SIQRS MODEL TO CONTROL TRANSMISSION OF MALICIOUS OBJECTS IN COMPUTER NETWORK

Prasant Kumar Nayak[1], Bimal Kumar Mishra[2], Srimanta Kumar Mahaptra[3]

Abstract: ***Thresholds, equilibria, and their stability are found for susceptible (S) – infectious (I) - quarantined (Q) - anti-malicious software treated nodes (R) epidemic model for the transmission of malicious objects in computer network with a non-linear incidence rate. It has been shown that if the basic reproduction number*** $R_0 < 1$ ***, the disease-free equilibrium is asymptotically stable and the endemic equilibrium does not exist. Numerical methods are employed to solve and simulate the system of equations developed. Effect of quarantine nodes on S, and I class along with the dynamical behavior of the system with different parametric values is analyzed.***

Keywords: malicious objects; quarantine; non-linear incidence rate; global stability.

AMS classification: 92D30 (Primary), 34D23 (Secondary)

1. INTRODUCTION

A year or two ago, most malware was spread via e-mail attachments, which resulted in mass outbreaks like Bagle, Mydoom and Warezov. Nowadays sending .EXE attachments in e-mail doesn't work so well for the criminals because almost every company and organization is filtering out such risky attachments from their e-mail traffic.

The criminals' new preferred way of spreading malware is by drive-by downloads on the Web. These attacks often still start with an e-mail spam run but the attachment in the e-mail has been replaced by a web link, which takes you to the malicious web site. So instead of getting infected over SMTP, you get infected over HTTP. It is predicted that the total number of viruses and Trojans will pass the one million mark by the end of 2008 [23].

Transmission of malicious objects in computer network is epidemic in nature. Malicious object is a code that infects computer systems. There are different kinds of malicious objects such as: Worm, Virus, Exploit, Denial of Service (DoS), Flooder, Sniffer, Spoofer, Trojan etc., which differ according to the way they attack computer systems and the malicious actions they perform.

To control the spread of malicious codes, the nodes which are highly infected by the malicious objects in the computer network, are kept in isolation for some time. This helps us to reduce the transmission of infection to susceptible nodes. Isolation most probably was the first infection control method in human disease and was successful in controlling many of the epidemic diseases. The word *quarantine* means to say about the forced isolation or stoppage of interaction with others. Same concept has been used in computer world.

In the SIQRS model for infections that don't confer immunity, susceptible nodes first goes through a latent period (and is said to become exposed) after infection before becoming infectious, thereafter some infected nodes stay in the I class while they are infectious and then move to the Anti-malicious software treated nodes class R upon temporary recovery after the run of anti malicious software. Other infected nodes are transferred into the quarantine class Q while they are infectious and then move to the R class. Since in the cyber world the acquired immunity is not permanent, the recovered nodes return back to the susceptible class. The schematic diagram for the flow of malicious objects in the computer network is depicted in Figure 1.

We assume the population has a homogeneous spatial distribution and the mixing of hosts follow the *law of mass action*. More specifically, we assume that the local density of the total population is a constant though the total population size $N(t) = S(t) + I(t) + Q(t) + R(t)$ may vary with time. Here $S(t), I(t), Q(t), R(t)$ denote the sizes of S, I, Q, R classes at any time t, respectively. The per capita contact rate β, which is the average number of effective contacts with other nodes per unit time is assumed to be a constant.

Since the malicious objects differ in their attacking behavior, a non-linear incidence rates can give a reasonable qualitative description of the disease dynamics. Many authors have developed mathematical models with non-linear incidence rate [8, 18, 24-30, 31,32]. Feng and Thieme [20, 21, and 22] considered SIQR models with arbitrary distributed periods of infection including quarantine and a general form for incidence term with a preliminary assumption that all individuals must go through the quarantine class. They proved extinction and persistence results and found minimum quarantine periods in order to make the endemic equilibrium unstable. Hethcote et al [6] studied the effect of quarantine in various endemic models with different form of incidence. For SIQR endemic models Wu and Feng [11] showed that an epidemic approximation near $R_0 = 1$ can have a homoclinic bifurcation, so that some perturbation of the original model might also have a homoclinic bifurcation. Several authors studied the global stability of several epidemiological models [5, 7,9, 10, 13, 12,14, 15, and 19]. Mishra et al [1-4] has studied epidemic models on the transmission of malicious objects in computer network.

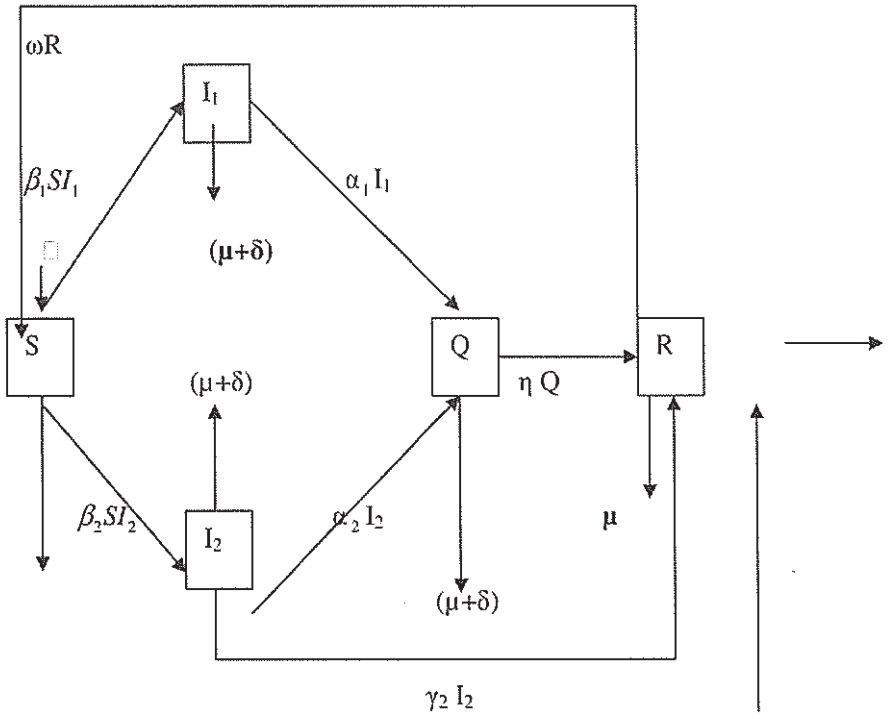
In a certain sense, the propagation of virtual malicious objects in a system of interacting computers could be compared with a disease transmitted by vectors when dealing with public health. Concerning diseases transmitted by vectors, one has to take into account that the parasites spend part of its lifetime inhabiting the vector, so that the infection switches back and forth between host and vector. Anderson and May [16, 17] discussed the spreading nature of biological viruses, parasites etc. leading to infectious diseases in human population through several epidemic models.

Predicting malicious objects outbreak is extremely difficult due to human nature of the attacks but more importantly, detecting outbreaks early with a low probability of

false alarms seems quite difficult. By developing models it is possible to characterize essential properties of the attacks.

2. MATHEMATICAL MODEL FORMULATION

A population size N (t) is partitioned into subclasses of nodes which are susceptible, exposed (infected but not yet infectious), infectious, quarantined, and anti-malicious software-treated nodes (nodes which are treated with anti-malicious software), with sizes denoted by $S(t), I(t), Q(t), R(t)$ respectively. Our assumptions on the dynamical transfer of the population are depicted in the Figure 1.



The SIQRS model equations are given as follows:

$$
\begin{aligned}
S'(t) &= A-(\beta SI_1+\beta SI_2)-\mu S+\omega R \\
I_1'(t) &= \beta SI_1-(\mu+\alpha_1+\gamma_1+\delta)I_1(t) \\
I_2'(t) &= \beta SI_2-(\mu+\delta+\gamma_2+\alpha_2)I_2(t) \\
Q'(t) &= \alpha_1 I_1+\alpha_2 I_2-(\mu+\delta+\eta)Q(t) \\
R'(t) &= \gamma_1 I_1+\gamma_2 I_2+\eta Q(t)+-(\mu+\omega)R(t)
\end{aligned}
\qquad (1)
$$

Table 1.Notations and initial values of the model

Notation	Explanation	Initial value
N(t)	Total number of nodes under consideration	10,000
S(t)	Number of susceptible nodes at time t	S(0)= 9,300
$I_1(t)$	Number of low infected nodes at time t	$I_1(0)$=400
$I_2(t)$	Number of high infected nodes at time t	$I_2(0)$=300
Q(t)	Number of removed hosts from the Infected nodes at time t	Q(0)=0
R(t)	Number of removed hosts from the infectious population at time t	R(0)=0
β_1	per capita contact rate	β_1= 0.03
β_2	per capita contact rate	β_2=0.02
Λ	rate at which new nodes are attached to the network	Λ=0.01
μ	Natural death rate	μ=0.025
δ	Death rate due to attack	δ=0.01
γ_1	rates at which nodes leave the I_1 class to R class	γ_1=0.17
γ_2	the rates at which nodes leave I_2 class to R	γ_2=0.10
α_1	rates at which nodes leave the I_1 class to Q class	α_1=
ξ	the rates at which nodes leave isolated classes	ξ= 0.325
α	the rate at which the nodes leave the infectious class and directly enters the recovered class after treatment of antivirus software	α =0.005
η	is the rate at which the nodes leaves the recovered class and enters the susceptible class	η=0.1

where A is the recruitment rate of susceptible nodes to the computer network, p is the fraction of recruited nodes which are given anti-malicious software treatment, μ is the per capita natural mortality rate (that is the crashing of nodes due to the reason other than the attack of malicious objects), α is the rate constant for nodes leaving the infective compartment I for quarantine compartment, δ is the disease related death rate (crashing of nodes due to the attack of malicious objects) constant in the

compartments I and Q; γ, η are the rates at which nodes recover temporarily after the run of anti malicious software and return to class Am from compartments I and Q respectively; ω is the rate at which the anti-malicious software effect wanes.

In this SIQRS model, the flow is from the S class to the I class, and then directly to the Am class or to the Q class and then to the Am class and as the recovery is not permanent in the cyber world, it again returns back to the S class.

The total population size N (t) is variable with $N^{'}(t) = A - \mu N - \delta(I(t) + Q(t))$. In the absence of the attack of malicious objects, the population size of the node N approaches the carrying capacity A/μ.

The differential equation for N implies that solution of (1) starting in the positive orthan R_5^+ either approach, enter or remain in the epidemiologically meaningful subset

$$D = \{(S, I, Q, R)/S \geq 0, I \geq 0, Q \geq 0, R \geq 0, S + I + Q + R \leq A/\mu\}$$

Thus it suffices to consider solutions in region D. Solutions of the initial value problem starting in D and defined by (1) exist and are unique on maximal interval [9].Since solution remain bounded in the positively invariant region D, the maximal interval is $[0, \infty)$ .Thus initial value problem is well posed both mathematically and epidemiologically.

To eliminate R (t) from the equations in (1), we use

$$R(t) = \frac{A}{\mu} - S(t) - I(t) - Q(t)$$

The reduced model is:

$$S^{'}(t) = (1-p)A - \frac{\beta SI}{\varphi(I)} - \mu S(t) + \omega\left[\frac{A}{\mu} - S(t) - I(t) - Q(t)\right]$$

$$I^{'}(t) = \frac{\beta SI}{\varphi(I)} - (\mu + \alpha + \gamma + \delta)I(t) \qquad (2)$$

$$Q^{'}(t) = \alpha I(t) - (\mu + \delta + \eta)Q(t)$$

Let, $N_1 = S(t) + I(t) + Q(t)$

From the above equations, it can be seen that, in the absence of the disease (I = 0, Q = 0)

$$N_1 \to \frac{[\mu(1-p)+\omega]A}{\mu(\mu+\omega)}$$

3. EXISTENCE AND STABILITY OF EQUILIBRIA

In this section we try to investigate the model (2) to find its equilibria and study its stability. The steady states of model (2) are given as:

$$\begin{aligned}
&(1-p)A-\frac{\beta SI}{\varphi(I)}-\mu S(t)+\omega\left[\frac{A}{\mu}-S(t)-I(t)-Q(t)\right]=0\\
&\frac{\beta SI}{\varphi(I)}-(\mu+\alpha+\gamma+\delta)I(t)=0 \qquad (3)\\
&\alpha I(t)-(\mu+\delta+\eta)Q(t)=0
\end{aligned}$$

System (3) has always the disease-free equilibrium $P_o=\left(\frac{[\omega+\mu(1-p)A]}{\mu(\mu+\omega)},0,0,0\right)$

Let,

$$R_0=\frac{\beta[\mu(1-P)+\omega]}{\mu(\mu+\omega)\mu(\mu+\gamma+\alpha)}A$$

The linearization of model (2) at the equilibrium P_0 has a characteristic equation which has always a negative eigenvalue $\lambda=-\mu-\omega,-\mu$

The other eigenvalues of the characteristic equation is determined by the equation

$$\lambda^2+(2\mu+2\delta+\eta+\gamma+\alpha)\lambda+\mu(\mu+\delta+\gamma+\alpha)-\frac{\beta[\omega+\mu(1-P)]}{\mu(\mu+\omega)}A=0 \qquad (4)$$

Thus all roots of (4) have negative real parts if and only if

$$\mu(\mu+\delta+\gamma+\alpha)-\frac{\beta[\omega+\mu(1-P)]}{\mu(\mu+\omega)}A>0$$

$that\ is, R_0<1.$

If $R_0 = 1$, one eigenvalue is zero and if $R_0 > 1$, one root has positive real parts.

Lemma 1: *If $R_0 < 1$, the disease-free equilibrium P_0 is locally asymptotically stable. If $R_0 = 1$, P_0 is stable; If $R_0 > 1$, P_0 is unstable.*

Let, $f_\infty = \lim_{t\to\infty} \inf_{\theta\geq t} f(\theta)$

$f^\infty = \lim_{t\to\infty} \sup_{\theta\geq t} f(\theta)$

Lemma 2: *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, $lim_{k\to\infty} f'(t_k) = 0$.*

Theorem 1: *If $R_0 < 1$, then the disease-free equilibrium P_0 is globally asymptotically stable.*

Theorem 2: *If $R_0 > 1$, then the system (2) has a unique equilibrium* P*(S*, E*, I*, Q*) *which is locally asymptotically stable.*

4. NUMERICAL METHODS AND DISCUSSION

The dynamical behavior of SIQRS has been investigated for the transmission of malicious objects in computer network. Global stability of the unique endemic equilibrium for the epidemic model has been established.

Runge-Kutta Fehlberg fourth-fifth order method is employed to solve the system (1) and the behavior of the susceptible, exposed, infectious, and quarantined nodes with respect to time are observed which is depicted in Figure 2. From Figure 2 (plotted in MAPLE), we observe that the system is asymptotically stable.

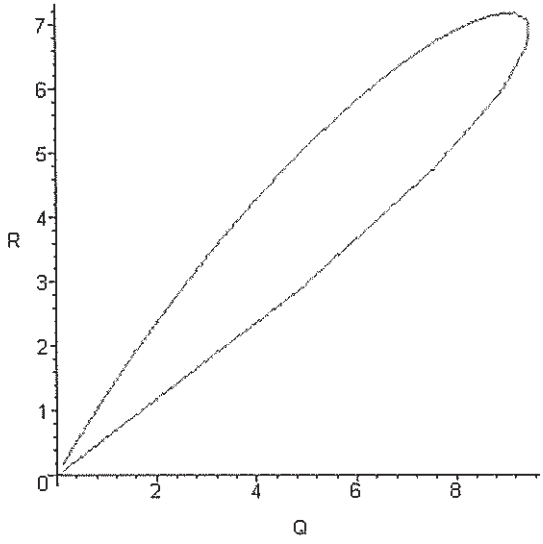


Figure 2: Effect of Quarantine nodes Q on recovered nodes R

5. REFERENCES

1. Proffesor Bimal Kumar Mishra , Navnit Jha, Fixed period of temporary immunity after run of anti-malicious objects software on computer nodes, Applied Mathematics and Computation, 190, 2007. pp,1207-1212.
2. Bimal Kumar Mishra et al, Differential susceptibility-infectiousness epidemic model of propagation of malicious objects with self-replication in a computer network, Applied Mathematics and Computation, To appear, doi: 10.1016/j.amc.2007.03.052
3. Bimal Kumar Mishra, D.K Saini, SEIRS epidemic model with delay for transmission of malicious objects in computer network, Applied Mathematics and Computation, 188, 2007.pp,1476-1482,
4. Bimal Kumar Mishra, Dinesh Saini, Mathematical models on computer viruses, Applied Mathematics and Computation, 187, 2007.pp,929-936.
5. D. Greenhalgh, Hopf bifurcation in epidemic models with a latent period and non-permanent immunity, Math. Comp. Modelling, 25, 1997.pp,85-107.
6. H. Hethcote, M. Zhein, L. Shengbing, Effects of quarantine in six endemic models for infectious diseases, Math. Biosc. 180, 2002.pp, 141-160.
7. H. W. Hethcote, H. W. Stech, P. van den Driessche, Periodicity and stability in epidemic in epidemic models: a survey, In Diff. Eqns. And Applications in Ecology, Epidemics and Population problems, K. L. Cook (ed.), Academic Press, N. York, 1981,pp, 65-85.
8. H. W. Hethcote, P. van den Driessche, Some epidemiological models with nonlinear incidence, J. Math. Bio. 29 , 1991.pp, 271-287.
9. J. K. Hale, Ordinary Differential Equations, 2nd ed, Krieger, Basel, 1980
10. K. L. Cook, P. van den Driessche, Analysis of SEIRS epidemic model with two delays, J. Math. Bio. 35 , 1996.pp, 240-260.
11. L. I. Wu, Z. Feng, Homoclinic bifurcation in an SIQR model for childhood disease, J. Diff. Eq. 168, 150, 2000
12. M. E. J. Newman, Stephanie Forrest, and Justin Balthrop, Email networks and the spread of computer viruses, Physical Review E 66, 035101-4,2002
13. M. Y. Li, J. R. Graff, L. C. Wang, J. Karsai, Global dynamics of a SEIR model with a varying total population size, Math. Biosc. 160 , 1999.pp, 191-213.
14. M. Y. Li, J. S. Muldowney, Global stability for the SEIR model in epidemiology, Math. Biosc. 125 , 1995.pp155-164.
15. M. Y. Li, L. Wang, Global stability in some SEIR epidemic models, In Mathematical approaches for emerging and reemerging infectious diseases: Models, methods and theory, C. C. Chavez, S. Blower, P van den Driessche, D. Kirscner, and A. A. Yakubu (Eds), Springer, Vol 126 , 2002.pp, 295-312.
16. R. M. Anderson, R. M. May, Infectious diseases of Humans, Dynamics and Control, Oxford University Press, Oxford, 1992
17. R. M. Anderson, R. M. May, Population Biology of infectious disease I, Nature 180, 1999.pp, 361-367.
18. S. Ruan, W. Wang, Dynamical behavior of an epidemic model with a non linear incidence rate, Journal of Differential Equations 188, 2003pp135-163,
19. Y. Michael, H.Smith, L.Wang, Global dynamics of SIER epidemic model with vertical transmission, SIAM Journal of Applied Mathematics 62(1), 58-69, 2001
20. Z. Feng, H. R. Thieme, Endemic models with arbitrarily distributed periods of infection, I: General theory, SIAM J. Appl. Math. 61, 803, 2000
21. Z. Feng, H. R. Thieme, Endemic models with arbitrarily distributed periods of infection, II: Fast disease dynamics and permanent recovery, SIAM J. Appl. Math. 61, 983, 2000
22. Z. Feng, H. R. Thieme, Recurrent outbreaks of childhood disease revisited: The impact of isolation, Math. Biosc. 128, 93,1995
23. http://www.f-secure.com/f-secure/pressroom/news/fsnews_20080331_1_eng.html, March31, 2008
24. V. Capasso, G. Serio, A generalization of the Kermack-McKendrick deterministic epidemic model, Math. Biosci., 42, 1978.pp, 43-61.

25. D. Xiao, S. Ruan, Global Analysis of an Epidemic Model with Nonmonotone Incidence Rate, Math. Biosci., 208, 2007pp. 419-429.
26. T. Zhang, Z. Teng, Pulse vaccination delayed SEIRS epidemic model with saturation incidence, Appl. Math. Model., (2007), doi:10.1016/J. apm. 2007.06.005.
27. H. W. Hethcote, The mathematics of infectious diseases, SIAM Rev., 42, 2000.pp, 599-653.
28. P. van den Driessche, J. Watmough, A simple SIS epidemic model with a backward bifurcation, J. Math. Biol., 40, 525-540, 2000.
29. M. E. Alexander, S. M. Moghadas, Periodicity in an epidemic model with a generalized nonlinear incidence, Math. Biosci., 189, , 2004.pp, 75-96.
30. M. E. Alexander, S. M. Moghadas, Bifurcation analysis of an SIRS Epidemic model with generalized incidence, SIAM J. Appl. Math., 65, 2005.pp, 1794-1816.
31. R. S. Varga, Matrix iterative analyasis, Englewood cliffs, N. J: Prentice – Hall Inc., 1962.
32. Li-Ming Cai, Xue Zhi Li, Analysis of a SEIV epidemic model with a nonlinear incidence rate, Appl. Math. Modelling, doi: 10.1016/j.apm.2008.01.005, 2008

****

[1]*Department of Mathematics, C.V.Raman college of engineering., Bhubaneswar, Orissa, 752054*
[2]*Department of Applied Mathematics, Birla Institute of Technology, Mesra, Ranchi, India – 835 215*
[3]*I B M India Pvt Ltd , Pune India 411028*