TAMKANG JOURNAL OF MATHEMATICS
Volume 51, Number 4, 333-347, December 2020
doi:10.5556/j.tkjm.51.2020.3249

ANALYTICAL SOLUTION OF PROPAGATION OF WORMS IN WIRELESS SENSOR NETWORK MODEL BY HOMOTOPY PERTURBATION METHOD

DEVIPRIYA GANESHAN AND KAVITHA THIRUVARUL SELVAN

Abstract. Wireless sensor networks (WSNs) have received wide-ranging consideration due to their boundless potential in civil and military applications. Malicious self-replicating codes, known as malware, pose substantial threat to the wire-less computing infrastructure. The attacks of the malicious signals in the WSN are epidemic in nature. Biological epidemic models will be helpful to under-stand the dynamical behavior of the malware attack in WSN. In this paper, A (SEIRS-V) Susceptible - Exposed - Infected - Recovered - Susceptible with a Vaccination compartment, describing the undercurrents of worm propagation with respect to time in wireless sensor network (WSN) is considered. The analytical solution of WSN is obtained by Homotopy Perturbation Method. Numerical results are obtained and are graphically interpreted using Maple. The results assures that the dynamics of worm propagation in WSN by the proposed model exhibits rich dynamics.

1. Introduction

Wireless Sensor Network (WSN) which has established vast attention due to its immense potential in civil and military application, are presently being used on a large scale to monitor real time environmental status. WSN is composed of large number of sensor nodes which communicate with each other through wireless medium. The sensor nodes are usually scattered in a sensor field. Each of these scattered sensor nodes have the capabilities to collect data and route data back to the sink. As wireless sensor networks are unfolding their vast potential in a plethora of application environment, security still remains one of the most critical challenges yet to be fully addressed. Because sensor nodes are resource constrained they generally have weak defense capabilities and are attractive targets for software attacks. Computer worms are self-replicating viruses which can propagate through computer network without

2010 *Mathematics Subject Classification*. 34B60, 34D10, 37M05, 74H10 (2000 MSC).
Key words and phrases. Wireless sensor network, system of non-linear differential equations, homotopy perturbation method, numerical simulations.
Corresponding author: Devipriya Ganeshan.

any human intervention. Cyber-attack by worm presents one of the most dangerous threats to the security and integrity of the computer and telecommunications networks [11].

Malware can be used to launch attacks that vary from the less intrusive confidentiality or privacy attacks, such as traffic analysis and eavesdropping, to the more intrusive methods that either disrupt the nodes normal functions such as those in relaying data and establishing end-to-end routes for example, sinkhole attacks [8], or even alter the network traffic and hence destroy the integrity of the information, such as unauthorized access and session hijacking attacks [7, 14]. Malware outbreaks like those of Slammer [12] and Code Red [15] worms in wired internet have already inflicted expenses of billions of dollars in repair after the viruses rapidly infected thousands of hosts within few hours. The attacks of the malicious signals in the wireless sensor network are epidemic in nature. Malicious signals targeting wireless devices, for example, the Cabir worm, can repeatedly send itself to blue-tooth enable devices inside it's host's scanning range. Similarly, the Mabir worm uses scanning techniques to attack. The spreading behavior of the Mabir and Cabir worm are epidemic in nature. Thus, to defend the sensor nodes against these types of malware attacks, we propose security mechanism using epidemic models. Biological epidemic models will be helpful to understand the dynamical behavior of the malware attack in Wireless sensor network (WSN).

Worms spread during data or control message transmission from nodes that are infected (infectives) and those that are vulnerable, but not yet infected (susceptibles). We consider a pernicious worm that may (i) eavesdrop, (ii) analyze, (iii) alter or destroy traffic and (iv) disrupt the infective host's normal functions (such as relaying data or establishing routes), and even kill the host, that is, render it completely dysfunctional (dead). This killing process may be triggered by performing a code which inflicts irretrievable hardware damage. For instance, Chernobyl virus could re-flesh the BIOS, corrupting the bootstrap program required to initialize the system. The worm can determine the time to kill, or equivalently the rate of killing the hosts, by regulating the rate at which it triggers such codes. Counter-measures can be launched by installing security patches that either immunize susceptible nodes against future attacks, by rectifying their underlying vulnerability, or heal the infective of the infection and render them robust against future attacks. For instance, for SQL-Slammer worms [12], while StackGuard programs immunize the susceptible by removing the buffer overflow vulnerability that the worms exploit, specialized security patches are required to remove the worm from (and thereby heal) the infective. Nodes that have been immunized or healed are denoted as recovered. Mishra and Jha proposed a susceptible-exposed-infectious-quarantined-removed (SEIQRS) e-epidemic model to understand the spreading behavior of worms in computer network and to reduce the infectiousness among the nodes in the computer network, a quarantine class(Q) was introduced where the nodes which are highly infectious were forcibly isolated and kept in the class Q [10]. In [11], reproduction number, equilibria, and the stability are found for the SEIRV-S compartmental system modeling the worm propagation in the wireless sensor network.

Mathematical modeling of most of the biological problems are inherently nonlinear and difficult to find the exact solutions to understand the biological phenomena. Therefore, numerical methods are necessary to find the exact solution and approximate solution to these nonlinear problems. In the numerical methods, stability and convergence of the solution is inevitable to avoid divergence or inappropriate results. To overcome these drawbacks in finding the approximate solution to the nonlinear dynamical models, Homotopy perturbation method is one of the best technique. The Homotopy Perturbation Method (HPM) is an analytical method for solving linear /nonlinear differential equations. It is a powerful and efficient technique for finding solutions of nonlinear equations without linearizing the problem. The method was first introduced by He [6]. The HPM is a combination of the perturbation and Homotopy methods. When two continuous functions moves from one topological space to another and one deforms into another it is said to be homotopic. It uses the idea of the homotopy from topology to create a convergent series solution - a Maclaurin series which transform the non linearities in the system of differential equation. This method takes the advantages of the conventional perturbation method while eliminating its restrictions.

In general, this method has been successfully applied to solve many kinds of linear and nonlinear equations in science and engineering by many authors. F. A. Adesuyi et al. [3], used HPM to solve cholera mathematical model incorporating three control strategy namely vaccination, therapetic treatment and water sanitation to control the spread of cholera epidemic over time. M. A. Khan et al. [9], studied the analytic solution of leptospirosis model by HPM. Abubakar et al. [1], proposed a SIR model for general infectious disease dynamics and the analytic solution is found using HPM. R. Senthamarai and S. Balamuralitharan [13], studied the transmission of malaria disease modelled by SIRS - SI model with treatments given to humans and mosquitoes and using HPM numerical solution is achieved B. Ebenezer et al. [4], used HPM to obtain the approximation solution of the Ebola mathematical model results shows that the HPM is very effective and accurate as few perturbation and obtained result on HPM is as good reliable as other known standard methods. G. Devipriya [5], considered a mathematical model of dengue virus transmission consists of human and mosquito compartments by incorporating with control strategy of imperfect treatment and delay in vector maturation whose analytical solution is obtained using HPM. G. Adambu et al. [2], considered mathematical model of Zika virus with two control strategies namely treatment for human and insecticide spray for mosquito and used HPM to get approximate solution and shows that 59% effective administration of infectious spray proved a great reduction in the infected human as well as infected vector population.

Thus we can see application of homotopy perturbation method to obtain the solution for almost all the infectious disease. To best of my knowledge, HPM has not been applied to obtain the solution for the worm propagation in the wireless sensor network model. Thus an attempt is made in this paper. The Mathematical formulation of the dynamics of worm propagation in WSN is done in section 2. In section 3, the analytic solution is obtained with aid of HPM. In section 4, the numerical solution is found and results are interpreted graphically using Maple. The variation of susceptible, exposed, infected, recovered and vaccinated population for different parameter are analyzed graphically.

2. Mathematical formulation

An dynamic propagation model is instrumental to understand the automated spread of a worm. Let $S(t), E(t), I(t), R(t)$ and $V(t)$ denote the number of susceptible, exposed, infectious, recovered, and vaccinated nodes at time t respectively. Consider the following system of nonlinear differential equations that describes the rate of change of different classes [11]:

$$\begin{aligned}
\frac{dS(t)}{dt} &= A - \beta S(t)I(t) - \mu S(t) - pS(t)(t) + dR(t) + \eta V(t) \\
\frac{dE(t)}{dt} &= \beta S(t)I(t) - (\mu + \alpha)E(t) \\
\frac{dI(t)(t)}{dt} &= \alpha E(t) - (\mu + \epsilon + \gamma)I(t) \\
\frac{dR(t)}{dt} &= \gamma I(t) - (\mu + d)R(t) \\
\frac{dV(t)}{dt} &= pS(t) - (\mu + \eta)V(t)
\end{aligned} \tag{2.1}$$

with initial conditions

$$S(0) \geq 0, E(0) \geq 0, I(0) \geq 0, R(0) \geq 0, V(0) \geq 0.$$

Here, A is the inclusion of new sensor nodes to the population, μ is the crashing rate of the sensor nodes due to hardware or software problem, ϵ is the crashing rate due to attack of worms. Let β be the infectivity contact rate. The rate of transmission from E-class to I-class is given by α, the rate of transmission from R-class to S-class is given by d and the rate of transmission from V-class to S-class is given by η. The rate of recovery is denote by γ and the rate at which the susceptible nodes are vaccinated is given by p.

3. Analytical solution by homotopy perturbation method

Consider the following nonlinear differential equation

$$L(u) + N(u) = f(r), \quad r \in \Omega \tag{3.1}$$

with the boundary conditions:

$$B\left(u, \frac{\partial u}{\partial n}\right) = 0, \quad r \in \Gamma$$

where L is a linear operator, N is a nonlinear operator, B is a boundary operator, Γ is the boundary of the domain Ω and $f(r)$ is a known analytic function.
By the homotopy perturbation technique [6], construct a homotopy:

$$v(r,q) : \Omega \times [0,1] \to R \tag{3.2}$$

which satisfies:

$$H(v,q) = (1-q)[L(v) - L(u_0)] + q[L(v) + N(v) - f(r)] = 0 \tag{3.3}$$

or

$$H(v,q) = L(v) - L(u_0) + qL(u_0) + q[N(v) - f(r)] = 0, \tag{3.4}$$

where $r \in \Omega$, $q \in [0,1]$ is an imbedding parameter and u_0 is an initial approximation which satisfies the boundary conditions. Obviously, from (3.3) and (3.4), we have:

$$H(v,0) = L(v) - L(u_0) = 0 \tag{3.5}$$

$$H(v,1) = L(v) + N(v) - f(r) = 0 \tag{3.6}$$

The changing process of q from zero to unity is just of $v(r,q)$ from $u_0(r)$ to $u(r)$. In topology, this is called deformation, $L(v) - L(u_0)$ and $L(v) + N(v) - f(r)$ are called homotopic. The basic assumption is that the solution of equation (3.4) can be expressed as a power series in q :

$$v = v_0 + qv_1 + q^2 v_2 + \cdots \tag{3.7}$$

The approximate solution of (3.1) is given as,

$$u = \lim_{q \to 1} v = v_0 + v_1 + v_2 + \cdots \tag{3.8}$$

which leads to rapid convergence.
Now, we apply the homotopy perturbation techniques to the model (2.1). Define the operator $\mathscr{L} = \frac{d}{dt}$. According to HPM, we construct a homotopy system as given below:

$$\begin{aligned}
&\mathscr{L}S(t) - \mathscr{L}S^0(t) = q(A - \beta S(t)I(t) - \mu S(t) - pS(t) + dR(t) + \eta V(t) - \mathscr{L}S^0(t)) \\
&\mathscr{L}E(t) - \mathscr{L}E^0(t) = q(\beta S(t)I(t) - (\mu + \alpha)E(t) - \mathscr{L}E^0(t)) \\
&\mathscr{L}I(t) - \mathscr{L}I^0(t) = q(\alpha E(t) - (\mu + \epsilon + \gamma)I(t) - \mathscr{L}I^0(t)) \\
&\mathscr{L}R(t) - \mathscr{L}R^0(t) = q(\gamma I(t) - (\mu + d)R(t) - \mathscr{L}R^0(t)) \\
&\mathscr{L}V(t) - \mathscr{L}V^0(t) = q(pS(t) - (\mu + \eta)V(t) - \mathscr{L}V^0(t))
\end{aligned} \tag{3.9}$$

with initial data,

$$S_0(t) = S^0(t) = S(0);\ E_0(t) = E^0(t) = E(0);\ I_0(t) = I^0(t) = I(0);\ R_0(t) = R^0(t) = R(0);$$
$$V_0(t) = V^0(t) = V(0).$$

The approximate solution of the above homotopy (3.9) is a power series in $q \in [0,1]$ and is given by

$$\begin{aligned} S(t) &= S_0^*(t) + qS_1^*(t) + q^2 S_2^*(t) + \cdots \\ E(t) &= E_0^*(t) + qE_1^*(t) + q^2 E_2^*(t) + \cdots \\ I(t) &= I_0^*(t) + qI_1^*(t) + q^2 I_2^*(t) + \cdots \\ R(t) &= R_0^*(t) + qR_1^*(t) + q^2 R_2^*(t) + \cdots \\ V(t) &= V_0^*(t) + qV_1^*(t) + q^2 V_2^*(t) + \cdots \end{aligned} \tag{3.10}$$

Making use of (3.10) in equation (3.9) and comparing the same coefficient of same power of q, we get
zeroth order system:

$$\begin{aligned} \mathscr{L}S_0^*(t) - \mathscr{L}S^0(t) &= 0 \\ \mathscr{L}E_0^*(t) - \mathscr{L}E^0(t) &= 0 \\ \mathscr{L}I_0^*(t) - \mathscr{L}I^0(t) &= 0 \\ \mathscr{L}R_0^*(t) - \mathscr{L}R^0(t) &= 0 \\ \mathscr{L}V_0^*(t) - \mathscr{L}V^0(t) &= 0 \end{aligned} \tag{3.11}$$

with initial conditions,

$$S_0^*(0) = S(0),\ E_0^*(0) = E(0),\ I_0^*(0) = I(0),\ R_0^*(0) = R(0),\ V_0^*(0) = V(0)$$

and
first order system:

$$\begin{aligned} \mathscr{L}S_1^*(t) &= A - \beta S_0^*(t)I_0^*(t) - \mu S_0^*(t) - pS_0^*(t) + dR_0^* + \eta V_0^*(t) - \mathscr{L}S_0^*(t) \\ \mathscr{L}E_1^*(t) &= \beta S_0^*(t)I_0^*(t) - (\mu+\alpha)E_0^*(t) - \mathscr{L}E_0^*(t) \\ \mathscr{L}I_1^*(t) &= \alpha E_0^* - (\mu+\epsilon+\gamma)I_0^*(t) - \mathscr{L}I_0^*(t) \\ \mathscr{L}R_1^*(t) &= \gamma I_0^*(t) - (\mu+\epsilon+\gamma)I_0^*(t) - \mathscr{L}I_0^*(t) \\ \mathscr{L}V_1^*(t) &= pS_0^*(t) - (\mu+\eta)V_0^*(t) - \mathscr{L}V_0^*(t) \end{aligned} \tag{3.12}$$

with initial conditions,

$$S_1^*(0) = 0,\ E_1^*(0) = 0,\ I_1^*(0) = 0,\ R_1^*(0) = 0,\ V_1^*(0) = 0.$$

and

second order system:

$$\begin{aligned}
&\mathscr{L}S_2^*(t) = -\beta[S_0^*(t)I_1^*(t) + S_1^*(t)I_0^*(t)] - \mu S_1^*(t) - pS_1^*(t) + dR_1^*(t) + \eta V_1^*(t)\\
&\mathscr{L}E_2^*(t) = \beta[S_0^*(t)I_1^*(t) + S_1^*(t)I_0^*(t)] - (\mu+\alpha)E_1^*(t)\\
&\mathscr{L}I_2^*(t) = \alpha E_1^*(t) - (\mu+\epsilon+\gamma)I_1^*(t)\\
&\mathscr{L}R_2^*(t) = \gamma I_1^*(t) - (\mu+d)R_1^*(t)\\
&\mathscr{L}V_2^*(t) = pS_1^*(t) - (\mu+\eta)V_1^*(t)
\end{aligned} \tag{3.13}$$

with initial conditions

$$S_2^*(0) = 0,\ E_2^*(0) = 0,\ I_2^*(0) = 0,\ R_2^*(0) = 0,\ V_2^*(0) = 0.$$

Solving the system of non - linear differential equation given in (3.11), (3.12) and (3.13) we will obtain the zeroth order solution, first order solution and second order solution and considering $q = 1$ in (3.10), we get

$$\begin{aligned}
S(t) &= S_0^*(t) + S_1^*(t) + S_2^*(t) + \cdots\\
E(t) &= E_0^*(t) + E_1^*(t) + E_2^*(t) + \cdots\\
I(t) &= I_0^*(t) + I_1^*(t) + I_2^*(t) + \cdots\\
R(t) &= R_0^*(t) + R_1^*(t) + R_2^*(t) + \cdots\\
V(t) &= V_0^*(t) + V_1^*(t) + V_2^*(t) + \cdots
\end{aligned} \tag{3.14}$$

The convergence of HPM is rapid, for few iteration.

4. Numerical results and discussions

In this section, numerical results of the problem is discussed. The solution of the dynamical model is obtained by homotopy perturbation method and results are graphically interpreted with the aid of Maple. In order to obtain the analytical solution to the problem, let us take the values of the parameter involved in the model as the following [11]:
$A = 0.33, \beta = 0.1, \mu = 0.003, p = 0.3, d = 0.3, \eta = 0.06, \alpha = 0.25, \epsilon = 0.07, \gamma = 0.4$
Let us assume the initial condition for the problem as
$S_0^*(t) = 100, E_0^*(t) = 3, I_0^*(t) = 1, R_0^*(t) = 0, V_0^*(t) = 0$. Solving the system of non - linear differential equation in (3.11), (3.12) and (3.13) using Maple, we will obtain

Zeroth Order Solution:

$$S_0(t) = 100, \quad E_0(t) = 3, \quad I_0(t) = 1, \quad R_0(t) = 0, \quad V_0(t) = 0;$$

First Order Solution:

$$S_1(t) = \frac{-3997}{100}t, \quad E_1(t) = \frac{9241}{1000}t, \quad I_1(t) = \frac{277}{1000}t, \quad R_1(t) = \frac{2}{5}t, \quad V_1(t) = 30t;$$

Second Order Solution:

$$S_2(t) = \frac{1525791}{200000}t^2, \quad E_2(t) = \frac{-3564973}{2000000}t^2, \quad I_2(t) = \frac{2179229}{2000000}t^2, \quad R_2(t) = \frac{-13}{2500}t^2,$$

$$V_2(t) = \frac{-13881}{2000}t^2$$

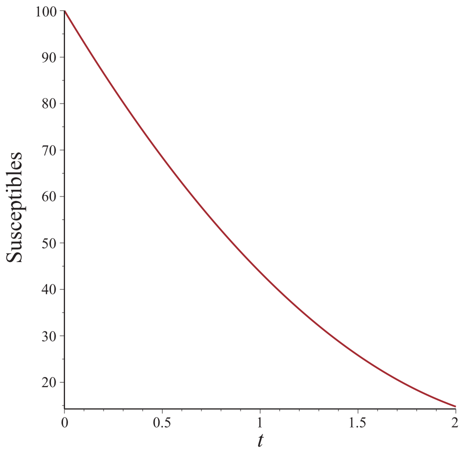

Figure 1: Variation of susceptible sensor nodes with respect to t.

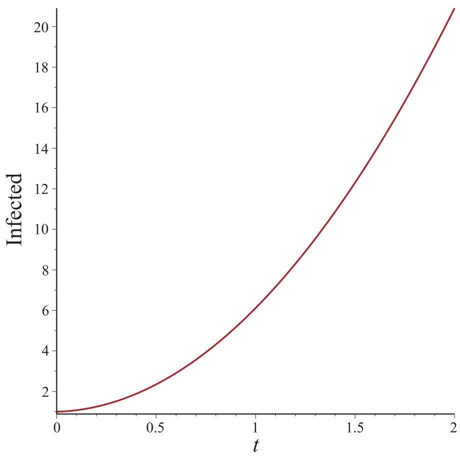

Figure 2: Variation of infected sensor nodes with respect to t.

In Figure 1, the variation of susceptible sensor nodes with respect to time is shown. The susceptible sensor nodes which are in contact with infected sensor nodes will be exposed

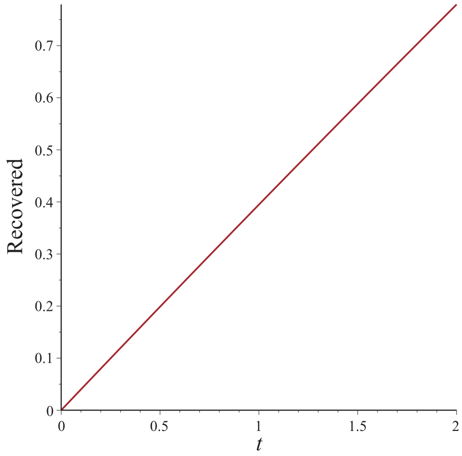

Figure 3: Variation of recovered sensor nodes with respect to t.

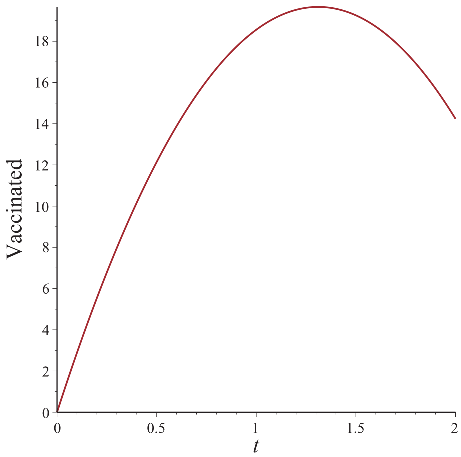

Figure 4: Variation of vaccinated sensor nodes with respect to t.

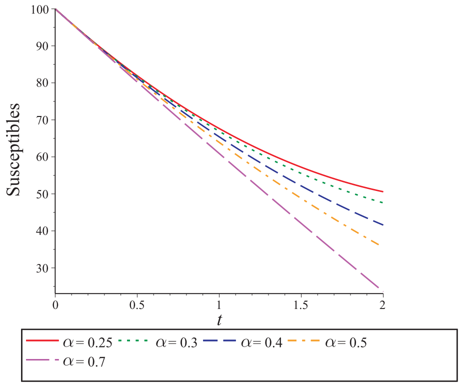

Figure 5: Variation of susceptible sensor nodes for different values of α.

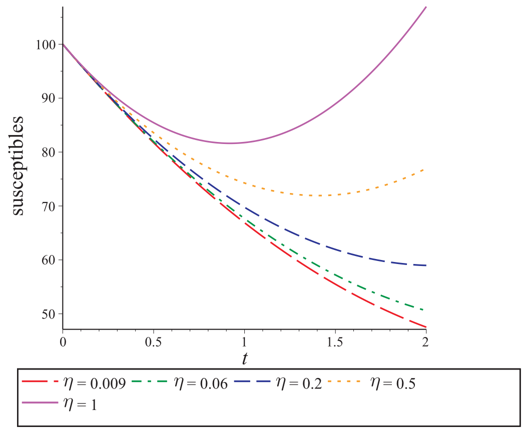

Figure 6: Variation of susceptible sensor nodes for different values of η.

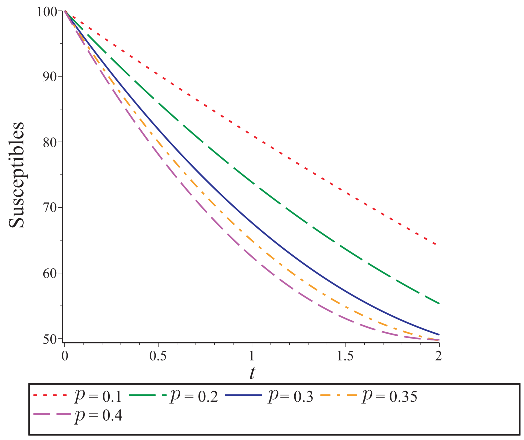

Figure 7: Variation of susceptible sensor nodes for different values of rate of vaccination p.

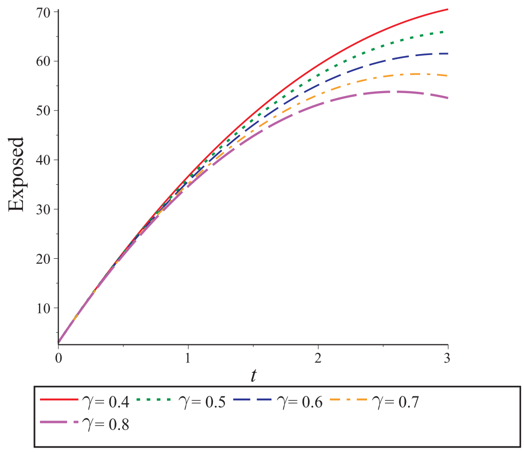

Figure 8: Variation of exposed sensor nodes for different values of rate of recovery γ.

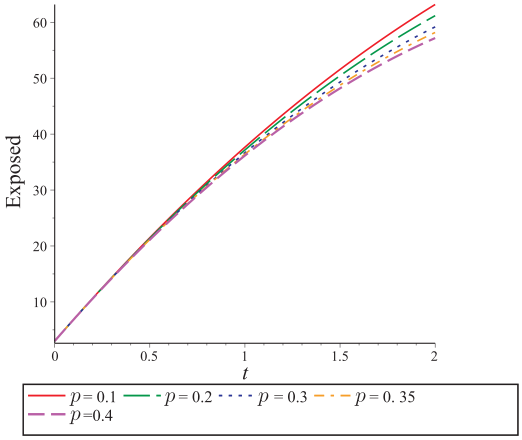

Figure 9: Variation of exposed sensor nodes for different values of rate of vaccination p.

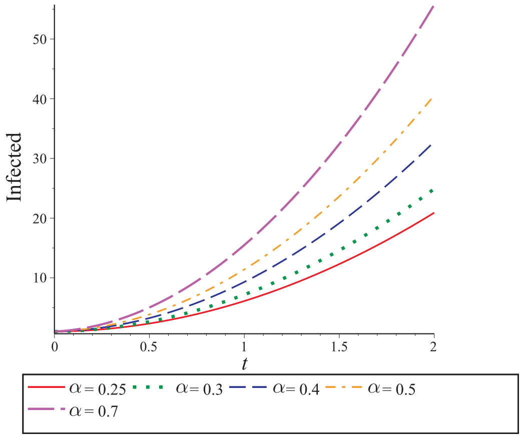

Figure 10: Variation of infected sensor nodes for different values of α.

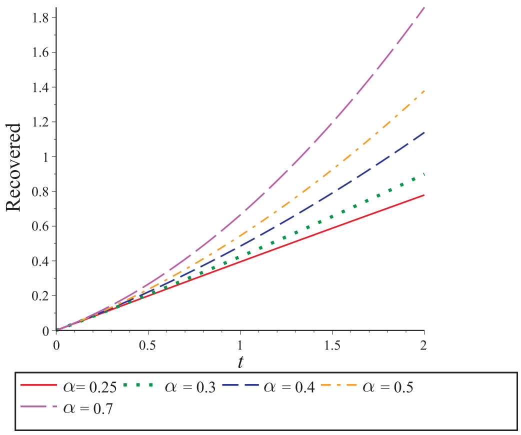

Figure 11: Variation of recovered sensor nodes for different values of α.

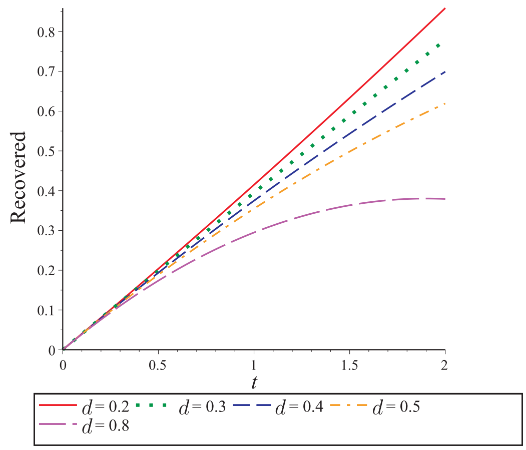

Figure 12: Variation of recovered sensor nodes for different values of d.

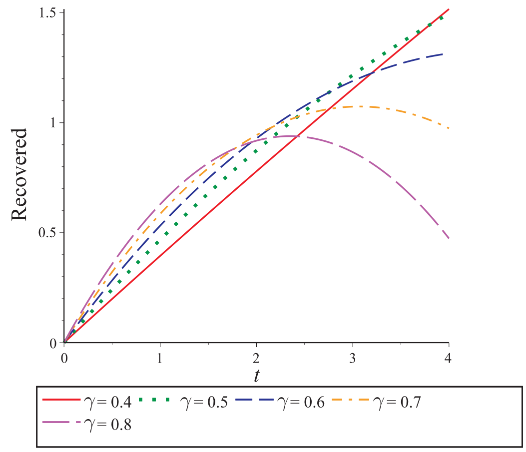

Figure 13: Variation of recovered sensor nodes for different values of rate of recovery γ.

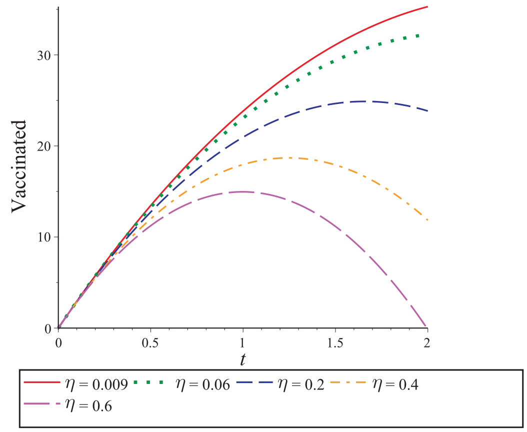

Figure 14: Variation of vaccinated sensor nodes for different values of rate of vaccination p.

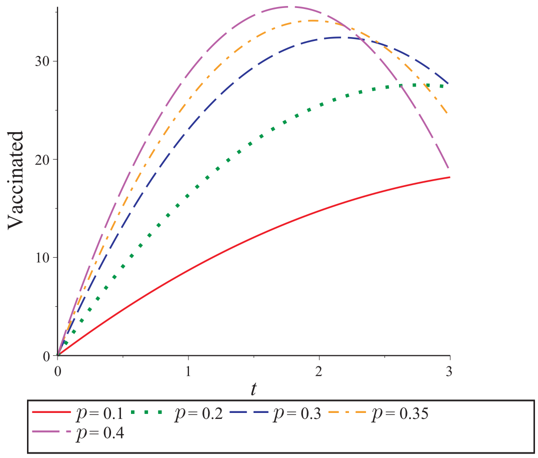

Figure 15: Variation of vaccinated sensor nodes for different values of η.

to the malware. Also proper vaccination is given to the sensor nodes hence susceptibility towards the attack of worms will be low. Thus, we observe a decline in the number of susceptible sensor nodes as they move to the exposed class and recovered class. In Figure 2, the variation of exposed sensor nodes with respect to time is shown. We notice an increase in the number of exposed sensor nodes. This is because the recovered sensor nodes may loss their immunity towards the worm attack and become susceptible, which in turn may get contact into infected. In Figure 3, the variation of infected sensor nodes with respect to time is shown. We notice an increase in the infected sensor nodes as there is an increase in exposed class. But the number of infected nodes is less compared to that of exposed from the graph. This is because of giving proper anti-virus software to those infected sensor nodes. In Figure 4, the variation of recovered sensor nodes with respect to time is shown. There is a slightly steady increase in the graph. This is due to the measure of the vaccination undergone. In Figure 5, variation of the vaccinated sensor node with respect to the time is shown. Initially, there is an increase thereafter we observe a decrease in the curve. This is because of the loss of immunity over the period of time and also inability towards the attack of the new worms. Anti-virus software are capable to protect the sensor nodes from a particular type of worms. When new kind of malware is attacking the nodes the present anti-virus may fail to prevent the nodes.

The susceptible sensor nodes when get in contact with the infected nodes, it will be exposed to the infection. Thus, in Figure 6, we notice that the number of susceptible sensor nodes decreases when the rate of transmission of the nodes from E-class to I-class, α increases. In Figure 7, we notice that when the rate of transmission from V-class to S-class, η increases the susceptible sensor nodes also increases. In Figure 8, we observe that when the vaccinating rate is high, there is a decrease in the number of susceptible sensor nodes, which assures that they are no more susceptible to worm attack. In Figure 9, it shown that if the rate of recovery is more, the number of exposed is less. Further, in Figure 10, it is noticed that if the vaccinating rate is more, the number of exposed is less comparative. In Figure 11, we notice that the number of infected sensor nodes increases when the rate of transmission of the nodes from E-class to I-class, α increases. In Figure 12, it is shown that when the rate of transmission of the nodes from E-class to I-class, α increases, there is an increase in the recovered sensor nodes. If more sensor nodes are infected, then more attention will be taken to recover them from the malware with the proper anti-virus software. But all the new malwares cannot be handled with the same anti-virus software. Thus, is is noted from the graph, that almost two sensor nodes are only recovered in the stipulated time considered. In Figure 13, we observe that when the rate of transmission from R-class to S-class, d increases, there is a decline in the number of recovered sensor nodes. In Figure 14, we notice that faster the recovery rate higher the number of recovered sensor nodes. If the rate at which the sensor nodes are recovering is more, we notice that there is decline in the graph. This is because if the sensor nodes takes more time to recover from the malware attack, the worms may become vulnerable and we might lose the sensor node. In Figure 15, it is shown that if the vaccination rate is more, the number of the sensor nodes who are immune against the malware is also more. But we notice a decline in curve this is because the preventive measure against malware is not permanent. When new malware attacks the sensor nodes the same vaccination might not be effective to protect it. In Figure 16, we infer that if the rate of transmission from V-class to S-class, η increases, the number of vaccinated sensor nodes decreases because of their immunity loss and may become susceptible to the worm attacks.

References

[1] S. Abubakar, N. I. Akinwande, O. R. Jimoh, F. A. Oguntolu and O. D. Oguwumu, *Approximate solution of SIR infectious disease model using homotopy perturbation method,* Pacific Journal of Science and Technology, **14** (2013), 163–169.

[2] G. Adamu, M. Bawa, M. Jiya and U. D. Chado, *A mathematical model for the dynamics of Zika virus via homotopy perturbation method,* Journal of Applied Science and Environmental Management, **21** (2017), 615–623.

[3] F. A. Adesuyi, A. Karawak, O. D. Adeyemi and F. R. Adunola, *A Mathematical Model for capturing Cholera spread and containment options,* International Journal of Mathematical Sciences and Computing, **4** (2018), 15–40.

[4] B. Ebenezer, A. Khan, M. A. Khan and S. Islam, *Solution of the Ebola epidemic model by homotopy perturbation method,* Journal of Applied Environmental and Biological Sciences, **6** (2016), 41–49.

[5] G. Devipriya, *Analytical solution of Dengue model with maturation delay by homotopy perturbation method,* Asia Mathematika, **1** (2017), 49–60.

[6] J. H. He, *Homotopy perturbation technique: A new nonlinear analytical technique,* Applied Mathematics and Computation, **135** (2003), 73–79.

[7] A. Herzog, N. Shahmehri and C. Duma, *An ontology of information security,* International Journal of Information Security and Privacy, **1** (2007), 1–23.

[8] C. Karlof and D. Wagner, *Secure routing in wireless sensor networks: attacks and countermeasures,* Ad Hoc Networks, **1** (2003), 293–315.

[9] M. A. Khan, S. Islam, M. Ullah, S. A. Khan, G. Zaman and S. F. Saddiq, *Analytical solution of the Leptospirosis epidemic model by homotopy perturbation method,* Research Journal of Applied Sciences, **2** (2013), 66–71.

[10] B. K. Mishra and N. Jha, *SEIQRS model for the transmission of malicious objects in computer network,* Applied Mathematical Modelling, **34** (2010), 710–715.

[11] B. K. Mishra and N. Keshri, *Mathematical model on the transmission of worms in wireless sensor network,* Applied Mathematical Modelling, **37** (2013), 4103–4111.

[12] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford and N. Weaver, *Inside the slammer worm,* IEEE Security & Privacy, **1** (2003), 33–39.

[13] R. Senthamarai and S. Balamuralitharan, *Analytical solutions of SIRS-SI Malaria disease model using HPM,* Journal of Chemical and Pharmaceutical Research, **8** (2016), 651–666.

[14] D. Welch and S. Lathrop, *Wireless security threat taxonomy, in information assurance workshop,* 2003. IEEE Systems, Man and Cybernetics Society,(2003), 76–83.

[15] C. Zou, W. Gong and D. Towsley, *Code red worm propagation modeling and analysis,* in Proceedings of the 9th ACM conference on Computer and Communications Security, (2002), 138-147, ACM New York, USA.

Department of Mathematics, Stella Maris College, Chennai - 600 086, INDIA.

E-mail: devipriyaganeshan@gmail.com

PG Department of Mathematics, Women's Christian College, Chennai - 600 006, INDIA.

E-mail: kavits1996@gmail.com