Journal of Engineering and Applied Sciences 4 (3): 215-220, 2009
ISSN: 1816-949X

Predator-Prey Models for the Attack of Malicious Objects in Computer Network

[1]Bimal Kumar Mishra and [2]Gholam Mursalin Ansari
[1]Department of Applied Mathematics, Birla Institute of Technology,
Mesra, 835 215 Ranchi, India
[2]Department of Computer Science, University of Polytechnic,
Birla Institute of Technology, Mesra, 835 215 Ranchi, India

Abstract: This study shows appropriate mathematical concepts for describing persistence by means of simple predator-prey models framed in system of integro-differential equations. Two mathematical models are proposed to study the predator-prey system inside a computer system. In mathematical model 1, the prey consists of infected and the uninfected nodes, whereas, the predator consists of malicious objects. In mathematical model 2, malicious objects constitute the prey and anti-malicious software is the predator. Stability of the result is stated in terms of threshold parameter R_0. Explicit formula for the reproductive number R_0 is derived and it has been shown that the malicious objects infection-free equilibrium, whose component of infective is zero, is asymptotically stable (globally) if threshold parameter is less than or equal to one and unstable if greater then one. Numerical method is employed to solve the system of equations developed. The simulated results may help us to understand the spread and control of malicious objects in computer network.

Key words: Malicious objects, computer network, intraspecific competition, anti-malicious software, self-replication time, predator-prey model

INTRODUCTION

The growth of internet technology has thrown severe challenges in form of requirement of a suitable cyber defense system to safeguard the valuable information stored on system and for information in transit. Towards this goal it makes us necessary to study and understand the various malicious objects (Worm, Virus, Trojan etc.) and develop a mathematical model to represent their behavior. Malicious objects behave like infectious diseases and are epidemic in nature. Model's ability to predict malicious objects behavior depends greatly on the assumptions made in the modeling process. The mathematical models will be generalized to represent the behavior of numerous other malicious objects. The generalized model will be incorporated into a cyber defense system to proactively safeguard the information and information interchange.

Malicious objects can be in any form; like attachment of malicious executable file, malicious hyperlink and Phishing. by clicking incidentally or wrongly an attachment of malicious executable file can infect the system, here the user's awareness is necessary to avoid such type of attacks. If a hyperlink looks likes a spy-ware then by clicking it a user can go to the direction of attack.

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.

Chen *et al*. (2003) presented a mathematical model, referred to as the Analytical Active Worm Propagation (AAWP) model, which characterizes the propagation of worms that employ random scanning taking the concept of prey-predator epidemiological model. They compared the model with the Epidemiological model and Weaver's simulator taking the Code Red v2 worm as an example and gave a quantitative analysis for monitoring, detecting and defending against worms.

Jeffrey *et al*. (1997) analyzed that perhaps computer viruses and computer immune systems are merely precursors of an eventual rich ecosystem of artificial life-forms that will live, die, cooperate and prey on one another in cyberspace.

Freedman (1990) studied a prey-predator system, in which some members of prey population and all predators are subjected to infection by parasites and derived

Corresponding Author: Bimal Kumar Mishra, Department of Applied Mathematics, Birla Institute of Technology, Mesra, 835 215 Ranchi, India

conditions for persistence of all populations. Anderson and May (1986) investigated the invasion of a resident prey-predator or host parasite system by a new strain of parasites. Hadeler and Freedman (1989) observed similar phenomena. Mishra and Saini (2007a, b) and Mishra and Navnit Jha (2007c, 2009) developed epidemiological models of transmission of malicious objects in the computer network.

Mukherjee (2003) analyzed a generalized prey-predator system with parasitic infection and obtained epidemiological model namely S-I, in order to investigate how predation process influences epidemics.

$$\begin{aligned}\frac{dS}{dt} &= S\left\{r\left(1-\frac{S+I}{K}\right)-\beta I\right\}\\ \frac{dI}{dt} &= I\{\beta S - c - pY - aI\}\\ \frac{dY}{dt} &= Y\{-d + qpI - bY\}\end{aligned} \quad (1)$$

where, S(t), I(t), Y(t) are the population density of susceptible prey, infected prey and predator, respectively at a given time t. Here, r is the intrinsic birth rate and K is carrying capacity of the environment. β is the transmission coefficient, c and d are the death rate of infected prey and predator, respectively. a and b denote the intraspecific competition coefficient of the prey and predator, respectively. The coefficient in conversing prey into predator is q($0<q<1$) represents predation coefficient.

In model 1, we incorporate the differential equations based on basic epidemiological model, namely the S-I model in order to investigate how the predation process, when malicious objects influences the computer networks. We consider the case where predator attacks both infected and uninfected prey, where we differ from Mukherjee (2003), which considered into account single prey and single predator and change in their population due to interaction between them.

Differential infectivity is considered, which classifies nodes being susceptible to infection, if they are free from any infection and also those nodes, which are infected by other malicious agents (since, even though it is infected by one kind of malicious agent, other malicious agents can attack the same node and can affect other applications of it's interest, for example, some attack executable file, while other attacks bootable files) and corresponding change in the predator population is obtained by the summation of all those nodes, which are infected by particular kind of malicious agents.

Model 2 describes the use of anti-malicious software inside a particular node keeping in view of the self replication time of malicious agents and *latency period* of anti-malicious software. If the software is not efficient enough to recover the node from malicious attacks, this results in the death of that anti-malicious software (i.e., the existing anti-malicious software is not capable of removing the malicious objects).

Basic terminologies: Deaths of malicious objects equivalently mean to say, the complete recovery of infected files from malicious objects, when anti malicious software is run in the computer node for a specific session.

- Natural death of a file equivalently mean to say that the file become irrelevant (garbage) after a certain interval of time
- Death rate of infected files equivalently mean to say that files get damaged and unable to be recovered after the run of anti-malicious software due to infection from the malicious objects
- Death of anti-malicious software equivalently mean to say the present version of the software is incapable of identifying the attack of new malicious objects
- Malicious objects is a computer program that operates on behalf of a potential intruder to aid in attacking a system or network. Historically, an arsenal of such agents consisted of viruses, worms and trojanized programs. By combining key features of these agents, attackers are now able to create software that poses a serious threat even to organizations that fortify their network perimeter with firewalls
- Anti-malicious software is a class of program that searches the hard drive and floppy disks for any known or potential malicious objects. As new malicious objects are discovered by the anti-malicious vendor, their binary patterns are added to a signature database that is downloaded periodically to the user's anti-malicious program via the web

MATERIALS AND METHODS

Development of mathematical models: An interaction between malicious objects and anti-malicious software inside a system can be modeled by considering the response in the computer system due to anti-malicious software Z, which is run at a constant rate g and h being the death rate of anti-malicious software. The anti-malicious software cleans the infected files at a rate γYZ.

On the basis of our assumption, we have the following system of equations:

$$\begin{aligned}\frac{dV}{dt} &= aY - bV\\ \frac{dX}{dt} &= c - dX - \beta XV\\ \frac{dY}{dt} &= \beta XV - fY - \gamma YZ\\ \frac{dZ}{dt} &= g - hZ\end{aligned} \quad (2)$$

Model 1: We assume uninfected and infected nodes to act as prey and infectious agents like Worm, Virus, Trojan etc. act as predator. There is conversing of prey to predator, i.e., once the node is infected by any one of the malicious agents, it is susceptible to other malicious agents, because the same node can be attacked by different types of malicious agents and some of these agents self replicate within the infected nodes, finally these nodes are converted into predator. Thus, predator population is going to increase over a period of time. There is intraspecific competition among prey, i.e., in a network, nodes, which are connected to outside ones are more susceptible to malicious attacks than that are connected within that particular network, which is represented by factor α.

Different malicious objects compete with each other to gain entry into the nodes, which we term as intraspecific competition. Suppose worms and virus attack a particular node and if the node has anti-virus software installed in it, then due to the intraspecific competition between worm and virus, the worm enters the node and the virus die-out. This is represented by factor b.

On the basis of the assumptions, we get the following system of equations.

$$\begin{aligned}\frac{dS}{dt} &= S\left\{r\left(1-\frac{S+I}{K}\right)-\beta I\right\}\\ \frac{dI}{dt} &= \sum_{k=1}^{n}\left[I_k\left\{\beta S - c - p_k Y_k - aI_k\right\} + \gamma_k p I_k \beta S\right]\\ \frac{dY}{dt} &= \sum_{k=1}^{n}\left[Y_k\left\{-d + q_k p_k I_k - bY_k\right\} + q_k p_k \gamma_k I_k\right]\end{aligned} \quad (3)$$

Model 2: In this model, infected node becomes prey and anti-malicious software acts as predator. The model differs from model 1, as here we consider self-replication time ϕ and latency period ω. In infected nodes, malicious agents self replicates with period ϕ, said to be self replication time. Anti-malicious software takes some time ω, to make the infected files recover temporarily from malicious agents within the same node said to be latency period. P is the probability of self-replication (either 0 or 1).

$$p = \begin{cases}0, & \text{do not self-replicate}\\ 1, & \text{self-replicates}\end{cases}$$

On the basis of our assumptions, we obtain the following system of integro-differential equations:

$$\begin{aligned}\frac{dV}{dt} &= a'Y(t-\phi) - b'V(t-\phi) + \sum_{k=1}^{n} p\gamma_k V(t-\phi)\\ \frac{dX}{dt} &= c' - \left\{d'X(t-\omega) + \beta X(t-\omega).V(t-\omega)\right\}e^{-d'\omega} + \alpha Y(t)\\ \frac{dY}{dt} &= \begin{Bmatrix}\beta X(t-\omega)V(t-\omega) - fY(t-\omega)\\ -\xi Y(t-\omega)Z(t-\omega)\end{Bmatrix}e^{-m\omega} - (\alpha+m)Y(t)\\ \frac{dZ}{dt} &= g - hZ\end{aligned} \quad (4)$$

Reproductive number: For the simplicity of the system, we neglect disease-induced mortality rate of the files within a particular node, i.e., m = 0. We denote this infection-free equilibrium by $E_0 = (S_i = m_i S^0, i = 1, 2, ..., n)$. Analyzing the local stability of E_0 gives the epidemic threshold conditions under, which the number of infected nodes will either increase or decrease to zero as a small number of infective introduced into a fully susceptible population. Thus, only the third equation of our system Eq. 4 is modified as:

$$\frac{dY}{dt} = \begin{Bmatrix}\beta X(t-\omega)V(t-\omega) - fY(t-\omega)\\ -\xi Y(t-\omega)Z(t-\omega)\end{Bmatrix} - \alpha Y(t) \quad (5)$$

We further assume that

$$c(X^0)/X = \eta$$

where, $c(X^0)$ is mean number of contacts.

Analyzing the stability of the above system Eq. 4 gives the threshold conditions under, which infected files will increase or decrease to zero.

The threshold conditions are characterized by reproductive number R_0 as given below, shows that system is asymptotically stable if $R_0 \leq 1$ and unstable if $R_0 \geq 1$.

The Jacobian of (4) at E_0 is of the form

$$J=\begin{bmatrix} -m & 0 & 0 & . & . & 0 & . & . & . & p\gamma_1 \\ 0 & -m & 0 & . & . & 0 & . & . & . & p\gamma_2 \\ 0 & 0 & -m & . & . & 0 & . & . & . & p\gamma_3 \\ 0 & 0 & 0 & . & . & -m & . & . & & p\gamma_n \\ 0 & 0 & 0 & . & . & 0 & . & . & . & -(\alpha+m)\sum_{i=1}^{n}(1+p\gamma_k) \end{bmatrix} \quad (6)$$

All eigenvalues of J have negative real part if and only if,

$$-(\alpha+m)\sum_{i=1}^{n}(1+p\gamma_{k)}<0$$

Therefore, the reproductive number can be defined as:

$$R_0=\frac{c(X^0)\beta}{\alpha+m}\left(\sum_{i=1}^{n}(1+p\gamma_k)\right) \quad (7)$$

Theorem 3.1 Define the reproductive number of infection, R_0, for system Eq. 4 as in Eq. 7. Then, the infection free-equilibrium E_0 is globally asymptotically if $R_0 \leq 1$ and unstable if $R_0 \geq 1$ (Hyman and Li, 1996).

RESULTS AND DISCUSSION

Numerical method is employed to solve Eq. 3. We analyze the behavior of prey when they are attacked by the predator and the corresponding change in predator population (Fig. 1 and 2).

On the basis of our result, we are able to analyze the rate, at which prey population is going to decrease and predator population is going to increase with respect to time. Initially, when there is no attack of predator, the prey population is high and as time progresses, prey are going to be attacked by the predators and there is corresponding decrease in the prey population. The infected preys are going to change into predators resulting in the increase of predator population.

Also, we employ numerical method to solve system Eq. 4, for appropriate values of c, d and β, in particular to the equation involving the rate of change of infected files within a particular node.

The rate at which files are affected due to malicious agents within a node and the effect of anti-malicious software can be easily analyzed with the help of Fig. 3. When, any malicious agent affects a group of nodes in a network, it replicates linearly in them. Thus, initially within a node, malicious objects attack files and anti-malicious software takes some time ω to recover those affected files, reducing the infected files to zero after the run of anti-malicious software and nodes again becomes susceptible. But as the agent is already increasing rapidly in network, it effects the node and attack the files mode

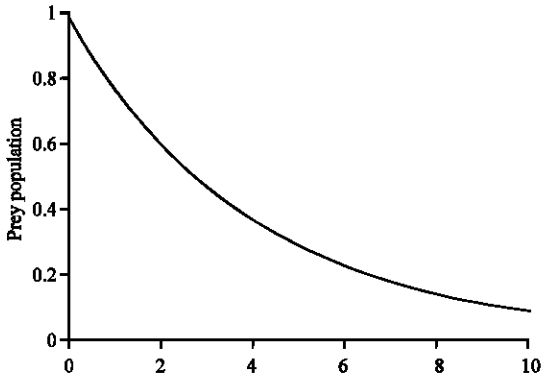

Fig. 1: Rate of change of the prey population with respect to time for $p_k = 1$, $p = 0$, $\mu = 2$

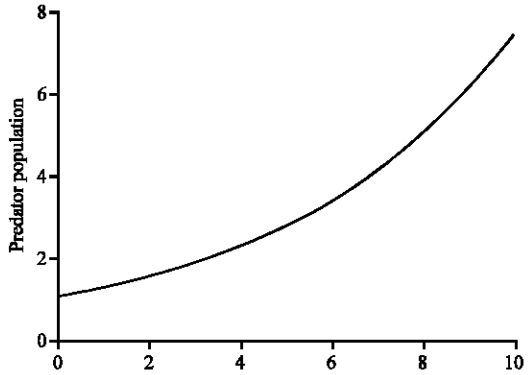

Fig. 2: Rate of change of the predator population with respect to time for $p_k = 1$, $p = 0$, $\mu = 2$

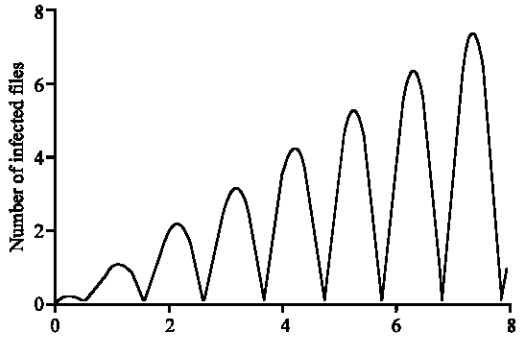

Fig. 3: Rate of change of infected files population with respect to time for d' = 1, m = 0.2, $\gamma_k = 1$, p = 1

rapidly (Fig. 3: rise in peak) and again anti-malicious software curbs further attack of malicious agents and recovers the node with faster rate within the same time ω.

The threshold conditions are characterized by reproductive number R_0 and the system is asymptotically stable if $R_0 \leq 1$ and unstable if $R \geq 1$. The reproductive number is obtained as:

$$R_0 = \frac{c(X^0)\beta}{\alpha + m}\left(\sum_{i=1}^{n}(1 + p\gamma_k)\right)$$

We are able to describe the rate at which prey population is going to decrease and predator population is going to increase with respect to time. Self replication time of malicious agents and latency period of anti-malicious software is considered. The concept of intraspecific competition in computer terminology makes us to understand the behavior of different malicious objects, which compete with each other to gain entry into the nodes. The attacking nature of malicious objects are also categorically analyzed.

CONCLUSION

Inspired by the biological epidemic models, we have developed predator prey models for the attack of malicious objects in computer network. One of the important characteristic of worms, self replication and latency period of anti malicious software is considered. The concept of intraspecific competition in computer terminology has been incorporated, which will make us to understand the behavior of different malicious objects, which compete with each other to gain entry into the nodes. Using real parametric values, we were able to analyze the rate, at which files are affected due to malicious agents within a node and how the anti-malicious software effects on them. From the simulated results, we observed that the use of anti malicious software to control malicious objects not only decreases the endemic infective class size when R_0 remains above 1, but also makes it easier to obtain $R_0<1$ leading to malicious objects extinction.

Nomenclature:

- S (t) : Population density of susceptible prey
- I (t) : Population density of infected prey
- Y (t) : Population density of predator
- S^0 : Inflow population rate
- r : Intrinsic birth rate
- K : Carrying capacity of the environment
- β : Transmission coefficient
- a : Intraspecific competition coefficient of infected prey
- b : Intraspecific competition coefficient of predator
- c : Death rate of infected prey
- d : Death rate of predator
- q_k : Coefficient of conversing prey into predator when attacked by the k^{th} malicious object
- p_k : Predation coefficient of the k^{th} malicious object
- p : Probability of replication of the k^{th} malicious object
- γ_k : Replication factor
- V : Number of malicious objects in a node
- X : Number of uninfected target files
- Y : Number of infected files
- a' : Replicating factor
- b' : Death rate of a malicious object
- c' : Birth of uninfected files by users
- d' : Natural death of an uninfected file
- m : Death rate of infected files
- m_k : Probability of getting susceptible by k^{th} malicious agent f = m + d'
- α : Recovery rate of infected files
- β : Infectious contact rate, i.e., the rate of infection per susceptible per infective
- Z : Response of anti-malicious software, which immunes the system
- g : Rate at which anti-malicious software is run, which is constant
- h : Death rate of anti-malicious software
- ω : Latency period
- φ : Self-replication time
- ξYZ : Rate at which anti-malicious software cleans the infected files

REFERENCES

Anderson, R.M. and R.M. May, 1986. The invasion and spread of infectious diseases within animal and plant communities. Philos. Trans. R. Soc., Lond B, 314: 533-570.

Chen, Z., L. Gao and K. Kwiat, 2003. Modeling the spread of active worms, INFOCOM, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE Publication, 3: 1890-1900.

Freedman, H.I., 1990. A model of predator-prey dynamics as modified by the action of a parasite. Math. Biosci., 99: 143-155.

Hyman, J.M. and J. Li, 1996. Differential susceptibility epidemic models. J. Math. Bio., 35: 240-260.

Jeffrey, K., G. Sorkin, D. Chess and S. White, 1997. Fighting Comput. Viruses, Computers and Security, 16 (8): 676-677(2).

Mishra, B.K. and Navnit Jha, 2009. SEIQRS model for the transmission of malicious objects in computer network. Applied Mathematical Modelling. DOI: 10.1016/j.apm.2009.06.011.

Mishra, B.K. and D.K. Saini, 2007a. SIERS epidemic model with delay for transmission of malicious objects in computer network. Applied Mathe. Comput., 188 (2): 1476-1482.

Mishra, B.K. and D.K. Saini, 2007b. Mathematical models on computer viruses. Applied Mathe. Comput., 187 (2): 929-936.

Mishra, B.K. and Navnit Jha, 2007c. Fixed period of temporary immunity after run of anti-malicious software on computer nodes, 190 (2): 1207-1212.

Mukherjee, D., 2003. Stability analysis of a stochastic model for prey-predator system with disease in the prey, nonlinear analysis: Modeling and Control, 8: 83-92.