Mathematical Models on Cyber Attack

Bimal Kumar Mishra, Ph. D., D.Sc.
Department of Applied Mathematics
Birla Institute of Technology,
Mesra, Ranchi – 835 215
Email: drbimalmishra@gmail.com

PUBLICATIONS (75)

- **International Journals: 54**
- **National Journals: 05**
- **Conference Proceedings: 16**
- **Research Area:**
  Mathematical Models on
  Cyber Attack and Defense
  Blood Flow

Attack by malicious objects in computer network are EPIDEMIC in nature

Malicious objects:

COMPUTER VIRUS
COMPUTER WORMS
TROZAN HORSE
SNIFFERS
Denial of Service (DoS)
FLOODER etc.

Basic Terminologies:

Computer virus is a program that can "infect" other programs by modifying them to include a possibly evolved version of it. With this infection property, a virus can spread to the transitive closure of information flow, corrupting the integrity of information as it spreads.

Basic Terminologies:

Self replicating virus may be defined as “A software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the same computer; "a true virus cannot spread to another computer without human assistance.

- **Anti-malicious software**

is a class of program that searches our hard drive and floppy disks for any known or potential viruses. This is also known as a "virus scanner." As new viruses are discovered by the antivirus vendor, their binary patterns are added to a signature database that is downloaded periodically to the user's antivirus program via the web.

Analogous to Biological Epidemic diseases like:

MALARIA

SARS

HIV etc.

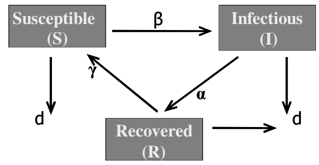
Various epidemic models

SIR

SIS

SEIR etc.

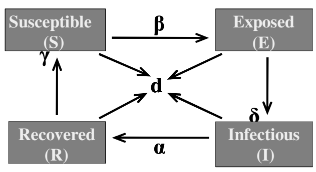
The SIRS Model



The System of Differential Equations for SIRS Model

$$\frac{dS}{dt} = -\beta SI - dS + \gamma R$$
$$\frac{dI}{dt} = \beta SI - \alpha I - dI \qquad \textbf{(1)}$$
$$\frac{dR}{dt} = \alpha I - \gamma R - dR$$

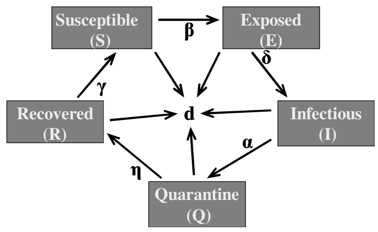
The SEIRS Model



The System of Differential Equations for SIRS Model

$$\frac{dS}{dt} = -\beta SI - dS + \gamma R$$
$$\frac{dE}{dt} = \beta SI - \delta E - dE$$
$$\frac{dI}{dt} = \delta E - \alpha I - dI \qquad (2)$$
$$\frac{dR}{dt} = \alpha I - \gamma R - dR$$

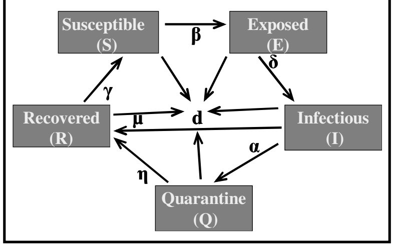
The SEIQRS Model (1)



The System of Differential Equations for SEIQRS Model (1)

$$\frac{dS}{dt} = -\beta SI - dS + \gamma R$$
$$\frac{dE}{dt} = \beta SI - \delta E - dE$$
$$\frac{dI}{dt} = \delta E - \alpha I - dI \qquad (3)$$
$$\frac{dQ}{dt} = \alpha I - \eta Q - dQ$$
$$\frac{dR}{dt} = \eta Q - \gamma R - dR$$

The SEIQRS Model (2)



The System of Differential Equations for SEIQRS Model (2)

$$\frac{dS}{dt} = -\beta SI - dS + \gamma R$$
$$\frac{dE}{dt} = \beta SI - \delta E - dE$$
$$\frac{dI}{dt} = \delta E - \alpha I - \mu I - dI \qquad (4)$$
$$\frac{dQ}{dt} = \alpha I - \eta Q - dQ$$
$$\frac{dR}{dt} = \eta E - \gamma R + \mu I - dR$$

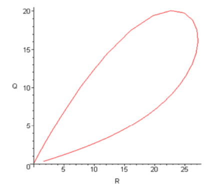
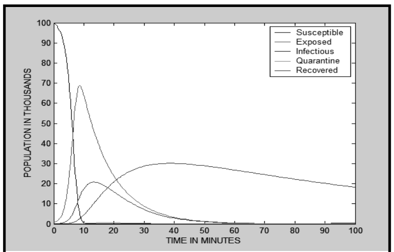


Figure 3: Effect of Quarantine Q on Recovered Nodes R.



Time series of susceptible population, S(t), E(t), I(t), Q(t) and R(t) for the system

SIR

ASSUMPTIONS:

(i)

An average infective nodes makes contact sufficient to transmit infection of malicious codes with **βN** others per unit time, where **N** represents the total nodes in the computer network, that is, population size and **β** is called the **infectious contact rate**, that is the rate of infection per susceptible and per infective.

SIR contd.

According to (i),

Since the prob. that a random contact by an infective is with a susceptible, who then can transmit infection, is **S / N**, the number of new infections in unit time is

(βN)(S / N)I= βSI.

Thus, $S' = -\beta SI$

SIR contd.

Note:

For the nodes which are infected my malicious codes recover when anti-malicious software is run, that is recover with immunity,

N = S + I + R

SIR contd.

(ii)

A fraction α of infectives leave the infective class per unit time.

(iii)

There is no entry into or departure from the population, except possibly through death from the infection due to malicious codes.

SIR contd.

- Based on our assumption, we have the following system of equations:

$$S' = -\beta SI$$
$$I' = \beta SI - \alpha I \quad (1)$$
$$R' = \alpha I$$

SIR contd.

THRESHOLD PARAMETER

In our model R is determined once S and I are known, and we can drop the R' equation from our model, that is, in (1) leaving the system of equations

$$S' = -\beta SI$$
$$I' = (\beta S - \alpha)I \quad (2)$$

SIR contd.

Analytical solution is not possible. We try to study the behavior of the solution by qualitative approach.

$$\because S' < 0, \forall t$$
$$I' > 0 \quad iff \quad S > \alpha/\beta$$

Thus I increases so long as

$$S > \alpha/\beta$$

SIR contd.

but since S decreases for all t, I ultimately decrease and approaches zero.

If $S(0) < \alpha/\beta$,I decreases to zero (**no epidemic**),

While if $S(0) > \alpha/\beta$

I first increases to a maximum attained when $S = \alpha/\beta$

and then decreses to zero **(epidemic).**

SIR contd.

The quantity $\dfrac{\beta S(0)}{\alpha}$ is a **threshold quantity**,

called the **basic reproductive number** and denoted by R0.

- If R0 < 1 the infection dies out.
- While if R0 > 1 there is an epidemic.

SIR contd.

We divide the two equations (1) of the model to give

$$\frac{I'}{S'} = \frac{dI}{dS} = \frac{(\beta S - \alpha)I}{-\beta SI} = -1 + \frac{\alpha}{\beta S}$$

and integrate to find the orbits (curve in the S–I plane)

$$I = -S + \frac{\alpha}{\beta}\ln S + c \quad \textbf{(3)}$$

with c as an arbitrary constant of integration.

SIR contd.

We define a function

$$V(S,I) = S + I - \frac{\alpha}{\beta}\ln S \qquad (4)$$

and the curve is given implicitly by the equation V(S, I) = c, for some of the constant c.
c is determined by the initial values S0, I0 of S and I respectively, because

$$c = V(S_0, I_0) = S_0 + I_0 - \alpha/\beta \ln S_0 \quad (5)$$

SIR contd.

Let us think a population of nodes of size K into which a small number of infective nodes is introduced, so that

$$S_0 \approx K, I_0 \approx 0, \quad and \quad R_0 = \beta K/\alpha$$

If we use the fact that

$$\lim_{t\to\infty} I(t) = 0, and \quad let \quad S_\infty = \lim_{t\leftarrow\infty} S(t)$$

then the relation

$$V(S_0, I_0) = V(S_\infty, 0)$$

SIR contd.

gives

$$K - \frac{\alpha}{\beta}\ln S_0 = S_\infty - \frac{\alpha}{\beta}\ln S_\infty \qquad (6)$$

$$\frac{\beta}{\alpha} = \frac{\ln \frac{S_0}{S_\infty}}{K - S_\infty} \qquad (7)$$

We note that $0 < S_\infty < K$

that is, a part of the population escapes infection.

SIR contd.

The maximum number of infectives at any time is the number of infectives when

$I' = 0$

that is, when $S = \alpha/\beta$

Thus maximum is given by

$$I_{\max} = S_0 + I_0 - \frac{\alpha}{\beta}\ln S_0 - \frac{\alpha}{\beta} + \frac{\alpha}{\beta}\ln\frac{\alpha}{\beta}$$

Obtained by substituting

$S = \alpha/\beta, I = I_{\max}$, into (2)

SEIRS Epidemic model

Assumptions:

- Any new node attached to the computer network is susceptible
- Death rate of the nodes other than attack of malicious object is constant and is same throughout the population
- Death rate of the infective nodes due to attack of malicious object is constant

SEIRS contd.

- Latent period ω and immune period τ is constant
- Waiting time in the infective, exposed and recovered class is exponentially distributed
- When a node is removed from the infected class, it recovers *temporarily*, acquiring *temporary* immunity with probability p and dies from the attack of malicious object with probability (1-p).

Simple SEIRS epidemic model

$$\frac{dS}{dt} = -\beta IS$$

$$\frac{dE}{dt} = \beta IS - \delta E$$

$$\frac{dI}{dt} = \delta E - \gamma I$$

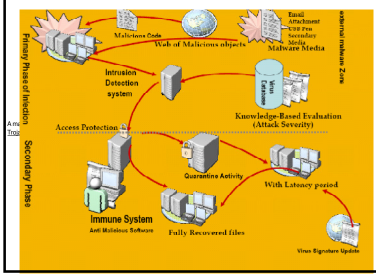
$$\frac{dR}{dt} = \gamma I$$

MATHEMATICAL MODELS ON INTERACTION BETWEEN COMPUTER VIRUS AND ANTIVIRUS SOFTWARE INSIDE A COMPUTER SYSTEM

Attempt has been made to develop mathematical models on interaction between computer virus and antivirus software inside a computer system. The basic reproductive ratio in the absence and presence of the immune system has been found and the criterion of spreading the computer virus is analyzed in Models 1 and 2. An analysis is also made for the immune response to clear the infection.

Effect of new or updated antivirus software on such viruses which are suppressed (quarantine) or not completely recovered by the lower version of installed antivirus software in the system is studied in model 3 and it has been shown that the number of infected files falls exponentially when new or updated antivirus software is run. Reactivation of computer virus when they are in the latent class is mathematically formulated and basic reproductive ratio is obtained in Model 4.

A mathematical model has also been developed to understand the recent attack of the malicious object Backdoor.Haxdoor.S and Trojan.Schoeberl.E and its removal by newly available tool FixSchoeb-Haxdoor in Model 5.



Model 1: Primary phase of an Infection

Viruses get entry to the computer node via various means (emails, infected disks etc.) and hijack various files (command files, executable files, kernel.dll, etc.) in the node for its own replication. It then leaves a specific file and the process is repeated. Viruses may be of different nature and as per their mode of propagation; they target different file types of the attacked computer for this purpose.

- As per the assumptions, the model is described by the system

$$\frac{dV}{d\tau} = aY - bV$$
$$\frac{dX}{d\tau} = c - dX - \beta XV \qquad (1)$$
$$\frac{dY}{d\tau} = \beta XV - fY$$

The relationship between the computer virus and uninfected file is analogous to the relationship between predator and prey as given in the classical work of Lotka-Volterra [3, 4].

- Let X be the number of uninfected files (prey) and V be the number of computer virus (predators) [8] Then,
- {Rate of change of X}= {net rate of growth of X without predation}-{rate of loss due of X to predation, and
- {Rate of change of V}= {net rate of growth of V due to predation}-{net rate of loss of V without prey}

- Let, R0 be the basic reproductive ratio for the computer virus; defined to be the expected number of viruses that one virus gives rise to an uninfected file population. A virus gives rise to infected files at a rate βX for a time 1/b, and each infected files gives rise to virus (self replication) at a rate *a* for a time 1/f. since X=c/d for a uninfected population,

$$R_0 = \frac{\beta ca}{dbf}$$

The criterion for the spread of the computer virus is $R_0>1$

We non-dimensionalise the system (1) by defining

$$x=\frac{d}{c}X,\ y=\frac{d}{c}Y,\ v=\frac{bf}{ac}V,\ t=d\tau$$

$$\varepsilon\frac{dv}{dt} = \alpha y - v$$
$$\frac{dx}{dt} = 1 - x - R_0 xv \qquad (4)$$
$$\frac{dy}{dt} = R_0 xv - \alpha y$$

where

For typical parameter values $\varepsilon << 1$.

$S_0 = (0,1,0)$

The steady states of the non-dimensionalised system (4) are

And S* =(v*,x*,y*) where V*= 1-1/R, x*= 1/R, y*=1/*a(1-1/Ro)*

Where $\varepsilon = \frac{d}{b}, \alpha = \frac{f}{d}$ (5)

For typical parameter values $\varepsilon << 1$.

The steady states of the non-dimensionalised system (4) are $S_0 = (0,1,0)$

,the uninfected steady state, and $S^* = (v^*, x^*, y^*)$ Where

$$v^* = 1 - \frac{1}{R_0}, x^* = \frac{1}{R_0}, y^* = \frac{1}{\alpha}(1 - \frac{1}{R_0}) \quad (6)$$

For $R_0 > 1$,the normal situation, $(v(t), x(t), y(t)) \rightarrow (v^*, x^*, y^*)\ as \quad t \rightarrow \infty$

The susceptible population X (uninfected files) is reduced by the attack until each virus is expected to give rise to exactly one new virus, $R_0 x^* = 1$

This we assume as the primary phase of an infection.

Model II: Secondary Phase of Infection (Effect of Immune system)

We assume the response of the immune in the computer system due to antivirus software Z which are run at a constant rate g and h being the death rate of antivirus software (which mean to say that the antivirus software is incapable to identify the attack of new viruses). The antivirus software cleans the infected files at a rate. There is an analogy here of Z antivirus software as predators and Y infected files as prey. We take linear functional response of Z

$$\frac{dV}{d\tau} = aY - bV$$

$$\frac{dX}{d\tau} = c - dX - \beta XV$$

(7)

$$\frac{dY}{d\tau} = \beta XV - fY - \gamma YZ$$

$$\frac{dZ}{d\tau} = g - hZ$$

The non-dimensionalisation of the system is done as what we have done in Model 1, with

$z = \frac{hZ}{g}$

in addition, we get,

$$\varepsilon \frac{dv}{dt} = \alpha y - v$$

$$\frac{dx}{dt} = 1 - x - R_0 xv$$

(8)

$$\frac{dy}{dt} = R_0 xv - \alpha y - \kappa yz$$

$$\frac{dz}{dt} = \lambda(1 - z)$$

Where

$$\lambda = \frac{h}{d}, \kappa = \frac{\gamma g}{dh}$$

(9)

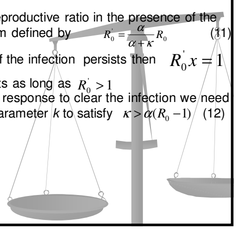
The steady states of the non-dimensionalised system (8) are $S_0 = (0,1,0,1)$, the uninfected steady state, and $S^* = (v^*, x^*, y^*, z^*)$

$$v^* = \frac{\alpha}{\alpha + \kappa}(1 - \frac{1}{R_0'})$$

$$x^* = \frac{1}{R_0'}$$

$$y^* = \frac{1}{\alpha + \kappa}(1 - \frac{1}{R_0'}) \quad (10)$$

$$z^* = 1$$



Let Ro be the basic reproductive ratio in the presence of the immune system defined by $R_0' = \frac{\alpha}{\alpha + \kappa} R_0$ (11)

Then we observe that if the infection persists then $R_0' x = 1$

and the infection persists as long as $R_0' > 1$

In order for the immune response to clear the infection we need the immune response parameter *k* to satisfy $\kappa > \alpha(R_0 - 1)$ (12)

Model III: Effect of new antivirus software on such viruses which are suppressed (quarantine)

We assume a case where the viruses are not completely cleaned (quarantine) from the infected files on run of installed antivirus software on the computer node. For the complete recovery of infected files from viruses, updated version of antivirus has to be run. Further we assume that such updated antivirus software is available and is 100% efficient. This antivirus software switches β to zero and thus the equations for the subsequent dynamics of the infected files and free virus from equation (1) is expressed as

---

$$\frac{dV}{d\tau} = aY - bV$$

$$\frac{dX}{d\tau} = c - dX \quad (13)$$

$$\frac{dY}{d\tau} = -fY$$

We further assume that the half-life of the virus is much less than that of the virus producing files. Then,

$$Y = Y_0 e^{-ft}$$

$$V = \frac{V_0 (be^{-ft} - fe^{-bt})}{(b - f)} \qquad (14)$$

From equation (14) we are able to say that the number of infected files falls exponentially. The behavior of V follows from the assumption on half-lives, so that $f << b$, that is, the amount of free virus falls exponentially after a shoulder phase.

Model IV: Reactivation of computer virus after they are in latent class

When computer virus attacks the computer node, some of them enter a latent class on their infection. While in this class they do not produce new viruses, but may later be reactivated to do so. Only the files in the productive infected class Y1 produce viruses, and files at latent infected class Y2 leave for Y1 at a per capita rate *δ*. Thus our system becomes:

$$\frac{dV}{d\tau} = aY_1 - bV$$
$$\frac{dX}{d\tau} = c - dX - \beta XV$$
$$\frac{dY_1}{d\tau} = q_1 \beta XV - f_1 Y_1 + \delta Y_2 \qquad (15)$$
$$\frac{dY_2}{d\tau} = q_2 \beta XV - f_2 Y_2 - \delta Y_2$$

Infected files at class Y_2 produce viruses in class Y_1 at a rate δ for a time $\frac{1}{\delta + f_2}$

Thus adding the contribution of both the classes, the reproductive ratio R_0 is expressed as

$$R_0 = \frac{\beta c}{db} (q_1 + q_2 \frac{\delta}{\delta + f_2}) \frac{a}{f_1} \qquad (16)$$

Model V: Recent Attack by malicious object <u>Backdoor.Haxdoor.S</u> and <u>Trojan.Schoeberl.E</u> and its Mathematical approach

On January 9, 2007 <u>*Backdoor.Haxdoor.S*</u> and <u>*Trojan.Schoeberl.E*</u> malicious object of type *Trojan Horse* having infection length of 56,058 bytes affected Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP. Backdoor.Haxdoor.S is a Trojan horse program that opens a back door on the compromised computer and allows a remote attacker to have unauthorized access. It also logs keystrokes, steals passwords, and drops rootkits that run in safe mode. It has been reported that the Trojan has been spammed through email as an email attachment. The tool ***FixSchoeb-Haxdoor.exe*** is designed to remove the infections of <u>*Backdoor.Haxdoor.S*</u> and <u>*Trojan.Schoeberl.E*</u>. [10].

FixSchoeb-Haxdoor.exe tool meant to remove the deadly <u>*Backdoor.Haxdoor.S*</u> and <u>*Trojan.Schoeberl.E*</u> prevent infected files from producing infectious virus. We assume that W are the un- infectious virus which start to be produced from the infected files Y after the tool *FixSchoeb-Haxdoor.exe* is run. Infectious virus are still present, and die as before, but are no longer produced. Under this assumption the system can be modeled as

$$\frac{dV}{d\tau} = -bV$$
$$\frac{dX}{d\tau} = c - dX$$
$$\frac{dY}{d\tau} = -fY \qquad (17)$$
$$\frac{dW}{d\tau} = aY - bW$$

We assume that the uninfected file population X remains roughly constant for a given time-scale, that is,

$X = X^* = \frac{bf}{a\beta}$ and that $f << b$

System (17) becomes a linear system which is integrated to have

$$V = V_0 e^{-b\tau}$$

$$Y = Y_0 \frac{fe^{-b\tau} - be^{-f\tau}}{f - b} \quad , when \quad f << b$$

(18)

$$W = W_0 \frac{b}{b-f} \left(\frac{b}{b-f} (e^{-f\tau} - e^{-b\tau}) - f\tau e^{-b\tau} \right)$$

From (18) it is clear that the total amount $V + W$ of free virus falls exponentially after a shoulder phase.

Discussion and Conclusion

The threshold parameter obtained in (2) for primary phase of infection discusses the criterion for the spread of the computer virus, that is, $R_0 > 1$

. The susceptible population X (uninfected files) is reduced by the attack until each virus expected to give rise to exactly one new virus, .

$$R_0 x^* = 1$$

For the viruses which are quarentined by the installed antivirus software, we assume that updated antivirus software is available and is 100% efficient. When this updated antivirus software is run, from equation (14) we are able to say that the number of infected files falls exponentially. The behavior of V follows from the assumption on half-lives, so that $f \ll b$

that is, the amount of free virus falls exponentially after a shoulder phase. Discussion is also made for those viruses which enter a latent class on their infection and in this class they do not produce new viruses, but may later be reactivated to do so. Infected files at class Y_2 produce viruses in class Y_1 at a rate δ for a time $1/\delta+f$ and the reproductive ratio is also obtained.

Nomenclature

- V : number of viruses in the computer
- X : number of uninfected target files
- Y : number of infected files
- a : Replicating factor
- b : Death rate of a virus
- c : Birth of uninfected files by users
- d : Natural Death of an uninfected file
- e : Death rate of infected files

$f = e + d$

- β : Infectious contact rate, i.e., the rate of election per susceptible and per infective
- R_0 : Threshold parameter
- Z : Response of antivirus software, which immunes the system
- g : Rate at which antivirus software is run, which is constant
- h : Death rate of antivirus software

- : Rate at which antivirus software cleans the infected files
- : Immune response parameter
- Y1 : productive infected class
- Y2 : latent infected class
- Q1 : Probability of entering productive infected class
- Q2 : Probability of entering latent infected class

References

[1] 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) 1476-1482

[2] Bimal Kumar Mishra, Dinesh Saini, Mathematical models on computer viruses, Applied Mathematics and Computation, 187 (2007) 929-936

[3] Lotka, A. J., Elements of Physical Biology, Williams and Wilkins, Baltimore, 1925; Reissued as Elements of Mathematical Biology, Dover, New York, 1956.

[4] Volterra, V., Variazioni e fluttazioni del numero d'individui in specie animali conviventi, Mem. Acad. Sci. Lincei, 1926, 2:31-13

[5] Jones, A.K. and Sielken, R.S., Computer System Intrusion detection: a survey, Technical report, Computer Science Department, University of Virginia, 2000

[6] Yu, J., Reddy, R., Selliah, S., Reddy, S., Bharadwaj, V. and Kankanahalli S., TRINETR: An Architecture for Collaborative Intrusion Detection and Knowledge-Based Alert Evaluation, In Advanced Engineering Informatics Journal, Special Issue on Collaborative Environments for Design and Manufacturing. Editor: Weiming Shen. Volume 19, Issue 2, April 2005. Elsevier Science, 93-

[7] Jinqiao Yu, Y.V.Ramana Reddy , Sentil Selliah, Srinivas Kankanahalli, Sumitra Reddy and Vijayanand Bhardwaj, A Collaborative Architecture for Intrusion Detection Systems with Intelligent Agents and Knowledge based alert Evaluation, In the Proceedings of IEEE 8th International Conference on Computer Supported Cooperative work in Design, 2004, 2: 271-276

[8] Nicholas F. Britton, Essential Mathematical Biology, Springer-Verlag, London, 2003 [9] 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) 1207-1212

[10] http://www.symantec.com/smb/security_response/writeup.jsp?docid=2007-011109-2557-99

[11] Masud, Mohammad M., Khan, Latifur and Thuraisingham, Bhavani, A Knowledge-based Approach to detect new Malicious Executables. In the proceedings of the Second Secure Knowledge Management Workshop (SKM) 2006, Brooklyn, NY, USA

[12] http://www.f-secure.com/f-secure/pressroom/news/fsnews_20080331_1_eng.html, March 31, 2008

Thank You !

NOMENCLATURE

N (t): Total Population size
E (t): Exposed Population
S (t): Susceptible Population
I (t): Infected Population
R (t): Recovered Population
b: Per capita birth rate
μ: Per capita death rate due to causes other than attack of malicious object
ε: Death rate due to malicious objects and is constant in the infective class

α: Recovery rate which is constant
γ: Product of average number of contacts of a node per unit time and the probability of transmitting the malicious object during one contact by an infective.
ω: Period of latency, which is constant and non-negative
τ: Period of *temporary* immunity, which is constant and non-negative
p: Probability of *temporary* immunity acquired when a node is recovered from the infective class

$$\frac{dS(t)}{dt} = bN(t) - \mu S(t) - \gamma \frac{S(t)I(t)}{N(t)} + \alpha I(t-\tau)e^{-\mu\tau}$$

$$\frac{dE(t)}{dt} = \gamma \frac{S(t)I(t)}{N(t)} - \gamma \frac{S(t-\tau)I(t-\tau)}{N(t-\tau)} e^{-\mu\omega} - \mu E(t)$$

$$\frac{dI(t)}{dt} = \gamma \frac{S(t-\tau)I(t-\tau)}{N(t-\tau)} e^{-\mu\omega} - (\mu+\varepsilon+\alpha)I(t)$$

$$\frac{dR(t)}{dt} = p\alpha I(t) - \alpha I(t-\tau)e^{-\mu\tau} - \mu R(t)$$

$$N(t) = S(t) + I(t) + E(t) + R(t)$$

For the continuity of the solution to this system , we require,

$$E(0) = \int_{-\omega}^{0} \frac{\gamma S(u)I(u)}{N(u)} e^{\mu u} du$$

$$R(0) = \int_{-\tau}^{0} p\alpha I(u)e^{\mu u} du$$

From the above system , we also get,

$$\frac{dN(t)}{dt} = (b-\mu)N(t) - (b-(1-p)\alpha)\varepsilon I(t)$$

References

- A D'Onofrio, On pulse vaccination strategy in the SIR epidemic model with vertical transmission, Applied Mathematics Letter 18 (2005) 729-732
- A D'Onofrio, Stability properties of pulse vaccination strategy in SIER epidemic model, Math Bioscience 179(2002) 57-72
- Bimal Kumar Mishra, Dinesh Saini, Mathematical models on computer viruses, Applied Mathematics and Computation, 187 (2007) 929-936.
- 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) 1207-1212.

- 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, doi: 10.1016/j.amc.2007.03.052
- 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) 1476-1482.
- Bimal Kumar Mishra, Generality of the final size formula for infected nodes due to the attack of malicious objects in a computer network, Applied Mathematics and Computation, doi: 10.1016/j.amc.2007.04.071

- G. Zeng, L. Chen, Complexity and asymptotical behavior of a SIRS epidemic model with proportional impulse vaccination, Advance Complex Systems 8 (4) (2005) 419-431
- H.W.Hethcote and P. Driessche, An SIS epidemic model with variable population size and a delay, J. Math. Biol. 34(1995)177-194
- H.W.Hethcote and P. Driessche, Two SIS epidemiologic models with delays, J. Math. Biol. 40(2000) 3-26
- K. Cooke and P. Driessche, Analysis of an SEIRS epidemic model with two delays, J. Math. Biol. 35(1996) 240-260

M. E. J. Newman, Stephanie Forrest, and Justin Balthrop, Email networks and the spread of computer viruses, Physical Review E 66 (2002) 035101-4
E. Beretta, T. Hara et al, Global asymptotic stability of an SIR epidemic model with distributed time delays, Non Linear Analysis 47 (2007) 4107-4115
G. Li, Z. Jin, Global stability of a SIER epidemic model with infectious force in latent, infected and immune period, Chaos Solutions and Fractals 25(2005) 1177-1184

- S. Ruan, W. Wang, Dynamical behavior of an epidemic model with a non linear incidence rate, Journal of Differential Equations 188(2003) 135-163
- W. Wang, Global behavior of an SIERS epidemic model with time delays, Applied Mathematics Letter 15(2002) 57-72
- X. Meng, L.Chen, H.Cheng, Two profitless delays for the SEIRS epidemic disease model with non-linear incidence and pulse vaccination, Applied Mathematics and Computation, 186(2007) 516-529.
- Y. Michael, H.Smith, L.Wang, Global dynamics of SIER epidemic model with vertical transmission, SIAM Journal of Applied Mathematics 62(1) (2001) 58-69
- Z. Jin, Z. Ma, The stability of an SIR epidemic model with time delays, Math Bioscience Engineering 3(1) (2006) 101-109