Applied Mathematics and Computation 227 (2014) 11–18

Contents lists available at ScienceDirect

Applied Mathematics and Computation

journal homepage: www.elsevier.com/locate/amc

Modeling and analysis of the effects of antivirus software on an infected computer network

J.B. Shukla [a,b], Gaurav Singh [a], Poonam Shukla [b], Agraj Tripathi [a,*]

[a] Bhabha Institute of Technology, BIIFRD, Aunaha, Kanpur(Rural), P.O. Box 209 204, U.P., India
[b] C-MEND, Kanpur 208016, U.P., India

ARTICLE INFO

Keywords:
Computer network
Infected nodes
Virus
Antivirus

ABSTRACT

In this paper, a nonlinear mathematical model for cleaning an infected computer network by using antivirus software is proposed and analyzed. In the modeling process, the total number of nodes in the network are divided in three subclasses, namely, the number of susceptible nodes, number of infected nodes and the number of protected nodes. A variable representing the number of antivirus softwares, assumed to be proportional to number of infected nodes, is also considered in the model which interacts with other nodes bilinearly to conduct the cleaning process. The model is analyzed by using stability theory of differential equations and computer simulation. The analysis shows that it is possible to clean the computer network under certain condition which depend upon the inflow rate of infected nodes in the computer network, the rate of interaction of infected nodes with susceptible nodes and their interactions with antivirus software, etc. It is found that the entire network can be cleaned eventually if the antivirus software is applied on the network, where a separate class of protected nodes is formed. The computer simulation confirms the analytical results.

1. Introduction

A virus is an unwanted small piece of software (malicious program) that gets transmitted into the computer network without the knowledge of its users and is not compatible with the system. When the computer programs are run, the viruses get circulated along with the programs and starts infecting associated programs which come into its contacts. There exists a possible threat of other connected systems getting infected too. Viruses can spread on a network easily because of the interconnectivity of workstations. Such spread can be dangerous if the computers have important database which can get corrupted by viruses because all nodes in the network are eventually infected. To clean the system, an antivirus software is used to eliminate viruses in infected network of nodes and protect other nodes by isolating them, the protection being carried out by another software with a constant rate which is always present in the system.

To study this problem quantitatively, mathematical models are very useful tools which have been applied in recent years by using the concepts well known in the theory of epidemics in human population [1–5,9–10].

In recent years, some mathematical models have been proposed to study the spread of infection in the computer network quantitatively [6–8,10]. In particular, Yuan and Chen [10] presented a network epidemic e-SEIR model and discussed the spread of virus in a computer network by using the stability theory of differential equations. Mishra and Jha [6] proposed a model for the transmission of malicious objects in computer network. Mishra and Saini [7] have also studied SEIRS type

* Corresponding author.
E-mail address: agrajtripathi@gmail.com (A. Tripathi).

0096-3003/$ - see front matter
http://dx.doi.org/10.1016/j.amc.2013.10.091

model for the spread of computer viruses by considering the effect of delay in the transmission process. Newman et al. [8] has studied the spread of computer viruses in e-mail network.

In these studies, the effect of antivirus software on infected computer network has not been modeled and analyzed. Therefore, in this paper, our focus is to model the computer network infected by viruses and to show how antivirus program could clean the system.

2. Mathematical model

Let $N(t)$ be the total number of nodes in a network which is sub-divided into three subclasses of susceptible nodes $X(t)$, infected nodes $Y(t)$, and protected nodes $Z(t)$. Let $V_a(t)$ be the variable representing the number of the antivirus programs used to clean the network which is assumed to be proportional to the number of infected nodes. Then using the concepts of theory of epidemics, the model can be proposed as follows.

$$\begin{aligned}\frac{dX}{dt}&=A-\beta XY-dX-KX+\pi YV_a\\ \frac{dY}{dt}&=B+\beta XY-dY-\alpha Y-\pi YV_a\\ \frac{dZ}{dt}&=KX-dZ\\ \frac{dV_a}{dt}&=\mu Y-\mu_0(V_a-V_{a0})\end{aligned}\tag{1}$$

The parameters A and B in the model are inflow rates of susceptible and infected nodes respectively, d is the rate at which nodes are crashing due to the reason other than attack of viruses, β is the rate at which susceptibles nodes become infected when come into contact with infected nodes, α is the rate at which the infected nodes become disabled and can not affect the susceptible nodes, π is the rate at which infected nodes are recovered and become susceptible again, K is the constant rate at which the nodes are being protected by another antivirus software, μ is the growth rate of antivirus program to clean the network and μ_0 is its rate by which it fails to work efficiently. V_{a0} is the value of the antivirus software which is always present in the system to protect the existing software. We assume that all the constants in the model are positive.

In model (1) it is assumed that cleaned nodes become susceptible again and they become protected only after having gone through a process of isolation caused by antivirus software, this method being similar to the well known concept of immunization in epidemic.

Since $N(t) = X(t)+Y(t)+Z(t)$, therefore, it is sufficient to study the following system which is equivalent to (1),

$$\begin{aligned}\frac{dN}{dt}&=A+B-dN-\alpha Y\\ \frac{dY}{dt}&=B+\beta(N-Y-Z)Y-dY-\alpha Y-\pi YV_a\\ \frac{dZ}{dt}&=K(N-Y-Z)-dZ\\ \frac{dV_a}{dt}&=\mu Y-\mu_0(V_a-V_{a0})\end{aligned}\tag{2}$$

The invariant region where solution exists is given as follows

$$\mathcal{R}=\{(N,I,Z,V_a);\quad N_{\min}\le N(t)\le N_{\max},\quad 0\le Y(t)<N(t)\le N_{\max},\quad 0\le Z(t)\le Z_{\max},\quad 0\le V_a(t)\le V_{a_{\max}}\}\tag{3}$$

where $N_{\max}=\frac{A+B}{d}$ and $N_{\min}=\frac{A+B}{\alpha+d}$

$$Z_{\max}=\frac{K}{(K+d)}N_{\max},\quad V_{a\max}=\frac{\mu}{\mu_0}Y_{\max}=\frac{\mu}{\mu_0}N_{\max}+V_{a0}$$

In the following, we present the equilibrium analysis of the model (2).

3. Equilibrium analysis

The model system (2) has only one equilibrium $E^*=(N^*,\ Y^*,\ Z^*,\ V_a^*)$ where N^*, Y^*, Z^*, and V_a^* are positive solutions of the following system of algebraic equations obtained by taking left hand sides of (2) to zero,

$$0=A+B-dN-\alpha Y\tag{4}$$

$$0=B+\beta(N-Y-Z)Y-dY-\alpha Y-\pi YV_a\tag{5}$$

$$0=K(N-Y-Z)-dZ\tag{6}$$