FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 8 No. 4, August, 2024, pp 105 - 119
DOI: https://doi.org/10.33003/fjs-2024-0804-2284

A DYNAMICAL MODEL OF COMPUTER VIRUS WITH INFECTIVE EXTERNAL STORAGE DEVICE

***[1]Nwaokolo, Martin Afam, [2]Gweryina, Reuben Iortyer and [2]Ogohi, Nissy Ufedo**

[1]Department of Mathematics and Statistics, Federal University Wukari, Taraba, Nigeria.
[2]College of Sciences, Mathematics /Statistics /Computer Science, Joseph Sarwuan Tarka University, Makurdi, Benue State, Nigeria.

*Corresponding authors' email: nwaokoloafam2@yahoo.com

ABSTRACT
A computer virus is a type of malicious software program ("Malware") that, when executed, replicates itself by modifying other computer programs and inserting its own code. Most of our computer systems, media devices and storages are victims of computer virus. Due to the continuous infections of computer systems, several studies and works are being done on the transmission, dynamics and epidemiology of computer virus. It is a major source of concern due to the importance and necessity of the computer system and the usefulness of the internet. Based on the menace caused by the virus to computers, the researcher decided to carry out this work so as to to investigate the propagation effects of computer viruses with infective external storage media on computer systems. In this work, a mathematical model of a dynamical system of computer virus with an infected external storage media on viral spread is formulated, by extending a four-compartment model proposed by Peng et al, (2013) to five compartments. We computed the reproduction potential, the local and global stability analysis of. Numerical simulation shows that when there is no repair for the exposed computers, the infection rate is high ($k = 0$), but when exposed computers are being repaired, there is reduction in the number of exposed and infected computers ($k \neq 0$).

Keywords: Computer virus, Internet, Continuous infections, Software program, Storage media

INTRODUCTION

The advent of Internet technology led to a drastic change in the way data is transferred and information exchange takes place. Internet technology usage has grown, offering numerous functionalities and facilities. This growth has thrown severe challenges in increasing attacks on cyber world (Mishra et al 2012) and in the form of requirements for a suitable cyber defense system to safeguard valuable information's stored on computer systems (Saini, 2012). Alas, they have not received much scientific scrutiny. There are varying views as regards the definition of a computer virus, but it is generally accepted that a virus contains a program code that can explicitly copy itself, and by doing so has the ability to infect other programs by modifying them or their environment. Computer viruses trace their pedigree to John von Neumann's studies of self-replicating mathematical automata in the 1940s. Although the idea of programs that could infect computers dates to the 1970s, the first well-documented case of a computer virus spreading "in the wild" occurred in 1986 (Solomon, 1995), when a code snippet known as the "Brain" virus appeared on several dozen diskettes at the University of Delaware. Today viruses afflict at least a million computers every year. Users spend several hundred million dollars annually on antivirus products and services, and this figure is growing rapidly. Computer systems of about 233 million as at January, 2004 (Mishra et al, 2007) that makes use of the internet, are prone to threats from various malicious objects such as worms, virus, Trojan horse, spam etc. According to Symantec Security Response Definitions (2010), the number of computer virus has been increasing exponentially from their first appearance in 1986 to over 74 000 different strains identified today. These spread over the Internet and may attack computers through; Secondary memory (Floppy, Hard Disk, CD-ROM, USB devices etc.), E-mail (Attachments), Instant Messaging (FTP, Text Messaging, Chat etc.), Phishing and malicious Bot Programs. These malicious codes can replicate themselves and spread among computers (Zhang, et al 2013), the spread of computer viruses still causes enormous financial losses that large organizations suffer for computer security problems (Serrazi et al, 2003; Gan et al 2015).The most devastating computer virus to date is "My Doom", which caused over $38 billion in damages (Zhu et al, 2012)thus; individuals and organizations are troubled by computer viruses.As an alternative to the anti-virus technique, understanding the epidemic dynamics of computer viruses is critical to appreciating the way the computer viruses can spread across networks and to work out robust policies of inhibiting their prevalence (Rahaman et al, 2015). Cyber defence is as a result of these various malicious objects and technologies misused for scams. To provide defences against them, awareness about the behaviour of these malicious objects, their features, propagating methods, means and their limitations using mathematical modelling is vital. To understand this effect, studies have been carried out on self-replication and self-propagation of malicious objects such as virus, worm, Trojan horse, Bots etc. (Saini, 2011). The dynamical mathematical modelling of the spread process of computer virus is an effective approach in understanding the behaviour of computer viruses and how to prevent infection (Gan, et al 2014) because on this basis, some effective measures can be posed to prevent infection (Peng et al, 2013). It also helps decision makers to develop strategies to control the spread of computer viruses.

Modeling is the study of a system before it is built and implemented. Often times, it is usually not feasible to implement a system or real-world problem in the actual environment due to huge cost and time. So, it is preferable to build a prototype or model and study the behavior of the system. A model is not only a substitute of the actual system, it also a simplification of the system (Saini et al 2007). Understanding the behavior of malicious objects is a necessity to mitigate cyber-attacks. For this mathematical modeling plays an important role. It can help to fix the possible parameters of the malicious object which are important to tell

how the malicious object can propagate in computer systems and networks.

MATERIALS AND METHODS

This chapter presents a dynamical model of a computer virus with infective external storage devices. We shall attempt to find - the computer virus free equilibrium, -the reproduction number with its analysis and the local and global stability of the disease-free equilibrium.

Model Formulation

The model described below comprises of four compartments: Susceptible computers, the Exposed computers, the Infectious computers and the Recovered computers denoted by their corresponding numbers at time t - S(t), E(t), I(t), R(t). Without ambiguity; S(t), E(t), I(t), R(t) will be abbreviated as SEIR respectively.

The susceptible computers (S) represent the uninfected computers and new computers that have not been infected with the virus. The exposed (E) computers represent the computers which have been infected with the virus but have not yet broken-out, while the infectious computers (I) are those computers that have been infected with the virus and have broken-out. Then the recovered computers (R) are the computers that are virus free and have immunity (Peng *et al, 2013*).

Assumptions of the Basic Model

According to *Peng et al, (2013)*, the basic model above has the following assumptions:

i. The computer virus has a latent period during which individuals are exposed to a computer virus but are not yet infectious.
ii. The computer virus also has latency, and the computer also has infectivity in the period of latency (*Yang et al, 2014*).
iii. The newly entered in the internet from the susceptible status to exposed status, the contact rate is the same as that of susceptible status entering into infected status.
iv. The computers which newly entered the internet are susceptible, the computers correspond with exposed computers and their adequate contact rate (β_1), and computers also correspond with infected computers and their adequate contact rate (β_1).
v. The fraction of the computer which newly entered the internet will enter the class R by anti-virus software.
vi. The fraction of computers contact with exposed and infected computer will stay latent before becoming infectious and enter a class

Parameters of the Basic Model

Table 1: Parameters of the basic model (Peng et al, 2013)

Parameters	Description
N	Rate at which external computers are connected to the network.
P	The recovery rate of susceptible computer due to the anti-virus ability of network.
K	Recovery rate of exposed computer due to anti-virus ability of network.
β_1	Rate at which when having a connection to one infected computer, one susceptible computer can become exposed but not broken-out.
β_2	Rate at which when having connection to one exposed computer, one susceptible computer can become exposed.
α	Rate at which the exposed computers cannot be cured by anti-virus software and broken-out.
r	Recovery rate of infected computers that are cured.
μ	Rate at which one computer is removed from the network.

Equations of the Basic Model

$$\begin{aligned}
\frac{dS}{dt} &= (1 - p)N - \beta_1 SI - \beta_2 SE - Ps - \mu S, \\
\frac{dE}{dt} &= \beta_1 SI + \beta_2 SE - k E - \alpha E - \mu E, \\
\frac{dI}{dt} &= \alpha E - rI - \mu I, \qquad (1) \\
\frac{dR}{dt} &= Ps + kE + rI \\
\frac{dN}{dt} &= S(t) + E(t) + I(t) + R(t)
\end{aligned}$$

The Extended Model

We seek to extend the basic model proposed by adding another compartment following the recommendation of Mishra and Saini (2006) stating that "further work should be done to distinguish between susceptible and immune in the unaffected groups". This would be ensured in the assumptions considered below.

Assumptions of the Extended Model

The basic model will be extended by adding the following assumptions;

i. We assume that the newly manufactured computers are installed with an anti-virus alongside their manufacturing number from the factory and forming a compartment of susceptible computers with immunity.
ii. The anti-virus installed in the new computers has an expiry date and when it expires, it forms a compartment of susceptible computers without immunity.
iii. The susceptible computers also get the virus through contact with an infected external storage device θ (*Zhang, 2016*).
iv. Computers which have been recovered (R) enters into the susceptible class without immunity (S).

Variables and Parameters of the Extended Model

Table 2: Shows the variables and parameters of the extended model alongside their description

Parameters/Variable	Description
A	The class of susceptible computers which have immunity.
S	The class of susceptible computers without immunity.
E	The exposed class of computers which are infected but not yet broken out.
I	The infected class of computers which have broken out.
R	The recovered class of computers which the virus has been repaired.
d_1	Manufacturing number given to the new computer alongside an anti-virus.
d_2	Manufacturing number given to the new computer without an anti-virus.
γ	Rate at which a recovered computer becomes susceptible.
k	Recovery rate of an exposed computer.
w	Rate at which a susceptible computer with immunity can become exposed.
α	Rate at which an exposed computer is broken out.
r	Recovery rate of an infectious computer
θ	Rate at which an infected storage media can infect a susceptible computer.
β_1	Contact rate between the susceptible computer and infected computer.
β_2	Contact rate between the susceptible computer and exposed computer.
a	Rate at which a susceptible computer without immunity becomes immune due to the presence of an anti-virus.
H	Rate at which an immune computer loses immunity due to the absence of an anti-virus.
μ	Rate at which a computer is damaged or destroyed.

Equations of the Extended Model

$$\left.\begin{aligned}\frac{dA}{dt} &= d_1 + aS - w\lambda A - \rho_1 A\\ \frac{dS}{dt} &= d_2 + \eta A + \gamma R - (\rho_2 + \lambda)S\\ \frac{dE}{dt} &= \lambda(S + wA) - \rho_3 E\\ \frac{dI}{dt} &= \alpha E - \rho_4 I\\ \frac{dR}{dt} &= kE + rI - \rho_5 R\end{aligned}\right\} \quad (2)$$

Where;

$\rho_1 = \eta + \mu$

$\rho_2 = a + \mu$

$\rho_3 = k + \alpha + \mu$

$\rho_4 = r + \mu$

$\rho_5 = \gamma + \mu$

And

$$\lambda = \beta_1 E + \beta_2 I + \theta \quad (3)$$

With

$$N(t) = A(t) + S(t) + E(t) + I(t) + R(t) \quad (4)$$

Model Analysis

In this section, we consider the quantitative behavior of the extended model. This would involve linearization of the model system to determine the local stability of the Computer Virus Free Equilibrium (CVFE), in terms of the computer reproduction number.

Existence and Stability of Equilibrium Points

Existence

By setting the derivatives of the system (2) to zero,

Let;

$$\left.\begin{aligned} d_1 + aS - w\lambda A - \rho_1 A &= 0\\ d_2 + \eta A + \gamma R - (\rho_2 + \lambda)S &= 0\\ \lambda(S + wA) - \rho_3 E &= 0\\ \alpha E - \rho_4 I &= 0\\ kE + rI - \rho_5 R &= 0\end{aligned}\right\} \quad (5)$$

Where;

$$A^* = \frac{d_1 + aS^*}{\rho_1 + w\lambda^*} \quad (6)$$

$$S^* = \frac{d_2 + \eta A^* + \gamma R^*}{\rho_2 + \lambda^*} \quad (7)$$

$$E^* = \frac{\lambda^*(S^* + wA^*)}{\rho_3} \quad (8)$$

$$I^* = \frac{\alpha E^*}{\rho_4} \quad (9)$$

$$R^* = \left(\frac{k}{\rho_5} + \frac{r\alpha}{\rho_4\rho_5}\right)E^* = Q_0 E^* \quad (10)$$

Where;

$$Q^0 = \frac{k}{\rho^5} + \frac{r\alpha}{\rho^4\rho^5} \quad (11)$$

Substituting (10) in (7) gives

$$S^* = \frac{d_2 + \eta A^* + \gamma Q^0 E^*}{\rho_2 + \lambda^*} \quad (12)$$

Consequently, substituting (12) in (6) gives;

$$A^* = \frac{(ad_2 + d_1\rho_2 + \lambda^* d_1 + a\gamma Q_0 E^*)}{(\rho_1\rho_2 - \eta a + (\rho_1 + w\rho_2)\lambda^* + \lambda^{*2} w)} \quad (13)$$

Using expressions (12) and (13) gives

$$E^* = \frac{\lambda^*(\lambda^*\epsilon_1 + \epsilon_0)}{h_2\lambda^{*2} + h_1\lambda^* + h_0} \quad (14)$$

Where;

$$\epsilon_0 = w(d^2 a + d^1\rho^2) + \eta d^1 + d2\rho^1$$

$$\epsilon_1 = w(d^1 + d^2)$$

$$h_0 = \rho^1\rho^2\rho^3 - \eta a\rho^3$$

$$h_1 = w(\rho^2\rho^3 - \alpha\gamma Q^0) + \rho^1(\rho^3 - \gamma Q^0)$$

$$h_2 = w(\rho^3 - \gamma Q^0)$$

Recall that: $\lambda^* = \beta_1 E^* + \beta_2 I^* + \theta$, from (3) so, $if\ \theta = 0, then$

$$\lambda^* = \beta^{1E^*} + \beta^{2I^*} = M_\alpha E^* \quad (15)$$

Where;

$$M_\alpha = \beta_1 + \frac{\beta_2\alpha}{\rho_4} \quad (16)$$

From which we obtain

$$\lambda\left(1 - M_\alpha\frac{\lambda\epsilon_1 + \epsilon_0}{h_2\lambda^2 + h_2\lambda + h_0}\right) = 0 \quad (17)$$

$$either\ \lambda = 0 \quad (18)$$

Or

$$1 - M_\alpha\frac{\lambda\epsilon_1 + \epsilon_0}{h_2\lambda^2 + h_2\lambda + h_0} = 0 \quad (19)$$

Substituting $\lambda = 0$ for A, S, E, I, R yields E_0=I_0 =R_0=0. Thus, the Computer Virus Free Equilibrium (CVFE) given by

$$C_0 = (A_0, S_0, E_0, I_0, R_0) = \left(A_0, \frac{d_2 + \eta A_0}{\rho_2}, 0, 0, 0\right) \quad (20)$$

Where

$$A_0 = \frac{d_1\rho_2 + ad_2}{\rho_1\rho_2 - \eta a}$$

Computation of Computer Virus Reproduction Number, $\mathcal{R}_c$

From epidemiology, the basic reproduction number is the expected number of secondary infections caused by a typical infected individual during his/ her entire period of infectiousness (Diekmann et. al, 1990; Heffernan et. al, 2005). The threshold quantity determines where a disease invades or is eradicated when $\mathcal{R}_0 > 1$ or $\mathcal{R}_0 < 1$ respectively. It is computed using the next generation matrix proposed by van den Driessche and Watmough (2002). In a similar manner, computer virus reproduction number refers to the expected number of secondary infections generated by a typical infected computer in a population where every computer is susceptible. Thus, the same approach used in epidemiology of disease to find the basic reproduction number of a disease shall be adopted in finding the computer virus reproduction number.

From (3.2)

$$\frac{dA}{dt} = d_1 + aS - w\lambda A - \rho_1 A$$
$$\frac{dS}{dt} = d_2 + \eta A + \gamma R - (\rho_2 + \lambda)S$$
$$\frac{dE}{dt} = \lambda(S + wA) - \rho_3 E$$
$$\frac{dI}{dt} = \alpha E - \rho_4 I$$
$$\frac{dR}{dt} = kE + rI - \rho_5 R$$

We see that E' and I' are the compartments which have been infected with the virus.

Thus:

$$\mathcal{F}_i = \begin{pmatrix} \lambda(S + wA) \\ \\ 0 \end{pmatrix} \quad (21)$$

$$V_i = \begin{pmatrix} \rho_3 E \\ \\ -\alpha E + \rho_4 I \end{pmatrix} \quad (22)$$

From which we obtain:

$$F = \begin{pmatrix} \beta_1(S_0 + wA_0) & \beta_2(S_0 + wA_0) \\ \\ 0 & 0 \end{pmatrix} \quad (23)$$

And

$$V = \begin{pmatrix} \rho_3 & 0 \\ \\ -\alpha & \rho_4 \end{pmatrix} \quad (24)$$

With

$$V^{-1} = \begin{pmatrix} \frac{1}{\rho_3} & 0 \\ \\ \frac{\alpha}{\rho_3\rho_4} & \frac{1}{\rho_4} \end{pmatrix} \quad (25)$$

Computing FV^{-1} mathematically, this is defined as the next generation matrix. (Diekmann et. al., 2000)

$$FV^{-1} = \begin{pmatrix} \frac{A_1}{\rho_3} + \frac{A_2\alpha}{\rho_3\rho_4 - \lambda E} & \frac{A_2}{\rho_4} \\ \\ 0 & -\lambda_E \end{pmatrix} \quad (26)$$

$$|FV^{-1} - \lambda_E| = 0 \quad (27)$$

This result to

$$\lambda_E{}^2 - \left(\frac{A_1}{\rho_3} + \frac{A_2\alpha}{\rho_3\tilde{n}_4}\right)\lambda_E = 0 \quad (28)$$

$$\lambda_E = 0 \ or \ \lambda_E = \frac{A^1}{\rho^3} + \frac{A^2\alpha}{\rho^3\rho^4} = R_c \quad (29)$$

Therefore, the Computer Virus Reproduction number for model is given as:

$$R_c = R_{c_1} + R_{c_2} \quad (30)$$

Where

$$R_{c_1} = \frac{A_1}{\rho_3} \text{and} \ \ R_{c_2} = \frac{A^2\alpha}{\rho_3\rho^4}$$

represents the susceptible classes with immunity and the susceptible classes without immunity respectively. Recall from (3.20) that;

$$A_0 = \frac{d_1\rho_2 + ad_2}{\rho_1\rho_2 - \eta a} \ and \ S_0 = \frac{d_2 + \eta A_0}{\rho_2}$$

This implies that

$$A_1 = \beta_1\left[\frac{d_2}{\rho_2} + (w + \frac{\eta}{\rho_2})(\frac{d_1\rho_2 + d_2 a}{\rho_1\rho_2 + \eta a})\right] \quad (31)$$

And

$$A_2 = \beta_2\left[\frac{d_2}{\rho_2} + (w + \frac{\eta}{\rho_2})(\frac{d_1\rho_2 + d_2 a}{\rho_1\rho_2 + \eta a})\right] \quad (32)$$

Thus,

$$R_{c_1} = \frac{\beta_1\left[\frac{d_2}{\rho_2} + \left(w + \frac{\eta}{\rho_2}\right)\left(\frac{d_1\rho_2 + d_2 a}{\rho_1\rho_2 + \eta a}\right)\right]}{\rho_3} \quad (33)$$

$$R_{c_2} = \frac{\beta_2\left[\frac{d_2}{\rho_2} + \left(w + \frac{\eta}{\rho_2}\right)\left(\frac{d_1\rho_2 + d_2 a}{\rho_1\rho_2 + \eta a}\right)\right]\alpha}{\rho_3\rho_4} \quad (34)$$

$$R_c = \frac{\beta_1\left[\frac{d_2}{\rho_2} + \left(w + \frac{\eta}{\rho_2}\right)\left(\frac{d_1\rho_2 + d_2 a}{\rho_1\rho_2 + \eta a}\right)\right]}{\rho_3} + \frac{\beta_2\left[\frac{d_2}{\rho_2} + \left(w + \frac{\eta}{\rho_2}\right)\left(\frac{d_1\rho_2 + d_2 a}{\rho_1\rho_2 + \eta a}\right)\right]\alpha}{\rho_3\rho_4} \quad (35)$$

Analysis of Computer Virus Reproduction Number

We analyze the computer virus reproduction number R_c in order to show the significance of the preventive measure of the computer virus which includes: d_1, a, η, was well as the control measures (k, r), on the virus spread.

From (30);

$$R_c = \frac{\beta_1\left[\frac{d_2}{\rho_2} + \left(w + \frac{\eta}{\rho_2}\right)\left(\frac{d_1\rho_2 + d_2 a}{\rho_1\rho_2 + \eta a}\right)\right]}{\rho_3} + \frac{\beta_2\left[\frac{d_2}{\rho_2} + \left(w + \frac{\eta}{\rho_2}\right)\left(\frac{d_1\rho_2 + d_2 a}{\rho_1\rho_2 + \eta a}\right)\right]\alpha}{\rho_3\rho_4}$$

But

$$\rho_1 = \eta + \mu$$
$$\rho_2 = a + \mu$$
$$\rho_3 = k + \alpha + \mu$$
$$\rho_4 = r + \mu$$
$$\rho_5 = \gamma + \mu$$

This implies that;

$$R_c = \frac{\beta_1\left[\frac{d_2}{(a+\mu)} + \left(w + \frac{\eta}{(a+\mu)}\right)\left(\frac{d_1(a+\mu)+d_2 a}{(\eta+\mu)(a+\mu)+\eta a}\right)\right]}{k+\alpha+\mu} + \frac{\beta_2\left[\frac{d_2}{(a+\mu)} + \left(w + \frac{\eta}{(a+\mu)}\right)\left(\frac{d_1(a+\mu)+d_2 a}{(\eta+\mu)(a+\mu)+\eta a}\right)\right]\alpha}{(k+\alpha+\mu)\,(r+\mu)} \tag{36}$$

In the absence of any control measure;

$$\lim_{d_1,a,\eta,w,k,r\to 0} R_c = R_{c_0} = \frac{\beta_1\left[\frac{d_2}{\mu}\right]}{(\alpha+\mu)} + \frac{\beta_2\left[\frac{d_2}{\mu}\right]\alpha}{(\alpha+\mu)(\mu)} \tag{37}$$

Taking an anti-virus as the only virus control measure;

$$\lim_{k,r\to 0} R_c = R_{c_1} = \frac{\beta_1\left[\frac{d_2}{(a+\mu)} + \left(w+\frac{\eta}{(a+\mu)}\right)\left(\frac{d_1(a+\mu)+d_2 a}{(\eta+\mu)(a+\mu)+\eta a}\right)\right]}{\alpha+\mu} + \frac{\beta_2\left[\frac{d_2}{(a+\mu)} + \left(w+\frac{\eta}{(a+\mu)}\right)\left(\frac{d_1(a+\mu)+d_2 a}{(\eta+\mu)(a+\mu)+\eta a}\right)\right]\alpha}{(\alpha+\mu)\,\mu)} \tag{38}$$

In the case of both antivirus and repair options, we refer to R_c in equation (36)

In the absence of antivirus as the control measure;

$$\lim_{d_1,a,\eta,w,\to 0} R_c = R_{c_2} = \frac{\beta_1\left[\frac{d_2}{\mu}\right]}{(k+\alpha+\mu)} + \frac{\beta_2\left[\frac{d_2}{\mu}\right]\alpha}{(\alpha+\mathrm{k}+\mu)(\mathrm{r}+\mu)} \tag{39}$$

$$\Delta_a = R_{c_0} - R_{c_1} = \frac{1}{(\alpha+\mu)\mu}\left[\{d_2 - \left[\left(\frac{d_2}{(a+\mu)} + w + \frac{\eta}{(a+\mu)}\right)\left(\frac{d_1(a+\mu)+d_2 a}{(\eta+\mu)(a+\mu)+\eta a}\right)\right]\mu\}\beta_1 + \left\{\frac{d_2\alpha}{\mu} - \left(\frac{d_2}{(a+\mu)} + (w + \frac{\eta}{(a+\mu)}\right)\left(\frac{d_1(a+\mu)+d_2 a}{(\eta+\mu)(a+\mu)+\eta a}\right)\alpha\right\}\beta_2] > 0 \tag{40}$$

$$\Delta_R = R_{c_0} - R_{c_2} = \frac{d_2}{\mu}\left[\beta_1\left(\frac{1}{\alpha+\mu} - \frac{1}{k+\alpha+\mu}\right) + \beta_2\alpha\left(\frac{1}{(\alpha+\mu)\mu} - \frac{1}{(\alpha+k+\mu)(r+\mu)}\right)\right] > 0 \tag{41}$$

$$\Delta_{aR} = R_{c_0} - R_{\mathrm{c}} = \frac{\beta_1\frac{d_2}{\mu}}{\alpha+\mu} - \left[\frac{\beta_1\left(\frac{d_2}{(a+\mu)} + \left(w+\frac{\eta}{(a+\mu)}\right)\left(\frac{d_1(a+\mu)+d_2 a}{(\eta+\mu)(a+\mu)+\eta a}\right)\right)}{k+\alpha+\mu}\right] + \frac{\beta_2\left(\frac{d_2}{\mu}\right)}{(\alpha+\mu)\mu} - \left[\frac{\beta_2\left(\frac{\left(\frac{d_2}{\mu}\right)}{(a+\mu)} + \left(w+\frac{\eta}{(a+\mu)}\right)\left(\frac{d_1(a+\mu)+d_2 a}{(\eta+\mu)(a+\mu)+\eta a}\right)\right)\alpha}{k+\alpha+\mu}\right] > 0 \tag{42}$$

From the analysis shown above, the control and preventive measures are essential to a lasting use of our computers. Thus, the next thing to check out for after purchasing a computer system is the installation of an anti-virus.

Stability of the Computer Virus Free Equilibrium

Local Stability of the Computer Virus free equilibrium

We discuss the local stability of the computer virus free equilibrium of the model by adopting the same procedure used in disease epidemiology. This is achieved by proving the lemma below using linearized stability theory.

Lemma 1

The computer virus - free equilibrium point of the model in equation (5) is locally asymptotically stable if $\mathcal{R}_{\mathrm{c}} < 1$and unstable if $\mathcal{R}_{\mathrm{c}} > 1$.

Proof

Considering the following equations:

$$\begin{aligned} f_1 &= d_1 + aS - w(\beta_1 E + \beta_2 E + \theta)A - \rho_1 A \\ f_2 &= d_2 + \eta A + \gamma R - (\beta_1 E + \beta_2 I + \theta)S - \rho_2 S \\ f_3 &= (\beta_1 E + \beta_2 I + \theta) + (S + wA) - \rho_3 E \\ f_4 &= \alpha E - \rho_4 I \\ f_5 &= kE + rI - \rho_5 R \end{aligned} \tag{43}$$

Then the Jacobian matrix is;

$$\mathrm{J}_\alpha = \begin{pmatrix} -(\lambda+\rho_1) & a & -\beta_1 wA & -\beta_2 wA & 0 \\ \eta & -(\lambda+\rho_2) & -\beta_1 S & -\beta_2 S & \gamma \\ \lambda w & \lambda & \beta_1(S+wA) - \rho_3 & \beta_2(S+wA) & 0 \\ 0 & 0 & \alpha & -\rho_4 & 0 \\ 0 & 0 & k & r & -\rho_5 \end{pmatrix} \tag{44}$$

The corresponding Jacobian matrix at the computer virus free equilibrium C^0 is given by;

$$\mathrm{J}_0 = \begin{pmatrix} -\rho_1 & a & -\beta_1 wA^0 & -\beta_2 wA^0 & 0 \\ \eta & -\rho_2 & -\beta_1 S^0 & -\beta_2 S^0 & \gamma \\ 0 & 0 & \beta_1(S^0+wA^0) - \rho_3 & \beta_2(S^0+wA^0) & 0 \\ 0 & 0 & \alpha & -\rho_4 & 0 \\ 0 & 0 & k & r & -\rho_5 \end{pmatrix} \tag{45}$$

The characteristics equation of (45) is;

$|J_0 - xI| = 0$ Or

$$\begin{vmatrix} -\rho_1 - x & a & -\beta_1 wA^0 & -\beta_2 wA^0 & 0 \\ \eta & -\rho_2 - x & -\beta_1 S^0 & -\beta_2 S^0 & \gamma \\ 0 & 0 & \beta_1(S^0+wA^0) - \rho_3 - x & \beta_2(S^0+wA^0) & 0 \\ 0 & 0 & \alpha & -\tilde{\mathrm{n}}_4 - x & 0 \\ 0 & 0 & k & r & -\rho_5 - x \end{vmatrix} = 0$$

$$= -(\rho_1 + x)\begin{vmatrix} -\rho_2 - x & -\beta_1 S^0 & -\beta_2 S^0 & \gamma \\ 0 & \beta_1(S^0+wA^0) - \rho_3 - x & \beta_2(S^0+wA^0) & 0 \\ 0 & \alpha & -\rho_4 - x & 0 \\ 0 & k & r & -\rho_5 - x \end{vmatrix}$$

$$-\eta\begin{vmatrix} a & -\beta_1 wA^0 & -\beta_2 wA^0 & 0 \\ 0 & \beta_1(S^0+wA^0)-\rho_3-x & \beta_2(S^0+wA^0) & 0 \\ 0 & \alpha & -\rho_4-x & 0 \\ 0 & k & r & -\rho_5-x \end{vmatrix}$$

$$= (\rho_1+x)(\rho_2+x)\left[-(\rho_5+x)\begin{bmatrix}\beta_1(S^0+wA^0)-\rho_3-x & \beta_2(S^0+wA^0)\\ \alpha & -(\rho_4+x)\end{bmatrix}\right]$$

$$-\eta a(-\rho_5-x)\begin{bmatrix}\beta_1(S^0+wA^0)-\rho_3-x & \beta_2(S^0+wA^0)\\ \alpha & -(\rho_4+x)\end{bmatrix}$$

$$= (-\rho_5-x)\{(-\rho_4-x[\beta_1(S^0+wA^0)-\rho_3-x]-\beta_2\alpha(S^0+wA^0)\}\{(\rho_1+x)(\rho_2+x)-\eta a\}= 0$$

$x = \rho_5 < 0$ or $(x^2+(\rho_1+\rho_2)x+\tau)(x^2+kx+\rho_3\rho_4(1-R_c))$ (46)

Where $\tau = \rho_1\rho_2 - \eta a$

From equation (3.46) above, we now obtain

$p_4x^4+p_3x^3+p_2x^2+p_1x+p_0$ (47)

Where

$p_4 = 1$

$p_3 = \rho_1+\rho_2+k$

$p_2 = k(\rho_1+\rho_2)+\tau+\rho_3\rho_4(1-R_c)$

$p_1 = (\rho_1+\rho_2)\rho_3\rho_4(1-R_c)$

$p_0 = \tau\rho_3\tilde{n}_4(1-R_c)$

From which we see that $p_0 > 0$ whenever $R_c < 1$ and $p_0 < 0$ whenever$R_c > 1$, hence the Computer Virus Free Equilibrium is locally asymptotically stable whenever $R_c < 1$ and unstable whenever$R_c > 1$.

Globally Asymptotic Stability (GAS) of the Computer Virus Free Equilibrium State

We discuss the global stability of the CVFE by considering a lemma gotten from the epidemiology of disease. We would consider the computer virus as a disease and proof the lemma in that format.

Lemma 2

The computer virus free equilibrium of the model in (3.5) is globally asymptotically stable (GAS) if $\mathcal{R}_c < 1$ *and unstable if* $\mathcal{R}_c > 1$.

Proof

We establish the proof using a comparison approach from disease epidemiology as proposed by Diekmann et al., 1990. The equations of the infected compartments from equation (2) are given as;

$\frac{dX}{dt} = (F-V)X, \qquad X = (E,I)$

Recall from (23) and (24) that

$$F = \begin{pmatrix}\beta_1(S_0+wA_0) & \beta_2(S_0+wA_0)\\ 0 & 0\end{pmatrix} \text{ and } V = \begin{pmatrix}\rho_3 & 0\\ -\alpha & \rho_4\end{pmatrix}$$

By Comparison method, we have the equations;

$\frac{dX}{dt} = (F-V)X \text{ where } X = (E,I)$

$$(F-V) = \begin{pmatrix}\beta_1(S_0+wA_0)-\rho_3 & \beta_2(S_0+wA_0)\\ \alpha & -\rho_4\end{pmatrix} \quad (48)$$

From which we obtain;

$$\begin{bmatrix}\frac{dE}{dt}\\ \frac{dI}{dt}\end{bmatrix} = \begin{bmatrix}\beta_1(S_0+wA_0)-\rho_3 & \beta_2(S_0+wA_0)\\ \alpha & -\rho_4\end{bmatrix}\begin{bmatrix}E\\ I\end{bmatrix}$$

$\Longrightarrow \frac{dE}{dt} = (\beta_1(S_0+wA_0)-\rho_3)E+\beta_2(S_0+wA_0)I$ (49)

$\frac{dI}{dt} = \alpha E-\rho_4 I$ (50)

From (49) we get

$\frac{dE}{dt}-(\beta_1(S_0+wA_0)-\rho_3)E = \beta_2(S_0+wA_0)I$

$\Longrightarrow E(t) = \frac{1}{e^{-\beta_1(S_0+wA_0)t}}\left[\frac{e^{-\beta_1(S_0+wA_0)t}}{-\beta_1(S_0+wA_0)}\int\beta_2(S_0+wA_0)I\right]$ (51)

At $t = \infty$, $E_0 = 0$ (52)

Similarly, from (50) we see that

$\frac{dI}{dt}+\rho_4 I = \alpha E$

$\Longrightarrow I(t) = \frac{1}{e^{\rho_4 t}}\left[\int e^{\rho_4 t}.\alpha E dt\right]$ (53)

At $t = \infty$, $I_0 = 0$ (54)

Therefore, $(E,I) = (0,0)$

The system will not be globally stable until all the eigenvalues of the matrix $(F-V)$ have negative real parts, van den Driesche and Watmough (2002). To ensure that this is true we would show that the trace of the matrix is negative and the result of the determinant is positive.

Thus, the trace of the matrix in (48) is;

$$-(\rho_3+\rho_4-\beta_1(S_0+wA_0)) \quad (55)$$

And the determinant is given by

$$\rho_3\rho_4\left(1-\frac{\rho_4\beta_1(S_0+wA_0)}{\rho_3\rho_4}-\frac{\beta_2(S_0+wA_0)\alpha}{\rho_3\rho_4}\right)=0 \quad (56)$$

$$\Rightarrow \rho_3\rho_4(1-R_c)=0 \quad (57)$$

At $R_c<1$,

$$\rho_3\rho_4(1-R_c)>0 \quad (58)$$

Hence the trace of matrix $(F-V)$ is negative and the determinant is positive such that trace<0 and determinant>0, we can conclude that all the eigenvalues have negative real parts. Thus, the system is stable whenever $R_c<1$ and $(E,I)\to(0,0)$ as $t\to\infty$. This proves that the Computer Virus Fee Equilibrium (CVFE) is globally asymptotically stable if$R_c<1$, the virus dies out.

Numerical Simulation

Numerical Methods are employed to solve Equation (2) under different real parametric values as shown in Table (3) below. The graphs are plotted using ©MATLAB 7.5.0 (R2007b). Analysis of the computer virus reproduction number is attempted. Some of the parametric values are gotten from the basic model while others are assumed.

Table 3: Parametric values of the extended model

Parameters	Description	Value	Source
d_1	Manufacturing number given to a new computer alongside an anti-virus	250	Assumed
d_2	Manufacturing number given to a new computer but without an anti-virus	250	Assumed
β_1	Contact rate between the susceptible computer and exposed computer	0.7	Peng 2013
β_2	Contact rate between a susceptible computer and an infected computer	0.8	Peng 2013
α	Rate at which an exposed computer is broken out.	0.6	Peng 2013
k	Recovery rate of an exposed computer	0.4	Peng 2013
r	Recovery rate of an infectious computer	0.6	Peng 2013
μ	Rate at which a computer is damaged or destroyed	0.02	Peng 2013
w	Rate at which a susceptible computer with immunity can become exposed.	0.4	Assumed
a	Rate at which a susceptible computer without immunity becomes immune due to the presence of an anti-virus	0.2	Assumed
θ	Rate at which an infected storage media can infect a susceptible computer	0.0	Assumed
η	Rate at which an immune computer loses its immunity due to the absence of an anti-virus	0.3	Assumed
γ	Rate at which a recovered computer becomes susceptible.	0.2	Assumed

RESULTS AND DISCUSSION

In this chapter, we present and discuss the results of the numerical simulation, conclusion and recommendations for further work.

Numerical Results

The graphs of the results obtained are presented below;

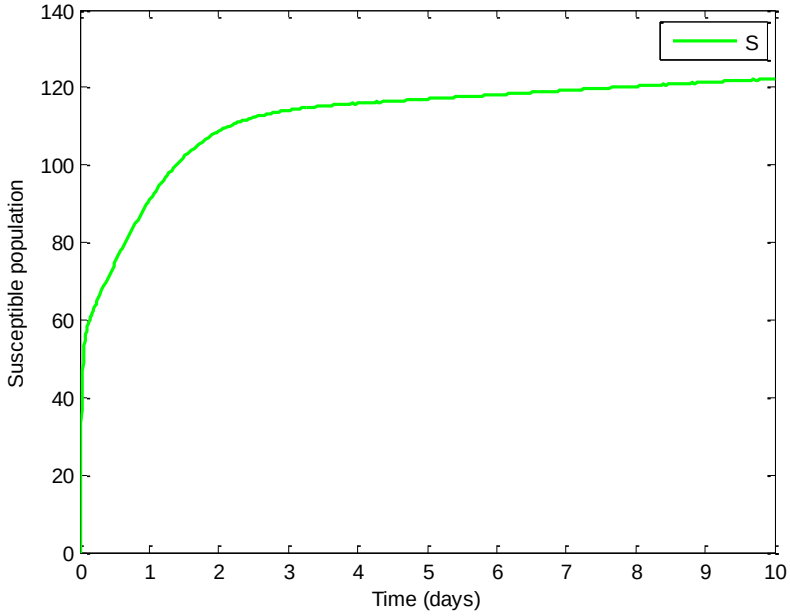

Figure 1: Graph showing the effect of anti-virus (a=0) on susceptible class S

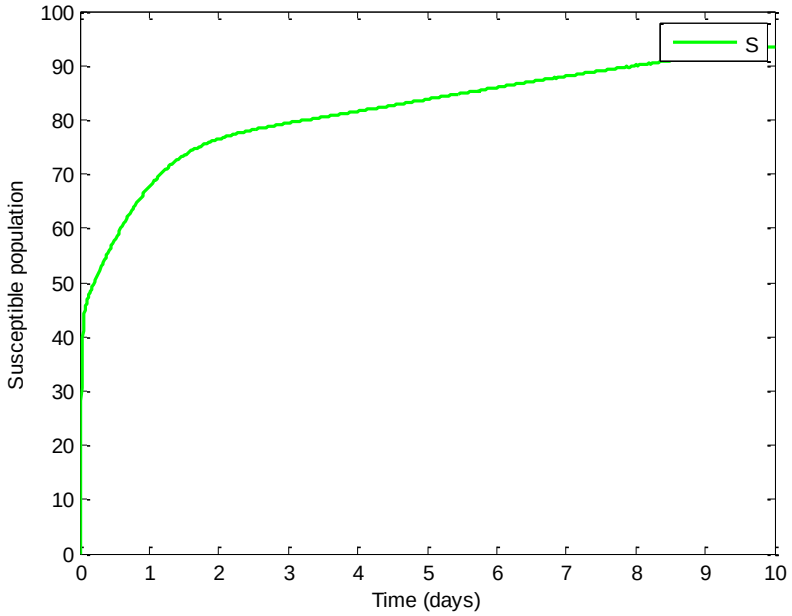

Figure 2: Graph showing the effect of anti-virus (a≠0) on susceptible class S

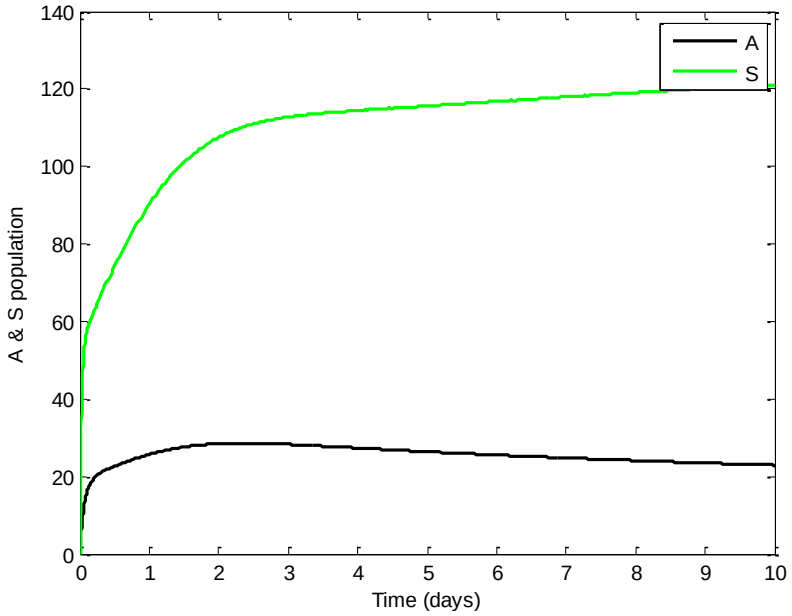

Figure 3: Graph showing the effect of infective storage media θ on the susceptible classes A and S ($\theta = 0$)

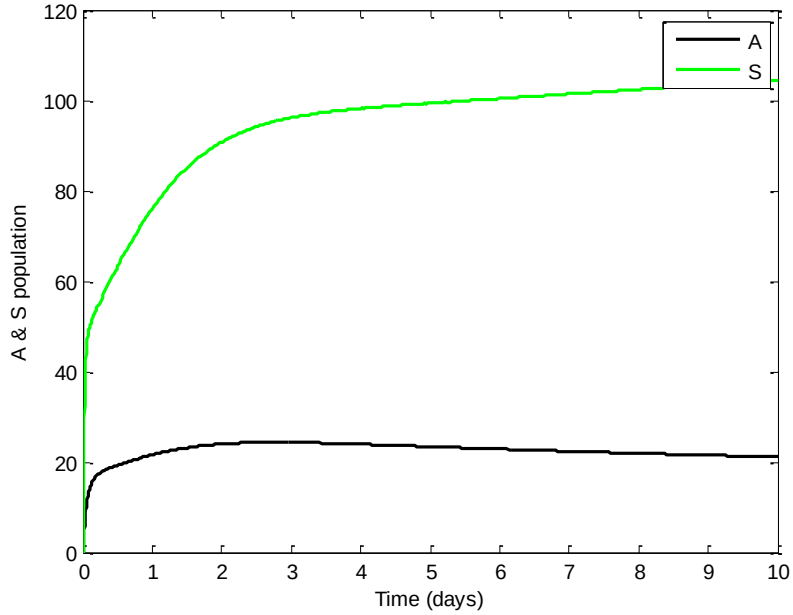

Figure 4: Graph showing the effect of infective storage media on the susceptible classes A and S ($\theta \neq 0$)

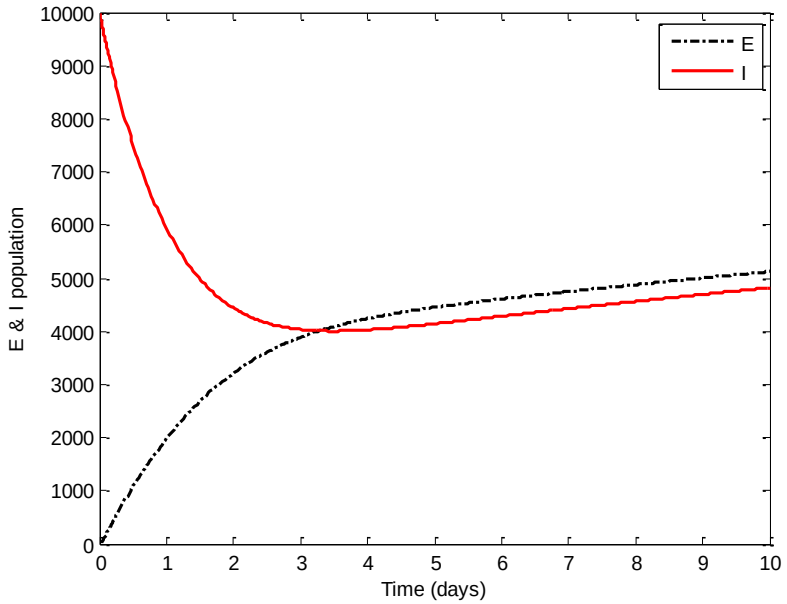

Figure 5: Graph showing the effect of infective storage media on the infected class I and exposed class E ($\theta = 0$)

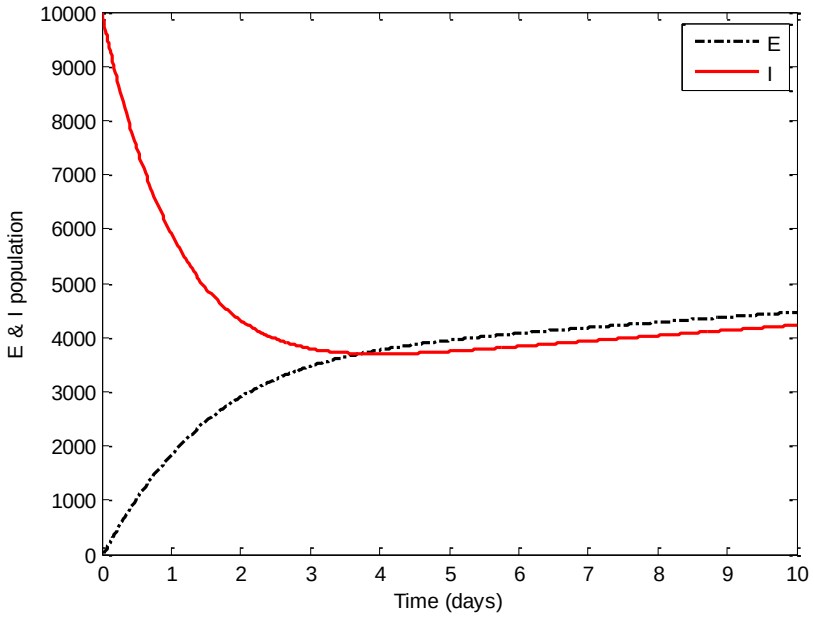

Figure 6: Graph showing the effect of infective storage media on the infected class I and exposed class E ($\theta \neq 0$)

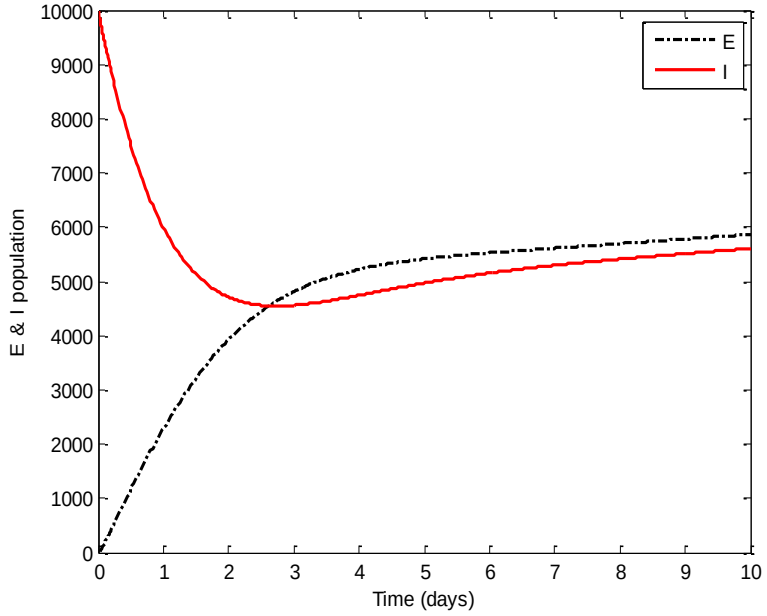

Figure 7: Graph showing the effect of k on the infected class I and exposed class E ($k = 0$)

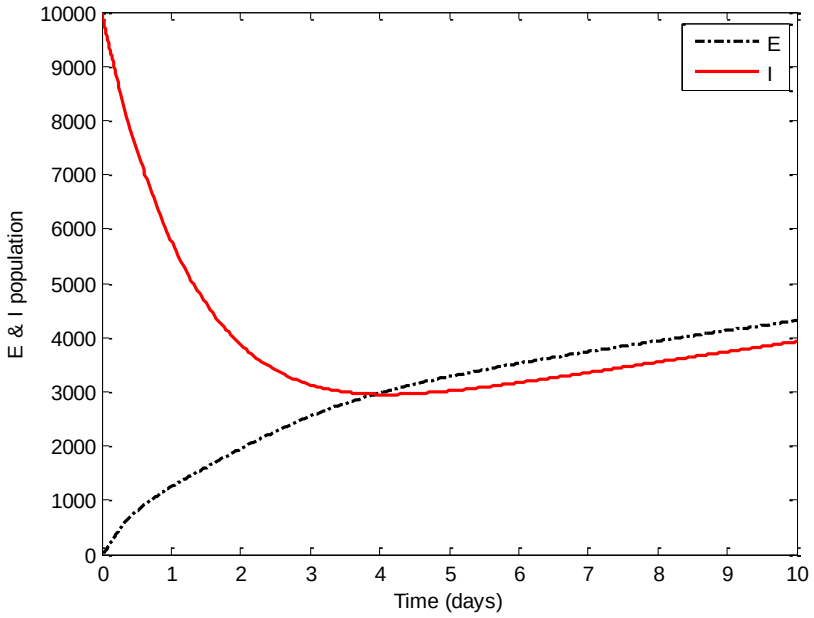

Figure 8: Graph showing the effect of k on the infected class I and exposed class E ($K \neq 0$)

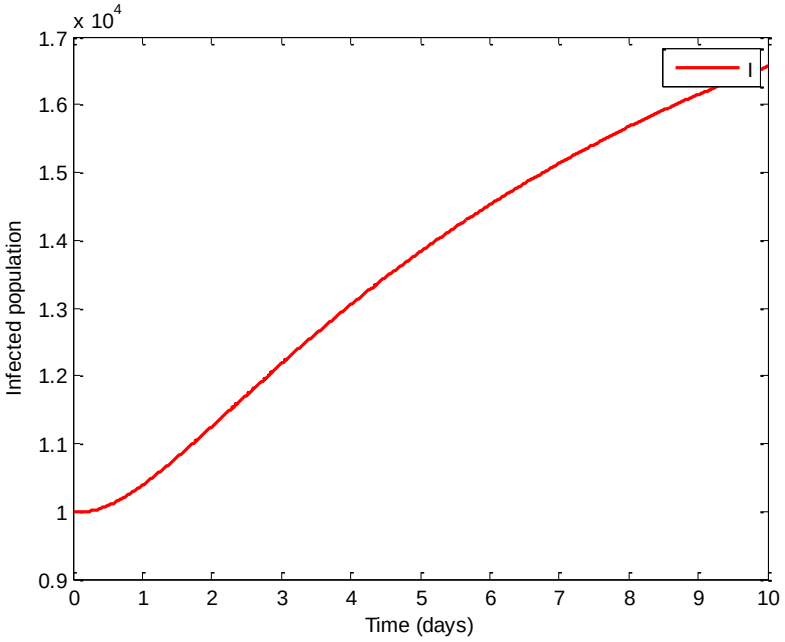

Figure 9: Graph showing the effect of r on the infected class I ($r = 0$)

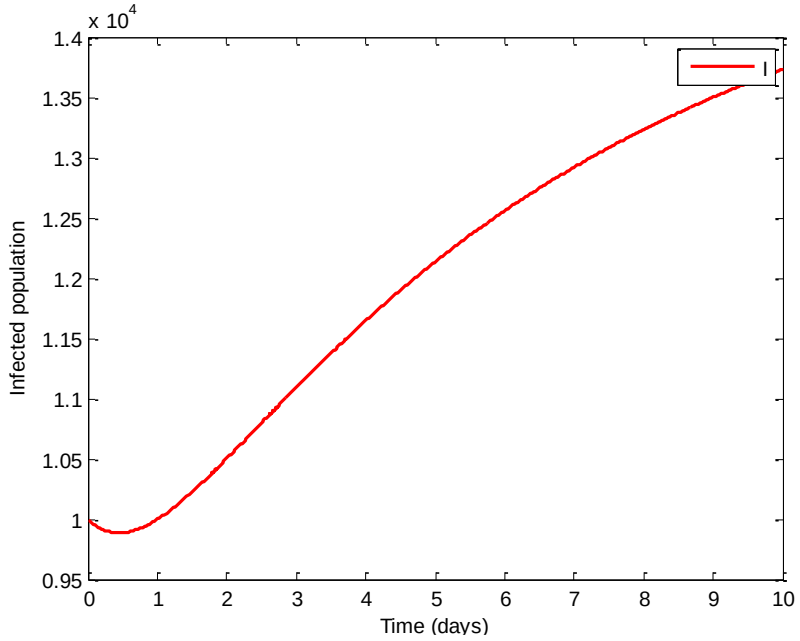

Figure 10: Graph showing the effect of r on the infected class I ($r \neq 0$)

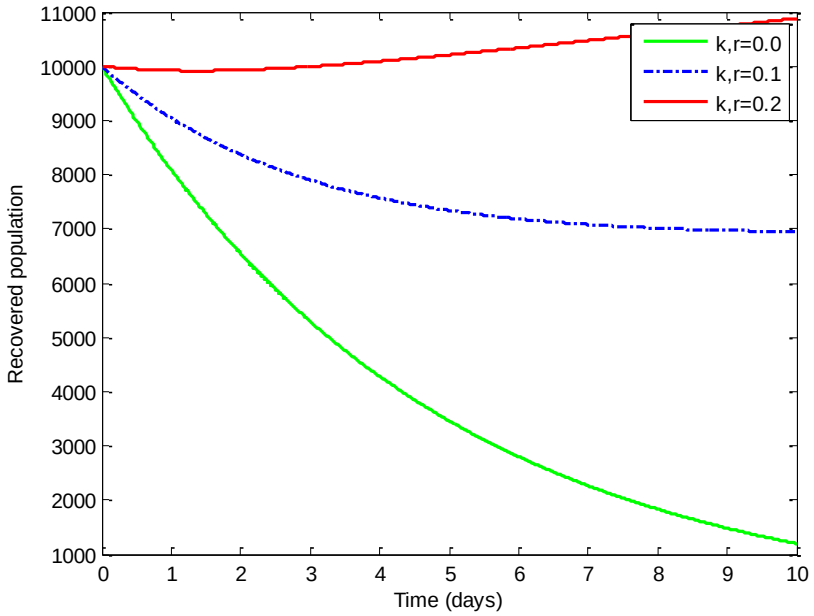

Figure 11: Graph showing the effect of recovery rate of infected and exposed computers k, r on the recovered class R ($k, r = 0, \neq 0$)

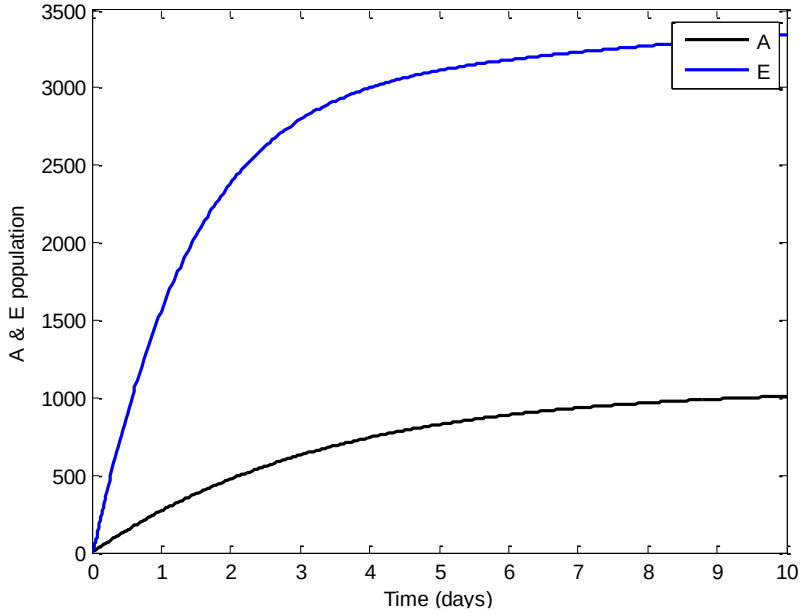

Figure 12: Graph showing the effect of w on the susceptible class A and exposed class E (w = 0)

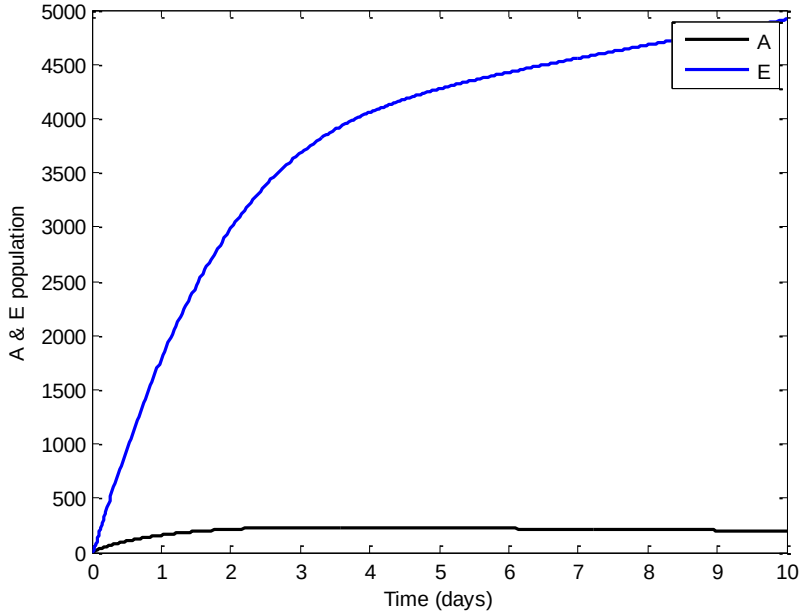

Figure 13: Graph showing the effect of w on the susceptible class A and exposed class E (w ≠ 0)

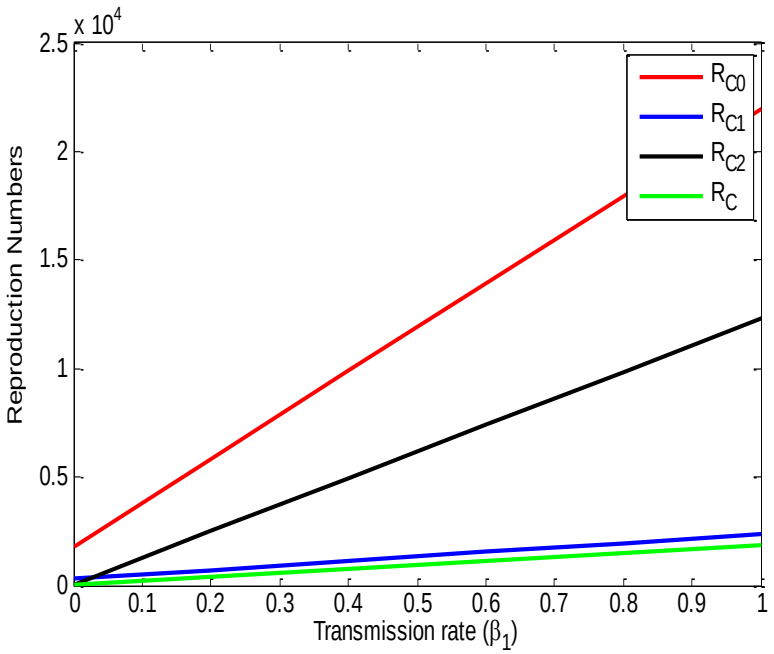

Figure 14: Graph showing the Analysis of Reproduction number vs. Transmission Rate (β_1)

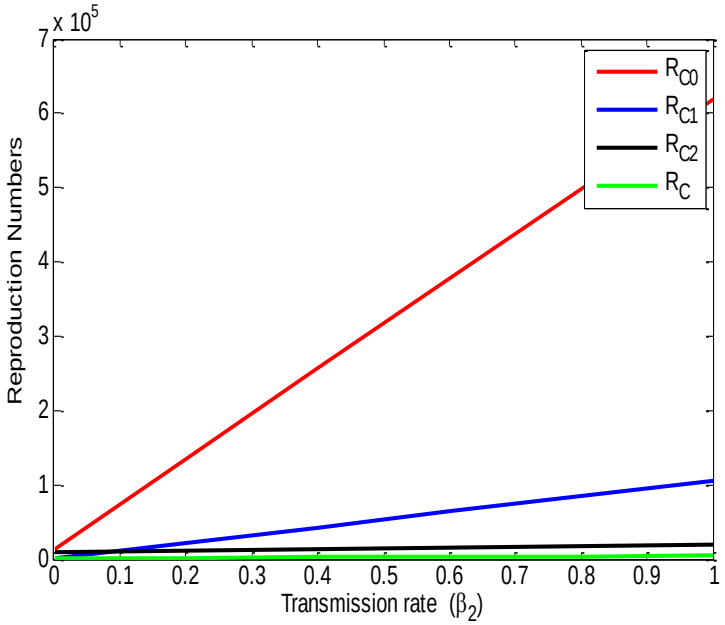

Figure 15: Graph showing the Analysis of Reproduction number vs. Transmission Rate (β_2)

Description of Figures

From Figure 1 to Figure 2, we see the effect of adding an anti-virus (a) to a susceptible class without immunity; therefore providing immunity to the class reduces the susceptibility of the class to the virus.

From Figure 3 and Figure 4 we observed that the susceptibility of the susceptible class without immunity is always higher than that of the immune class with or without an infective storage media ($\theta = 0, \theta \neq 0$).

The result from Figure 5 and Figure 6 shows that the number of exposed computers to the virus is always higher than the number of infected computers with or without an infective storage media ($\theta = 0, \theta \neq 0$).

From Figure 7 and Figure 8 we observed that when there is no repair for the exposed computers, the infection rate is high ($k = 0$), but when exposed computers are being repaired, there is reduction in the number of exposed and infected computers ($k \neq 0$).

From Figures 9 and 10 we see that when the infected computers are being repaired ($r \neq 0$), the infectiousness of the infected class of computers reduces but when there is no repair ($r = 0$), the infectiousness of the infected class is very high.

From Figure 11 we observe that as the repair or recovery rate of the infected and exposed computers are increasing, the population of the recovered class of computers also increases, ($k, r = 0, 0.1, 0.2$).

From Figures 12 and 13, we observed that at $w = 0$, the population of the exposed computers is low, but when w $\neq 0$, more computers move from the susceptible class with immunity into the exposed class therefore, increasing the population of the exposed computers and reducing drastically the population of the immune class.
From Figure 14 and Figure 15 we observe that the absence of any control measure (R_{c_0}) is always higher compared to when we use anti- virus as the only control measure (R_{c_1}) which is also higher compared to using repair as the only control measure (R_{c_2}) which is also greater than using both repair and anti-virus as control measure which gives us R_c, ($R_{c_0} > R_{c_1} > R_{c_2} > R_c$). Therefore, a reduction in R_c translates in decrease in the prevalence of the computer virus.

CONCLUSION

This work formulated a mathematical model of a dynamical system of computer virus with an infected external storage media on viral spread, by extending a four-compartment model proposed by Peng et al, (2013) to five compartments. To better understand the effect of the infected external storage media on viral spread, an exhaustive model analysis showed that; (i) an infected external storage device speeds up the viral spread, (ii) the computer virus free equilibrium is locally and globally asymptotically stable; (iii) the model is viable via numerical simulations. From the Computer Reproduction number analysis of this model, we established that control measures (anti-virus software and repair) are very essential in mitigating and controlling computer virus.
It is recommended that the endemic existence of a dynamical system of computer virus with an infected external storage media on viral spread be considered. Lastly, this work considered only when $\theta = 0$, so further work should be carried out on when θ is not zero.

REFERENCES

Diekmann, O.and Heesterbeek, J. A. P (2000), "Mathematical epidemiology of infectious diseases: Model building, analysis and interpretation". *Wiley andsons*, New York

Diekmann, O., Heesterbeek, J. A. P. and Metz, J. A.P (1990). On the definition and computation of the basic reproduction ratio$\mathcal{R}_0$ in models for infectious diseases in heterogeneous populations *Journal of mathematical biology*, 28 (2): 365 – 382

Gan C. and Yang, X. (2015). Theoretical and experimental analysis of the impacts of removable storage media and antivirus software on viral spread, *Communications in Nonlinear Science and Numerical Simulation*, 22 (1): 167-174

Gan, C., Yang, X., Liu, W., Zhu, Q., Jin J and He, L. (2014) "Propagation of computer virus both across the Internet and external computers: A complex-network approach". *Commun. Nonli. Sci. Numer. Simul.* **19**, 2785-2792

Heffernan, J. M., Smith, R. J and Wahl, L. M (2005), " Perspective on the basic reproduction ratio", *Journal of the Royal Society Interface*, 2(4): 281-293.

Mishra, B. K and Ansari, G. M (2012). Differential Epidemic Model of Virus and Worms in Computer Network, *International Journal of Network Security*, 14(3): 149-155.

Mishra, B. K. and Saini, D. K (2007). Mathematical Models on Computer Viruses, *Elsevier International Journal of Applied Mathematics and Computation*, 187 (2): 929-936

Peng, M., He, X., Huang, J. and Dong, T. (2013). Modelling Computer Virus and Its Dynamics" *Mathematical Problems in Engineering*, Corporation. http://dx.doi.org/10.1155/2013/842614

Rahaman**, A.,** Bhuiyan, A., Habib, M.and Mozumder Z. (2015). Modelling and Threshold Sensitivity Analysis of Computer Virus Epidemic". *IOSR Journal of Computer Engineering*, 17 (1): 43-47

Saini, D. K. (2011). A Mathematical Model for the Effect of Malicious Object on Computer Network Immune System. *Applied Mathematical Modelling*, 35(1): 3777-3787 doi:10.1016/.2011.02.025

Saini, D. K. (2012). Cyber Defense: Mathematical Modelling and Simulation. *International Journal of Applied Physics and Mathematics*, 2(5): 199-209

Saini, D. K. and Mishra B. K. (2007). Design Patterns and their effect on Quality, *ACCST Research Journal*, 5 (1): 356-365

Serazzi G. and Zanero S. (2003). Computer virus propagation models. *Proceedings of 11th IEEE/ACM Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS)*.

Solomon, A. (1995). A Brief History of PC Viruses, http://www.bocklabs.wisc.edu/~janda/solomhis.html#H06

Symantec Security Response Definitions, (2010) (*http://www.symantec.com/avcenter/defs.added.html*)

Van den Deriessche, P. and Watmough, J (2002). Reproduction numbers and sub-threshold endemic equilibrium for compartment models of disease transmission. *Mathematical Bioscience* 180, 29-48

Yang, X., Liu, B. and Gan,C. (2014). "Global stability of an epidemic model of computer virus" *Abstract and Applied Analysis*. doi:10.1155/2014/456320.

Zhang, C., Feng, T., Zhao, Y. and Jiang, G. (2013). A new model for capturing the spread of computer viruses on complex-networks. *Discr. Dyn. Nat. Soc.* **2013**, Article ID 956893,

Zhang, X.(2016). "Modelling the Spread of Computer Viruses under the Effects of Infected External Computers and Removable Storage Media" *International Journal of Security and Its Applications*. 10(3): 419-428.http://dx.doi.org/10.14257/ijsia.2016.10.3.36.

Zhu, Q., Yang, X. and Ren, J. (2012). Modelling and Analysis of the spread of Computer Virus. *CommunNonlin Sci. Numer. Simul.* **17**, 5117-5124