I.J. Mathematical Sciences and Computing, **2017, 4, 37-51**
Published Online November 2017 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijmsc.2017.04.04

Available online at ***http://www.mecs-press.net/ijmsc***

Parametric Equation for Capturing Dynamics of Cyber Attack Malware Transmission with Mitigation on Computer Network

Falaye Adeyinka A[a], Etuk Stella Oluyemi[b], Adama Ndako Victor[c], Ugwuoke Cosmas Uchenna[d],'Olujimi Ogedengbe[e], Seun Ale[f]

[a]Department of Computer Science, Federal University of Technology Minna , Niger state, 920211, Nigeria.
[b]Department of Information and media Technology, Federal University of Technology Minna, Niger state, 920211, Nigeria.
[c]Department of Computer Science, Federal University of Technology Minna, Niger state ,920211 Nigeria.
[d]Department Computer Science, Federal University of Technology Minna, Niger state ,920211 Nigeria.
[e]Integration and support mobile technologies, amuwo odofin industrial estate apapa-oshodi expresss way, Lagos.
[f]Department of Mathematic Science, Federal University of Technology Minna, Niger state ,920211 Nigeria.

Received: 21 December 2016; Accepted: 05 January 2017; Published: 08 November 2017

Abstract

One distress of network and data security professionals and advisers globally is about the abilities of infectious malicious agents (Malware) to invade the entire network terminals to wreak havoc extending from identity theft, financial fraud to systemic digital assault on critical national resources. This work studies the behavioural dynamics of the susceptible, infected, the recovered terminals on the mobile wireless network and the effective use of antivirus security signature as countermeasure. Solving for stability state, we found out that its Eigen value gives a positive value which means that the stability is at an unstable state. Using Homotopy perturbation to calculate the approximate solution of the system. The expression derived was simulated using a mathematical tool (mat lab).

Index Terms: Homotopy Pertubation Method, SIR model, Malicious ware, Stability, Equillibrium.

1. Introduction

One big threat to network security is malware (malicious software) spread Generally the spread of malwares takes place rapidly across the network within few days of outbreak when a susceptible (vulnerable)

* Corresponding author.
E-mail address: [a]falaye.adeyinka@futminna.edu.ng, [b]abiolastella@futminna.edu.ng, [c]Nigeria.vnadama@futminna.edu.ng, [d]ask4cosmas@yahoo.co.uk, [e]Lagos. jimmiog@yahoo.com, [f]profgurujoe@gmail.com

node/system /terminal/user/host handshake with the infected node/system /terminal/user/host in the course of data exchange or during passing of controls and commands.

Against the backdrop of malware incidents regularly becoming a source of major concern due to its destructive nature accounted for by hijacking of devices, private inversion, identity theft, scam running of phishing technical support, radicalization and terrorism: This study will put its search light on the modes of spread, evaluation of counter measure effectiveness and finally to forecast potential outbreak of cyber-attack malwares on the network.

The model to study the dynamics of the spread and propagation of cyber-attack malwares on the network will incorporate more significant parameters like contact and recovery rates to explain the patterns of both infection of the susceptible and the recovery of the infected user or host respectively

The homotopy perturbation method (HPM) which was proposed by Ji-Huan in 1999 will be used as method of solution. In this method, the solution is considered as the summation of an infinite series, which usually converges rapidly to the exact solution. This method is employed to solve the Susceptible, Infected, Recovered (SIR) model proposed by Kermack and McKendrick in 1927.

The HPM method is based on the use of a power series, which transforms the original nonlinear differential equation into a series of linear differential equations. Two continuous functions from one topological space to another are called homotopic if one can be “continuously deformed" into the other, such a deformation being called a homotopy between the two functions. The Homotopy Perturbation Method (HPM), which provides analytical approximate solution, is applied to various linear and non-linear equations.

The aim of this paper is to develop a quantitative frame work that can show the spread and control of general malwares on the mobile wireless network .The study objectives’ includes one, to study and understand the SIR (Susceptible Infected Recovered) epidemiology model equations, two to apply the equation to capture the phenomenon of malware spread and its countermeasure, three to solve and analyse the equilibrium or steady state equations using Homotopy perturbation method to obtain the approximate solution. In summary section II of this paper is an overview of related works, Section III focuses on the formulation of the model. Section IV presents the results while section V discusses the Results. Section VI is a conclusion while recommendations are contained in section VII.

2. Related Works

Outbreaks of Malwares in wireless networks has created an evolving research area (e.g., though, the work on spread of malware has conventionally concentrated on wired networks). Epidemic research works based on the classic Kermack-Mckendrick model has broadly been used in analysing the blow-out of malware in wired networks and recently in wireless networks. From these works, we discovered that, through numerical simulations and matching with actual data, when the number of nodes in a network is large, the deterministic epidemic models can effectively characterize the mode of the spread of the malware D Daley and J Gani (2009). Active control of parameters of the network or the worm have been explored in some research works.

Most of these however do not identify the ideal strategies nor offer verifiable performance securities, but as a substitute propose empirical dynamic strategies in different situations, and assess via simulations the effectiveness and several trade-offs of the strategies they suggest. For example, C Zhou *et al*. proposed heuristics for dynamic quarantining of nodes in wired networks that appear suspicious through traffic analysis, and V.Karyotis and S.Papavassiliou (2007), introduced heuristic strategies for dynamically adjusting the transmission power of attacker nodes in wireless networks. We instead obtain attack policies that provably attain the maximum possible damage and consider a general model that incorporates healing, immunization and mortality of nodes. Interestingly, tools from the optimal control theory such as the effective theorem of Pontryagin maximum Principle has rarely been used for analysing network security X. Yan and Y. Zou and our previous work M. Khouzani *et al*. constitute notable exceptions.

The first formulates the trade-off for optimal treatment of the infective nodes in wired networks. However, in contrast to our work, the solution is based on numerical evaluations only and no structural property of the optimal policy is established. One of our earlier works M. Khouzani *et al*. proposed reduction of reception gain of wireless nodes as a counter-measure for slowing down the spread of malware in wireless networks. Another one of their papers focuses on the attack viewpoint and considers the transmission range of the infective nodes and the rate of killing as two independent dynamic parameters of the worm to inflict the maximum damage. In particular, killing a node is achieved by executing a malicious code damaging a vital part of the hardware. Moreover, M. Khouzani *et al.* considered a worm with a power budget which specifically ensures that every infective node lasts the entire duration of interest. In contrast, we consider the case in which the killing process of the infective nodes is not independent of the energy-greedy media access activities. Furthermore, we consider another side-effects of an aggressive media access activity, which is exposing an anomaly and hence, easier detection of the malware.

Falaye *et al* (2016) in their work on dynamics SCADA systems said population of the infectious power line carriers stabilizes mostly due to the implementation of anti-virus signatures which at some points gradually detects infected USB devices. After some days, the population of the infectious power line carriers begins a rapid declination due to the disinfection of the infected USB devices by the anti-virus signatures until the infected power line carriers goes into extinction totally after few days.

One major concern of cyber security experts and consultants is the tendency of treat agents to invade the entire network land scape to hijack devices, invade privacy and also wreck havocs on the entire system network. Falaye *et al (2016).*

3. Formulation of the Model

A model formulation includes basic assumptions of the model which are undoubtedly specified while relating these assumptions from the real world to the mathematical model. The assumptions of the model include:

- The entire population is divided into three (3) compartments i.e. the Susceptible Class, the Infectious Class and the Recovered Class; all based on their epidemiological status
- New nodes are being recruited on the system network at a constant rate.
- The interaction between the susceptible systems and the infected systems is constant and as a result, more systems are being infected
- Some of the infected systems terminates as a result of the malware, while some get recovered due to the usage of anti-virus signature.
- Finally, all interactions within the network occur homogeneously.

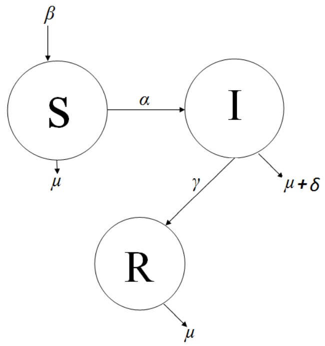

Fig.1. The Schematic Diagram of Malware Transmission on a System Network.

Table 1. The model Variables

Variables of the Model
S = Susceptible/Vulnerable Systems on network
I = Infectious Systems on network
R= Recovered Systems on network
t = time (days)
N= Total Population size of both Susceptible, Infectious and Recovered.

Table 2. Model Parameters

Parameters of the Model
β = Infectious Systems on network
μ = Recovered Systems on network
γ = time (days)
α = Total Population size of both Susceptible, Infectious and Recovered.
δ = rate at which systems terminate due to infection.

Translating our assumptions into mathematical relationship. We have the rate of increase in the population rate of the susceptible systems without interaction with the infected systems is denoted as

$$\frac{ds}{dt} = \beta S - \mu S - \alpha SI \tag{1}$$

$$\frac{dI}{dt} = \alpha SI - (\gamma + \mu + \delta)I \tag{2}$$

$$\frac{dR}{dt} = \gamma I - \mu R \tag{3}$$

3.1. Model Equation

The standard SIR model equation for susceptible, infected and recovered classes giving by is the equation 4,5,6;

$$\frac{dS}{dt} = \beta S - \alpha SI - \mu S, S(0) = S_0 \tag{4}$$

$$\frac{dI}{dt} = \alpha SI - (\gamma + \delta + \mu) I, I(0) = I_0 \tag{5}$$

$$\frac{dR}{dt} = \gamma I - \mu R, R(0) = R_0 \tag{6}$$

3.2. Equilibrium Points

To obtain the first equilibrium point; we set the derivatives to zero.

$$\frac{dS}{dt} = 0, \frac{dI}{dt} = 0, \frac{dR}{dt} = 0 \tag{7}$$

$$\beta S - \alpha SI - \mu S = 0 \tag{8}$$

$$\alpha SI - (\gamma + \delta + \mu) = 0 \tag{9}$$

$$\gamma I - \mu R = 0 \tag{10}$$

P$_1$=first equilibrium point

P$_1$= [S, I, R] = [0, 0, 0,] (11)

Equation 11 gives the malware free equilibrium.
Endemic Equilibrium point p_2

$$p_2 = [\text{S=}\frac{(\gamma + \delta + \mu)}{\alpha}\text{), I=}\frac{\beta - \mu}{\alpha}\text{, R=}\ \gamma(\frac{\beta - \mu}{\alpha\mu})\ ] \tag{12}$$

3.3. Stability Analysis

$$u\sin g\ \ jacobian\ \ metrix\ \ given\ by$$

$$j = \begin{bmatrix} \frac{df_1}{dS} & \frac{df_1}{dI} & \frac{df_1}{dR} \\ \frac{df_2}{dS} & \frac{df_2}{dI} & \frac{df_2}{dR} \\ \frac{df_3}{dS} & \frac{df_3}{dI} & \frac{df_3}{dR} \end{bmatrix} \tag{13}$$

$$Df[S,I,R] = \begin{bmatrix} (\beta-\mu)-\alpha I & -\alpha & 0 \\ \alpha I & \alpha S-(\gamma+\delta+\mu) & 0 \\ 0 & \gamma & \mu \end{bmatrix}$$

$$the\ \ linearization\, at\ \ p_1\, is\ \ given\ by$$

$$\begin{bmatrix} (\beta-\mu)-\alpha I & -\alpha & 0 \\ \alpha I & \alpha S-(\gamma+\delta+\mu) & 0 \\ 0 & \gamma & -\mu \end{bmatrix}$$

$$Df[0,0,0] = \begin{bmatrix} \beta-\mu & -\alpha & 0 \\ 0 & -(\gamma+\delta+\mu) & 0 \\ 0 & \gamma & -\mu \end{bmatrix} \tag{14}$$

Transforming the above in the sequence of *a;*

$$(\beta-\mu) = a_1; -\alpha = a_2; -(\gamma+\delta+\mu) = a_3; \gamma = a_4; -\mu = a_5 \tag{15}$$

$$\textit{the eigen value is given by } |A-\lambda I| = 0 \tag{16}$$

Thus the Eigen values are

$$a_1, = a_3 = a_5 = \lambda \tag{17}$$

3.4. Stability Analysis Discussion.

Stability properties of linear systems

Eigen Values	**Types of critical points**	**Stability**
$\lambda_1 \succ \lambda_2 \succ 0$	Improper node	unstable
$\lambda_1 \prec \lambda_2 \prec 0$	Improper node	asymptotically unstable
$\lambda_2 \prec 0 \prec \lambda_1$	Saddle point	unstable
$\lambda_1 = \lambda_2 \succ 0$	Proper or improper node	unstable
$\lambda_1, \lambda_2 = r + i\mu$	Spiral point	unstable
$\lambda_1 = i\mu, \lambda_2 = -i\mu$	Centre	stable

Therefore, the Eigen value shows that it is unstable

3.5. Homotopy Perturbation Method

We apply Homotopy perturbation to our equation *1.13*, *1.14* and *1.15* on follows:
Applying HPM 1.13 we have

let

$$S = (x_0 + px_1 + p^2 yx_2 + \cdots), \qquad I = (y_0 + py_1 + p^2 y_2 + \cdots)$$

$$R = (z_0 + pz_1 + p^2 z_2 + \ldots)$$

$$(1-p)\frac{dS}{dt} + p\left[\frac{dS}{dt} + \alpha SI + \mu S - \beta\right] = 0$$

$$(1-p)(x_0' + px_1' + p^2x_2' + \cdots)\text{+p}$$
$$x_0' + px_1' + p^2\, x_2' + .. + \alpha(x_0 + px_1 + p^2x_2 + \ldots)((y_0 + py_1 + p^2\, y_2 + \ldots) + \mu(x_0 + px_1 + p^2x_2 + \ldots) - \beta\}\} = 0$$

$$\big((x_0' + px_1' + p^2x_2' - px_0' - p^2x_1' - p^3x_2')(px_0' + p^2x_1' + p^3x_2' + \alpha px_0\, y_0 + \alpha p^2x_0\, y_1 + \alpha p^3x_0\, y_2 + \alpha p^2x_1y_0 + \alpha p^3x_1y_1 + \alpha p^4x_1y_2 + \alpha p^3x_2y_0 + \alpha p^4x_2y_1 + \alpha p^5x_2y_2 + \mu px_0 + \mu p^2x_1 + \mu p^3x_2) - \beta p\big) \quad =0$$

Collecting the coefficient of powers of p we have

$$p^0 : x_1' = 0$$

$$p^1 : x_1' + \alpha x_0\, y_0 + \mu x_0 - \beta = 0$$

$$p^2 : x_0' + \alpha(x_0\, y_1 + x_1\, y_0) + \mu x_1 = 0$$

Applying HPM to 3.14 we have:

$$(1-p)\frac{dI}{dt} + p\left[\frac{dI}{dt} - \alpha SI + (\gamma + \delta + \mu)I\right] = 0$$

Expanding the expression above, we have:

$$(y_0' + py_1' + p^2y_2' - py_0' - p^2y_1' - p^3y_2') + p[(y_0' + Py_1' + P^2\, y_2' + \ldots) - \alpha(x_0 + Px_1 + P^2x_2 + \ldots) + (y_0 + Py_1 + P^2\, y_2 + \ldots) + (\gamma + \delta + \mu)(y_0 + py_1 + p^2\, y_2 + \ldots)] = 0$$

Collecting the coefficients of powers of p we have:

$$p^0 : y_0' = 0$$

$$p^1 : y_1' - \alpha x_0\, y_0 + (\gamma + \delta + \mu)y_0 = 0$$

$$p^2 : y_2' - \alpha(x_0\, y_1 + x_1\, y_0)$$

$$+ (\gamma + \delta + \mu)\, y_1 = 0$$

Applying HPM to 1.15, we have:

$$\text{(1-p)}\frac{dR}{dt} + p\left[\frac{dR}{dt} + \mu R - \gamma \mathrm{I}\right] = 0$$

Expanding the expression, we have:

$$(1-p)(z_0' + pz_1' + p^2z_2' + \ldots) + p[(z_0' + Pz_1' + P^2\, z_2' + \ldots) + \mu(z + Pz_1 + P^2z_2 + \ldots) - \gamma(y_0 + Py_1 + P^2\, y_2 + \ldots)] = 0$$

$$(z_0' + pz_1' + p^2z_2' - pz_0' - p^2z_1' - p^3z_2') + p[(z_0' + Pz_1' + P^2\, z_2' + \ldots) + \mu(z + Pz_1 + P^2z_2 + \ldots) - \gamma(y_0 + Py_1 + P^2\, y_2 + \ldots)] = 0$$

Collecting the coefficients of powers of p we have:

$$p^0 : z_0' = 0$$

$$p^1 : z_1' + \mu z_0 - \gamma y_0 = 0$$

$$p^2 : z_2' + \mu z_1 - \gamma y_1 = 0$$

According to Homotopy perturbation method, the approximate solution of equation can be expressed as a series of the power of P i.e.

$$x(t) = \lim_{p \to 1} x_0(t) + px_1(t) + p^2 x_2(t) + \ldots.$$

$$x(t) = x_0(t) + x_1(t) + x_2(t) + \ldots..$$

i.e.

$$S(t) = S_0 + [(\beta - \alpha S_0 I_0 - \mu S_0)t] - \{\alpha S_0 I_0 [\alpha S_0 - (\gamma + \delta + \mu) + (\beta - \alpha S_0 I_0 - \mu S_0)(\alpha I_0 + \mu)]\} \frac{t^2}{2}$$

$$y(t) = \lim_{p \to 1} y_0(t) + py_1(t) + p^2 y_2(t) + \ldots.$$

$$y(t) = y_0(t) + y_1(t) + y_2(t) + \ldots.$$

$$I(t) = I_0 + [\alpha S_0 - (\gamma + \delta + \mu)] I_0 t + \{I_0 [\alpha S_0 - (\gamma + \delta + \mu)]^2 + \alpha I_0 (\beta - \alpha S_0 I_0 - \mu S_0)\} \frac{t^2}{2}$$

$$z(t) = \lim_{p \to 1} z_0(t) + pz_1(t) + p^2 z_2(t) + \ldots.$$

$$z(t) = z_0(t) + z_1(t) + z_2(t) + \ldots..$$

$$R(t) = R_0 + [(\gamma I_0 - \mu R_0)t] + \{\gamma I_0 [\alpha S_0 - (\gamma + \delta + \mu)] - \mu(\gamma I_0 - \mu R_0)\} \frac{t^2}{2}$$

4. Results

In this section we present the results obtained as given below.

4.1. Tables and Graphical Presentation

In this section, the tables and graphical representation were realized using the approximate solution of the Homotopy perturbation model equation for the S, I, R. using math lab software to plot the graph and to generate the tables.

In generating the tables, we use hypothetical values for contacting rate and the recovery rate.

Table 3. Low Contacting Rate and High Recovery Rate (α=0.001 and γ=0.15).

T	S(t)	I(t)	R(t)
0	50.0000	20.0000	10.0000
1	50.6600	17.3266	12.6300
2	49.5400	16.2065	14.8200
3	46.6400	16.6396	16.5700
4	41.9600	18.6260	17.8800
5	35.5000	22.1656	18.7500
6	27.2600	27.2585	19.1800
7	17.2400	33.9046	19.7000
8	5.4400	42.1040	18.7200
9	-8.1400	51.8566	17.8300
10	-23.5000	63.1625	16.5000

Simulated result for β = 0.2, α = 0.001, δ = 0.01, μ = 0.015, γ = 0.15, S_0= 50, I_0= 20, R_0= 10.

Table 3. is a table that shows the behavior of a system when the contacting rate of systems on the network is lower and the rate at which these systems recovers from the malwares infection. We see from the table that the decrease was not too noticeable in susceptible and the decrease in infected individuals was much noticed due to the recovery rate that was high, and the rate of recovery was increasing.

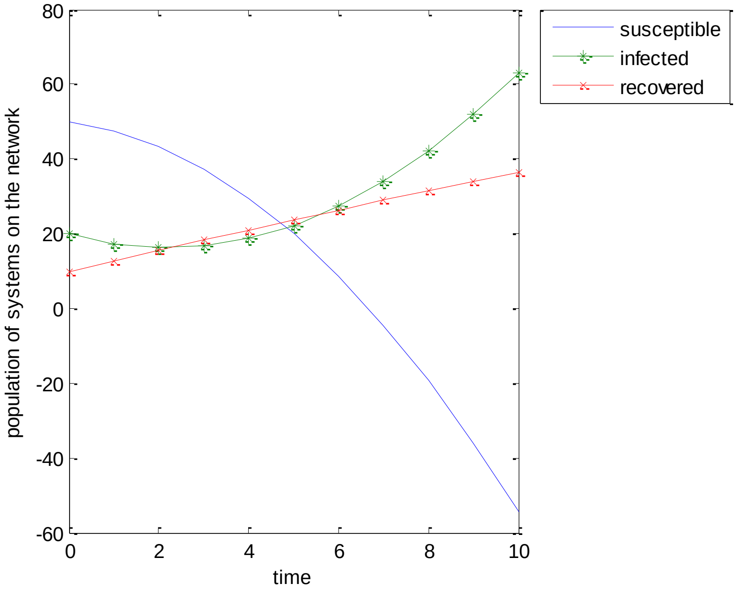

Fig.1. Graph for low contacting Rate and High Recovery Rate (α= 0.001 and γ= 0.15).

Figure 1. is the graph that displays the pictorial representation of the behaviors of the table above where the blue line in the graph symbolizes the behavior of the population of the susceptible systems that was declining, the green line symbolizes that infected systems which was increasing gradually and the red coloured line symbolizes the population of recovered systems.

Table 4. High Contacting Rate and High Recovery Rate (α=0.002 and γ=0.15).

T	S(t)	I(t)	R(t)
0	50.0000	20.0000	10.0000
1	48.1412	20.41226	12.7677
2	46.1949	22.3705	15.3710
3	44.1609	25.8736	17.8098
4	42.0394	30.9220	20.0840
5	39.8303	37.5156	22.1938
6	37.5337	45.6545	24.1390
7	35.1494	55.3386	25.9198
8	32.6776	66.5680	27.5360
9	8.1182	79.3426	28.9877
10	-15.4713	93.6625	30.2750

Simulated result for β=0.2, α=0.002, δ=0.01, μ=0.015, γ=0.15, S_0=50, I_0=20, R_0=10.

Table 4 is a table that shows the behavior of a system when the contacting rate of systems on the network is high and the high rate at which these systems recovers from the malwares infection. We see from the table that the decrease was noticeable in susceptible and the increase in infected individuals was much noticed due to the recovery rate that was high, and the rate of recovery was increasing.

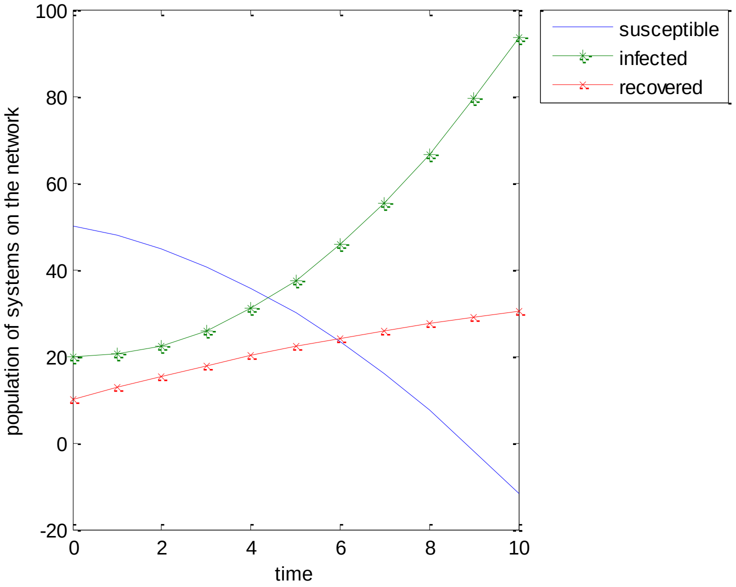

Fig.2. Graph of Response of Population of Systems on the Network Amidst High Contact and High Recovery Rate (α= 0.002 and γ= 0.15).

Figure 2. is the graph that displays the pictorial representation of the behaviors of the table above where the blue line in the graph symbolizes the behavior of the population of the susceptible systems that was declining, the green line symbolizes that infected systems which was increasing gradually and the red coloured line symbolizes the population of recovered systems.

Table 5. Low Contacting Rate and Low Recovery Rate (α=0.001 and γ=0.1).

T	S(t)	I(t)	R(t)
0	50.0000	20.0000	10.0000
1	48.3931	18.3116	11.6450
2	46.6725	12.1465	12.8800
3	44.8382	8.5046	13.7050
4	42.8901	-9.3859	14.1200
5	40.8282	-20.7905	14.1250
6	38.6527	-32.7183	15.7200
7	38.3634	-40.1694	16.9050
8	33.9603	-49.1437	17.6800
9	31.4435	-59.4212	18.0450
10	28.8130	-71.6260	19.0000

Simulated result for β=0.2, α=0.001, δ=0.01, μ=0.015, γ=0.1, S_0=50, I_0=20, R_0=10.

Table 5 shows the behavioural dynamics of Malware infection when the contacting rate of the infected nodes with Susceptible nodes on the network is low on low recovery rate for the infected nodes .Consequently, we see from the table that the decrease in the Susceptible nodes in this instance was may not be very si when compare with when the contacting rate was high with the Infected. Albeit the increase in infected individuals nodes was much noticeable due to the recovery rate that was high resulting in the population of recovered individuals nodes increasing.

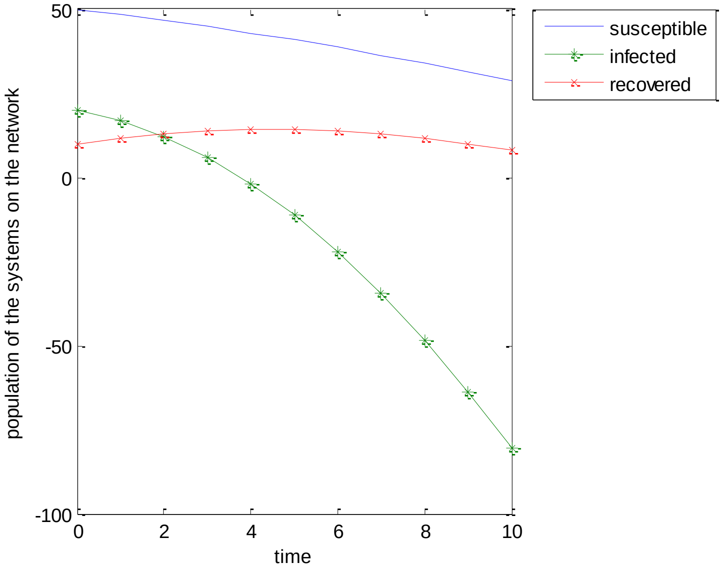

Fig.3. Graph for Low contacting Rate and Low Recovery Rate (α= 0.001 and γ= 0.1).

Figure 3 is the graph that displays the pictorial representation of the behaviours of the table above where the blue line in the graph symbolizes the behaviour of the population of the susceptible systems that was declining but not very much, the green line symbolizes that infected systems which was decreasing gradually and the red coloured line symbolizes the population of recovered systems.

Table 6. High Contacting Rate and Low Recovery Rate (α=0.002 and γ=0.1).

T	S(t)	I(t)	R(t)
0	50.0000	20.0000	10.0000
1	47.3660	35.8758	11.6450
2	44.5640	48.3030	12.8800
3	41.5940	57.2819	13.7050
4	38.4560	62.8122	14.1200
5	35.1500	64.8941	14.1250
6	31.6760	63.5257	13.7200
7	28.0340	58.7124	12.9050
8	24.2240	50.4488	11.6800
9	20.2460	38.7368	10.0450
10	16.1000	23.5762	8.0000

Simulated result for β=0.2, α=0.002, δ=0.01, μ=0.015, γ=0.1, S_0=50, I_0=20, R_0=10.

Table 6 is a table that shows the behaviour of a system when the contacting rate of systems on the network is high and the low rate at which these systems recovers from the malwares infection. We see from the table that there was decrease in susceptible and the increase in infected individuals was much noticed due to high contact rate cum low recovery rate, and the population of recovered individuals was increasing.

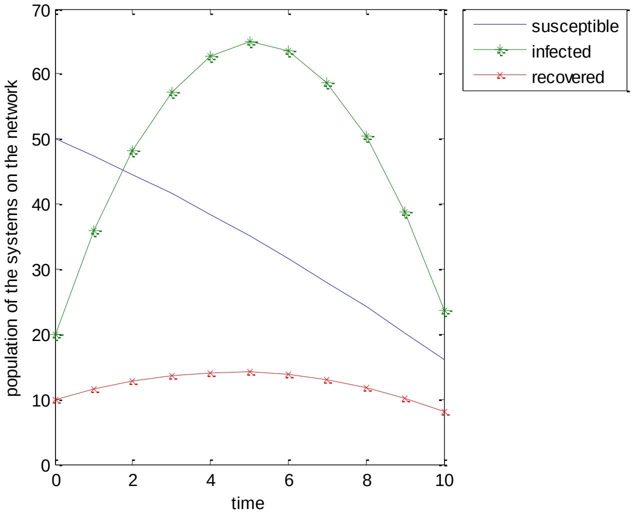

Fig.4. Graph for High contacting Rate and Low Recovery Rate (α= 0.0002 and γ= 0.1).

Figure 5 is the graph that displays the pictorial representation of the behaviours of the table above where the blue line in the graph symbolizes the behaviour of the population of the susceptible systems that was declining, the green line symbolizes that infected systems which was increasing was very noticed for long period before declining gradually and the red coloured line symbolizes the population of recovered systems.

5. Discussion of Results, Conclusion and Recommendation

In this section we discuss the results obtained as given below.

5.1. Discussion of Results

Table 3 and Figure 1 are low contacting rate, α= 0.001 and high recovery rate, γ= 0.15. This shows that the population of susceptible system and infected system were decreasing, while the population of recovered system was increasing and this shows that as malware breakout efforts are made to tackle it and over time the infected system will be moved to recovered system.

Table 4 and Figure 2 are high contacting rate, α= 0.002 and high recovery rate, γ= 0.15. The graph shows that the population of susceptible system and infected system decreased more than when the contacting rate was low but the population of recovered system increased. The more infected system the lesser the susceptible systems population and the more effort are made to eradicate the malware from the population.

Table 5 and Figure 3 are low contacting rate, α= 0.001 and low recovery rate, γ= 0.1. The graph shows that the population of recovered systems is not as high as when the contacting rate is high.

Table 6 and Figure 4 are high contacting rate, α= 0.002 and low recovery rate, γ= 0. The malware infected population was on the high increase compared to other results. The malware will remain on the network for a longer time before a new anti-malware code is made available to counter the persistent of malwares and then the network recovers.

6. Conclusion

The use of Homotopy Perturbation Method (HPM) has enabled us to get the approximate solution of each compartment of the Model. The approximate solution was to present the Model graphically, which gives us the understanding to tackle the malware. It is obvious from the results that whether high or low contact rate, the recovered system population increases; though it increase more with high usage of control measures such as anti-virus which leads to quick recovery of infected systems. The number of recovered system population depends on the contact rate. It is clear that once there is malware breakout, efforts are made to get rid of the malware from the entire system network.

7. Recommendation

Malwares cannot be completely eliminated from the network because new forms of malware spring up frequently. The research recommends that in order to control the spread of malwares, systems on network should have an up to date anti malware packages installed on them. The access point for all system on the network should be protected.

The research also recommends that access to malicious sites and nodes should be restricted. The aforementioned recommendations were made by the study.

References

[1] Badakhshan B and Ariter D, (2007.) *Simulation Based Analysis of Spreading Dynamics of Malware in Wireless Sensor Networks*," International Conference on Sensor Technologies and Applications, 2007.Sensor Comm 2007. Publication Date: 14-20 Oct. 2007, page(s): 164 – 169.

[2] Davis N, Abbott L, Park J & James (2006): Epidemiology, Bio-mathematical Modeling, Demographic Analysis, Network Stealth Worms, Network Security. Blacksburg, Vol. 2; No 1, 149-156.

[3] Daley D and Gani J. *Epidemic modelling: an introduction*. Cambridge Univ Pr, 2001.

[4] Debany W. H, *Modeling the spread of internet worms via persistently unpatched hosts*," IEEE Network, Volume 22, Issue 2, March-April 2008 Page(s): 26-32.

[5] Falaye A, Osho O, Emehian M, Ale S. Dynamics of SCADA System Malware: Impacts on Smart Grid Electricity Networks and Countermeasures. International Conference on Information and Communication Technology and Application. ICTA 1st ed. Nigeria: 2016.

[6] Falaye A, Osho O, Emehian M, Ale S. Dynamics of SCADA System Malware: Impacts on Smart Grid Electricity Networks and Countermeasures. International Conference on Information and Communication Technology and Application. ICTA 1st ed. Nigeria: 2016.

[7] Garetto M, (1995) "*Modeling Malware Spreading Dynamics,*" extended version, http://www1.tlc.polito.it/˜garetto/pub/ virusreport.ps.gz

[8] Juil C. Martin 1, Legand L. Burge, Washington(2005) *Modeling the Spread of Mobile Malware* Department of Systems & Computer Science, Howard University2300 Sixth St. NW, Washington, DC, 20059 Department of Physics and Astronomy, Howard University 2355 Sixth St. NW, Washington, DC, 20059.

[9] Karyotis V. and Papavassiliou S., "Risk-based attack strategies for mobile ad hoc networks under probabilistic attack modeling framework," *Computer Networks*, vol. 51, no. 9, pp. 2397–2410, 2007.

[10] Khouzani M., Altman E., and Sarkar S., "Optimal Quarantining of Wireless Malware Through Power Control," in *Proceedings of the Fourth Symposium on Information Theory and Applications*, University of California at San Diego, 2009.

[11] Khouzani M., Sarkar S., and Altman E., "Maximum Damage Malware Attack in Mobile Wireless Networks," *To appear in Infocom 2010.*

[12] Nikola v. & Ljupco K (2009): *Modeling Malware Propagation in Networks* Macedonian Academy of Sciences and Arts, Skopje, Macedonia. University of California San Diego, La Jolla, CA, USA.

[13] O'Donnell J, *When Malware Attacks* (Anything but Win-dows)," IEEE Security & Privacy, Volume 6, Issue 3, May-June 2008, Page(s):68-70.

[14] Yan x and Y. Zou, "Optimal Internet Worm Treatment Strategy Based on the Two-Factor Model," *ETRI JOURNAL*, vol. 30, no. 1, p. 81, 2008.

[15] Zhu Z., Cao G., Zhu S., Ranjan S., and Nucci A. "A social network based patching scheme for worm containment in cellular networks," *IEEE INFOCOM.*

[16] Zou C C., Gong W., Towsley D., (2002) "*Code Red Worm Propagation Modeling and Analysis,*" 9th ACM Conference on Computer and Communications Security.

[17] C. Zou, W. Gong, and D. Towsley, "Worm propagation modeling and analysis under dynamic quarantine defense,"in *Proceedings of the 2003 ACM workshop on Rapid Malcode*, pp. 51–60, ACM New York, NY, USA, 2003.

Authors' Profiles

Mr. Adeyinka Adesuyi Falaye (October 7, 1974) is currently a lecturer at the School of Information and Communication Technology, Department of Computer Science, Federal University of Technoloy Minna,Nigeria. Prior to this in 2007 through 2016, he was a Lecturer at Department of Mathematics and Statistics in the same University.He received his MS, and BTECH in Computer Science from University of Lagos (Nigeria) and Mathematics with Computer Science from Federal University of Technology, Minna (Nigeria) respectively. His research is mainly focused on Cyber security within Critical National Infrastructure, System Modelling & Simulation, Risk Management, Complex and Policy Analysis and Epidemiology.

Etuk Stella Oluyemi (May 23, 1986) is a Lecturer at the Information and media Technology department, of the Federal University of Technology Minna, Niger State. Her research area of interests is in Applied Mathematics.

Adama Ndako Victor (born March 4, 1985) is a Lecturer at the Computer Science department, of the Federal University of Technology Minna, Niger State. His research area interests are in the following HCI and Security Systems.

Ugwuoke Cosmas Uchenna (born July 3, 1977) is a Lecturer at the Computer Science department, of the Federal University of Technology Minna, Niger State. His research area interests are in the following Computer Networks and Mobile Security.

Olujimi Ogedengbe (born November 14, 1982) is an integration Engineer with Mobile Technologies. His area of interest is majorly in computing and system interactions.

Gbenga Olugbodi Jonathan was a student from Federal University of Technology Minna .His research area of interest include mathematical modelling.

How to cite this paper: Falaye Adeyinka A, Etuk Stella Oluyemi, Adama Ndako Victor, Ugwuoke Cosmas Uchenna, Olujimi Ogedengbe, Seun Ale,"Parametric Equation for Capturing Dynamics of Cyber Attack Malware Transmission with Mitigation on Computer Network", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.3, No.4, pp.37-51, 2017.DOI: 10.5815/ijmsc.2017.04.04