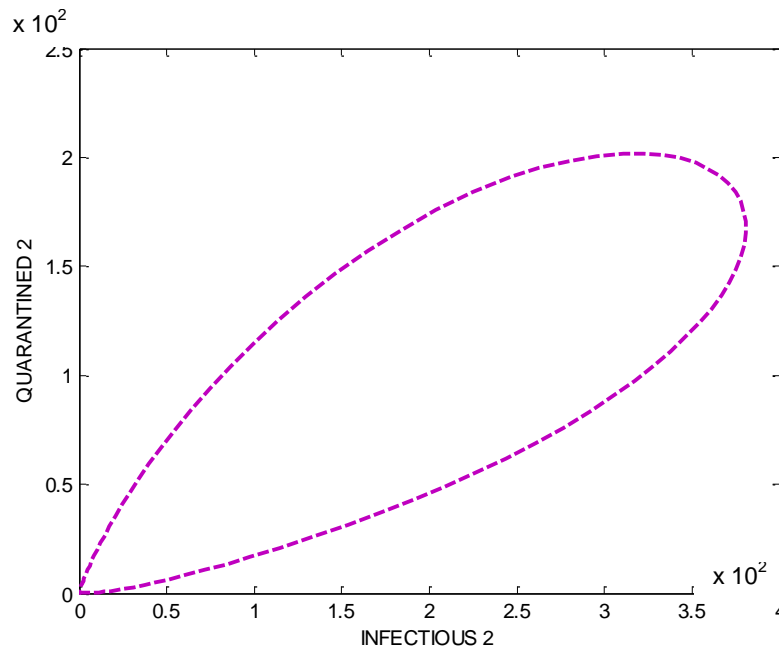


Figure 4. Effect of Q_2 with Respect to I_2 with Parametric Values, $\Lambda=0.03$, $\xi=0.07$, $\beta=0.15$, $\theta=0.35$, $\mu=0.03$, $\gamma=0.05$, $\alpha=0.45$, $\phi=0.35$, $\psi=0.15$, $\delta=0.25$, $\eta=0.15$, $\chi=0.45$

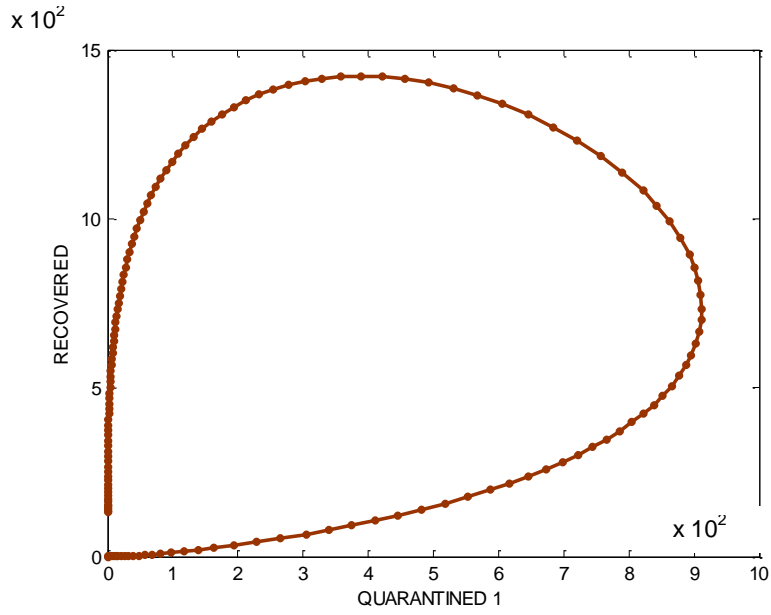


Figure 5. Effect of Q_1 with Respect to R_2 with Parametric Values, $\Lambda=0.03$, $\xi=0.07$, $\beta=0.15$, $\theta=0.35$, $\mu=0.03$, $\gamma=0.05$, $\alpha=0.45$, $\phi=0.35$, $\psi=0.15$, $\delta=0.25$, $\eta=0.15$, $\chi=0.45$

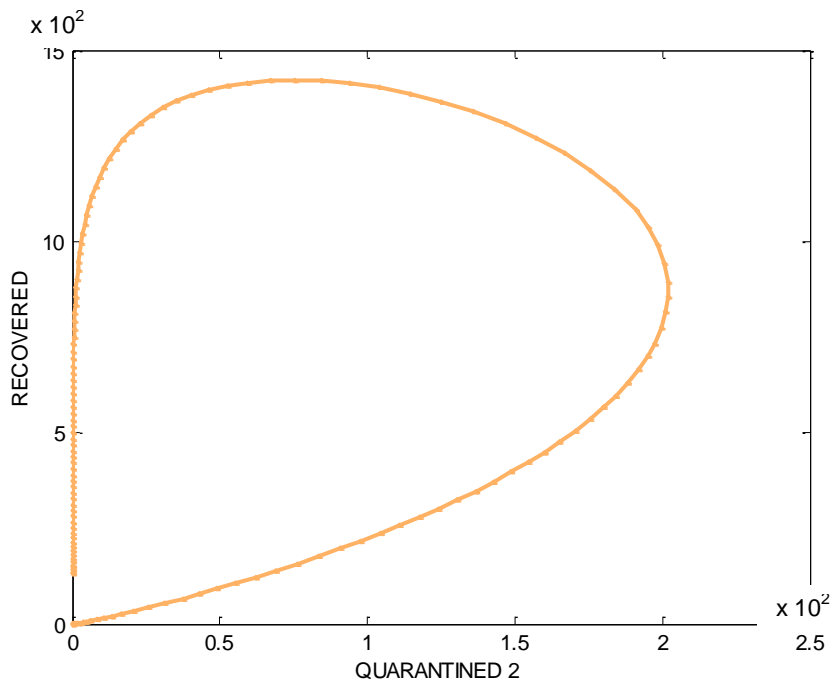


Figure 6. Effect of Q_2 with Respect to R_2 with Parametric Values, $\Lambda=0.03$, $\xi=0.07$, $\beta=0.15$, $\theta=0.35$, $\mu=0.03$, $\gamma=0.05$, $\alpha=0.45$, $\phi=0.35$, $\psi=0.15$, $\delta=0.25$, $\eta=0.15$, $\chi=0.45$

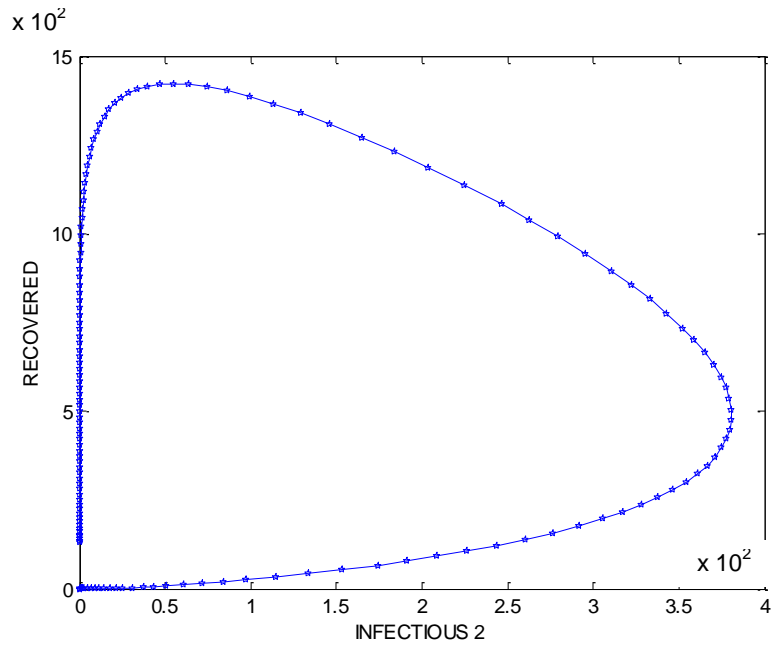


Figure 7. Dynamics of R_2 with Respect to I_2 with Parametric Values, $\Lambda=0.03$, $\xi=0.07$, $\beta=0.15$, $\theta=0.35$, $\mu=0.03$, $\gamma=0.05$, $\alpha=0.45$, $\phi=0.35$, $\psi=0.15$, $\delta=0.25$, $\eta=0.15$, $\chi=0.45$

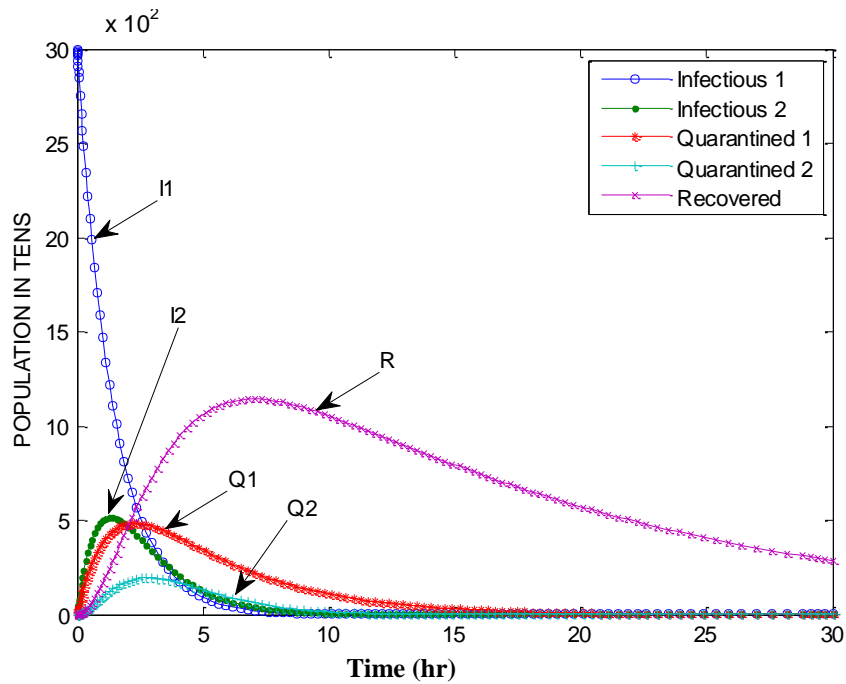


Figure 8. Dynamical Behavior of the System with Parametric Values, $\Lambda=0.03$, $\xi=0.07$, $\beta=0.15$, $\theta=0.35$, $\mu=0.03$, $\gamma=0.05$, $\alpha=0.45$, $\phi=0.35$, $\psi=0.15$, $\delta=0.25$, $\eta=0.15$, $\chi=0.45$

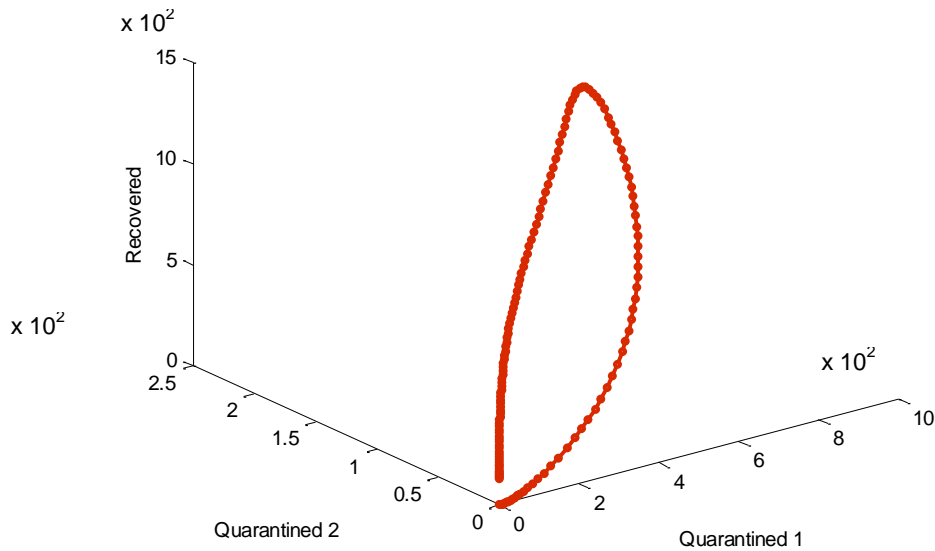


Figure 9. Dynamics of R_2 , Q_2 & Q_1 with Parametric Values, $\Lambda=0.03$, $\xi=0.07$, $\beta=0.15$, $\theta=0.35$, $\mu=0.03$, $\gamma=0.05$, $\alpha=0.45$, $\phi=0.35$, $\psi=0.15$, $\delta=0.25$, $\eta=0.15$, $\chi=0.45$

7. Conclusion

We proposed $SEI_1I_2Q_1Q_2R_1R_2$ model of worm propagation under quarantine control strategy. We have considered different infective, quarantined and recovered (or removed) group in our model. Our worm propagation with quarantined based defense is based on staged-progression (SP) hypothesis of infectivity. Exposed nodes first enter into infective subgroup I_1 and then gradually progressed into infective subgroup I_2 , when other infection also gets added into previously infected subgroup. Both infectious groups may be quarantined till they are recovered. Q_1 represents quarantine of I_1 . Q_2 represents quarantine of I_2 . The necessity of different quarantine group is due to difference in infectiousness, and therefore variation in treatment. Simulation result shows that when basic reproductive number $R_0 < 1$ infection diminishes and prevent epidemic condition. Result also shows that optimal quarantine helps in reducing infection and increases recovery.

Acknowledgements

This work is partially supported by Birla Institute of Technology, Mesra, Ranchi, India and Waljat College of Applied Science (Birla Institute of Technology, International Centre, Muscat, Oman). The authors would also like to thank the anonymous reviewers for their constructive comments and feedback on this paper.

References

- [1] D. Moore, C. Shannon, G. M. Voelker and S. Savage, "Internet quarantine: requirements for containing self-propagating code", in: Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '2003), San Francisco, California, USA, (2003) April, pp. 1901-1910.
- [2] T. M. Chen and N. Jamil, "Effectiveness of quarantine in worm epidemics", in: Proceedings of IEEE International Conference on Communications, (2006), pp. 2142-2147.

- [3] L. Tao, W. Huihui and Z. Zhengping, "Modeling and analyzing the spread of worm based on quarantine", in: Proceedings of IEEE 27th Chinese Control Conference, (2008), pp. 299-301.
- [4] H. Hethcote, M. Zhien and L. Shengbing, "Effects of quarantine in six endemic models for infectious diseases", *Mathematical Biosciences*, vol. 180, no. 1, (2002), pp. 141-160.
- [5] B. K. Mishra and N. Jha, "SEIQRS model for the transmission of malicious objects in computer network", *Applied Mathematical Modeling*, vol. 34, (2010), pp. 710-715.
- [6] M. Khouzani and E. Altman, "Optimal quarantining of wireless malware through reception gain control", *IEEE Transaction on Automatic Control*, vol. 57, no. 1, (2012), pp. 49-61.
- [7] Z. Ma and J. Li, "Dynamic Modeling and Analysis of Epidemics", World Scientific Press, (2009).
- [8] B. K. Mishra and A. K. Singh, "SI₁RS e-Epidemic model with multiple groups of infection in computer networks", *International Journal of Nonlinear Science*, vol. 13, (2012), pp. 357-362.
- [9] F. Cohen, *Computer Viruses: Theory and Practice*, vol. 4, (1987), pp. 22-35.
- [10] N. T. Bailey, "Mathematical theory of infectious diseases and its applications", Hafner Press, New York, (1975).
- [11] D. J. Daley and J. Gani, "Epidemic modeling: an introduction", Cambridge University Press, (2001).
- [12] W. O. Kermack and A. G. McKendrick, "A contribution to the mathematical theory of epidemics", in: Proceedings of the Royal Society of London Series, vol. 115, no. 772, (1927), pp. 700-721.
- [13] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses", in: Proceedings of the IEEE Symposium on Security and Privacy, California, USA, (1991) May, pp. 343-361.
- [14] S. Staniford, V. Paxson and N. Weaver, "How to own the Internet in your spare time", in: Proceedings of the 11th USENIX Security Symposium, (2002) August, pp. 149-167.
- [15] D. Moore, "Caida analysis of Code-Red", in: Technical Report of the Cooperate Association for Internet Data Analysis, (2001).
- [16] N. Weaver, I. Hamadeh, G. Kesidis and V. Paxson, "Preliminary Results using scale-down to explore worm dynamics", in: Proceedings of the ACM Workshop on Rapid Malcode (WORM '04), Washington DC, USA, (2004), pp. 65-72.
- [17] K. Rhoades, Code Red I, Code Red II and SirCam, "Attacks highlight need for proactive measures", Available online: <<http://www.gao.gov/new.items/d011073t.pdf>>, (2001).
- [18] D. Moore, "Inside the slammer worm", *IEEE Security and Privacy*, vol. 1, no. 4, (2003), pp. 33-39.
- [19] Z. Chen, L. Gao and K. Kwiat, "Modeling the spread of active worms", in: Proceedings of IEEE INFOCOM, San Fransisco, (2003), pp. 1890-1900.
- [20] G. Yan and S. Eidenbenz, "Modeling propagation dynamics of bluetooth worms", *IEEE Transaction on Mobile Computing*, vol. 8, no. 3, (2009), pp. 353-368.
- [21] X. Fan and Y. Xiang, "Modeling the propagation of peer-to-peer worms", *Future Generation Computer Systems*, vol. 26, no. 8, (2010), pp. 1433-1443.
- [22] C. C. Zou, D. Towsley and W. Gong, "Modeling and simulation study of the propagation and defense of Internet email worms", *IEEE Transaction on Dependable and Secure Computing*, vol. 4, no. 2, (2007), pp. 105-118.
- [23] H. Andersson and T. Britton, "Stochastic epidemic models and their statistical analysis", *Springer Lecture Notes in Statistics*, vol. 4, (2000).
- [24] Z. Chen, C. Chen and C. Ji, "Understanding localized-scanning worms", in: IEEE International Performance, Computing, and Communication. Conference (IPCCC), (2007), pp. 186-193.
- [25] W. Yu, X. Wang, P. Calyam and D. Xuan, "On detecting camouflaging worm", in: IEEE Computer Security Applications Conference, (ACSAC'06), (2006), pp. 235-244.
- [26] B. K. Mishra and D. K Saini, "Mathematical models on computer virus", *Applied Mathematics and Computation*, vol. 187, no. 2, (2007), pp. 929-936.
- [27] P. Yan and S. Liu, "SEIR epidemic model with delay, *J. Aust. Math. Soc. Series B – Applied*", *Mathematics*, vol. 48, no. 1, (2006), pp. 119-134.
- [28] B. K. Mishra and N. Jha, "Fixed period of temporary immunity after run of anti-malicious software on computer nodes", *Applied Mathematics and Computation*, vol. 190, no. 2, (2007), pp. 1207-1212.
- [29] S. Fei, L. Zhao-Wen and M. Yan, "Modeling and Analysis of worm propagation in Internet", *The Journal of China universities of Post and Telecommunications*, vol. 17, no. 4, (2010), pp. 63-68.
- [30] S. Kondakci, "Epidemic state analysis of computers under malware attacks", *Simulation Modeling Practice and theory*, vol. 16, (2008), pp. 571-584.
- [31] A. Kamra, H. H. Feng, V. Mishra and A. D. Keromytis, "The effect of DNS delays on worm propagation in an IPv6 Internet", in: Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'05), Miami, FL, USA, (2005), pp. 2405-2414
- [32] O. A. Toutonji, S. Yoo and M. Park, "Stability analysis of VEISV propagation modeling for network worm attack", *Applied Mathematical Modeling*, vol. 36, (2012), pp. 2751-2761.
- [33] Y. Yao, "Hopf bifurcation in an Internet worm propagation model with time delay in quarantine", *Mathematical and Computer Modeling*, vol. 57, no. 11, (2011), pp. 2635-2646.