Computer Modeling in Engineering & Sciences CMES, vol.120, no.2, pp.445-465, 2019

Numerical Treatment for Stochastic Computer Virus Model

Ali Raza[1], Muhammad Shoaib Arif[1, *], Muhammad Rafiq[2], Mairaj Bibi[3], Muhammad Naveed[1], Muhammad Usman Iqbal[4], Zubair Butt[4], Hafiza Anum Naseem[4] and Javeria Nawaz Abbasi[3]

Abstract: This writing is an attempt to explain a reliable numerical treatment for stochastic computer virus model. We are comparing the solutions of stochastic and deterministic computer virus models. This paper reveals that a stochastic computer virus paradigm is pragmatic in contrast to the deterministic computer virus model. Outcomes of threshold number C^* hold in stochastic computer virus model. If $C^* < 1$ then in such a condition virus controlled in the computer population while $C^* > 1$ shows virus persists in the computer population. Unfortunately, stochastic numerical methods fail to cope with large step sizes of time. The suggested structure of the stochastic non-standard finite difference scheme (SNSFD) maintains all diverse characteristics such as dynamical consistency, boundedness and positivity as defined by Mickens. The numerical treatment for the stochastic computer virus model manifested that increasing the antivirus ability ultimates small virus dominance in a computer community.

Keywords: Computer virus, euler maruyama scheme, stochastic differential equations, stochastic euler scheme, stochastic runge-kutta scheme, stochastic NSFD scheme, stability.

1 Introduction

A computer virus is a program that can copy itself and infect a computer without the permission or knowledge of the user. Virus stands for vital information resources under siege. A computer virus has two features as the potential to duplicate itself and the potential to affix itself to an alternative computer folder. They spread via disks, network or services such as email. Earlier viruses were propagated by computer programs or by hiding in floppy disks. Modern viruses transmit in a subtler way such as phishing which is a fraudulent practice of sending emails inquiring personal information [Patil and Jadhav 2014)]. A virus infected computer shows various symptoms. A small number of signs that may inform that a computer has the virus are slow response time, random hard drive crashes and great pop-up ads. A carefully engineered computer virus can disrupt production and cause billions of dollars in damages. For example, the con-flicker also known as down up

[1] Department of Mathematics, Stochastic Analysis & Optimization Research Group, Air University, PAF Complex E-9, Islamabad, Pakistan.

[2] Faculty of Engineering University of Central Punjab, Lahore, Pakistan.

[3] Department of Mathematics, Comsats University, Park Road Chak Shahzad Campus, Islamabad, Pakistan.

[4] Faculty of Computing National College of Business Administration and Economics, Lahore, Pakistan.

[*] Corresponding Author: Muhammad Shoaib Arif. Email: shoaib.arif@mail.au.edu.pk.

virus which was discovered in 2008, had infected millions of computers across the world. The estimated damage was over $9.1 billion [Zhu, Yang and Ren (2012)]. Viruses have evolved over a period. Their numbers are increasing each day, and they are becoming more sophisticated and harmful. Each new virus assimilates new features along with the old ones, thus making it more difficult to detect and erase [Albazzaz and Almuhanna (2016)]. The computers that we usually use do not have adequate built-in security measures as compared to larger systems thus leaving it to the users to purchase, install and utilise anti-virus software. Among significant types of computer viruses, the first type is called the boot sector virus. The boot sector is that first portion of our hard disk where routines to load our operating system reside. If these routines are disturbed or modified, our computer will not be able to work. As the name suggests, the boot sector virus modifies the boot sector program and is loaded in the memory whenever the computer is turned on. The virus is attached with the system executable files, for example, exe, .com etc. Chernobyl virus detects all the Microsoft office files and corrupts them. It also deletes the logical partition information of the disks. Users cannot access their files from the drives, because of this virus. Logic bomb virus occurs only when a particular condition is met. The condition could be any date or any completion of the process (time). After the condition is met, the virus is invoked. This virus can be discovered by chance. Trojan horse virus is embedded in the computer programs. When we run these programs, this virus is activated. Its primary purpose is destruction. The Redlof virus is a polymorphic virus, which is written in VB Script (language). When instructions are being written, this virus is embedded in the programs. It corrupts the folder data file, which is the part of windows active desktop.

An ideal structure of a computer virus holds three subroutines. The task of first sub-routine, known as infect-executable, is to find executable files and infect them by copying its code into them. Second sub-routine, namely do-damage also called the payload of the virus, is a code which delivers the malicious part of the virus. The final sub-routine trigger-pulled inspects if the required conditions are met in order to deliver its payload [Patil and Jadhav (2014)]. Much work has been done on the concept of computer viruses such as new techniques for virus detection and its prevention. New researches help us to understand how sophisticated viruses work. To inspect computer viruses, the compartment modelling technique of infectious diseases was proposed [Cohen (1987); Murray (1988)].

1n last decade of the twentieth century the authors were the first ones to typical the spreading behaviour of the computer virus. This paved the way for developing mathematical models for computer virus propagation [Billings, Spears and Schwartz (2002); Han and Tan (2010); Mishra and Jha (2007); Piqueira and Araujo (2009); Piqueira, Vasconcelos, Gabriel et al. (2008); Ren, Yang, Yang et al. (2012); Ren, Yang, Zhu et al. (2012); Wierman and Marchette (2004); Yuan and Chen (2008)]. Just like any biological virus the computer virus also contains a dormant period. During this period a single computer is vulnerable to a computer virus but is not infectious yet. An exposed computer, which is an infected computer in dormancy, will not transmit the virus to other computers quickly; but it still can be infected. The delay used in some models of computer virus is also based on these characteristics. It shows that although the exposed computer does not infect other computers, it still has infectivity [Han and Tan (2010); Zhu, Yang and Ren (2012)]. The authors proposed SLB and SLBS models in which they observed that the computer has latency [Yang, Yang, Zhu et al. (2013); Yang, Yang, Wen et al. (2012)] and

in this period of latency it also has infectivity. Multilayer networks can be responsible for spreading computer viruses. Examples of computer virus include mobile phone virus, which can use 3G, 4G, Wi-Fi, or Bluetooth as a tool to communicate with other networks. Founded on the notion of multilayer network, the IBMF (Individual-Based Mean Field) was applied to the SLBS model by Zhang [Zhang (2018)]. A model was developed to expect the activities of worm on the network. A time-delayed SIQVD worm propagation model with variable infection rate was framed. This model can be utilized for internet worms [Yao, Fu, Yang et al. (2018)]. A research has been conducted on the susceptible, latent, breaking-out, quarantine and susceptible (SLBQRS) computer virus model. Three finite difference patterns have been used to solve the epidemic system [Fatima, Ali, Ahmed et al. (2018)]. HAM (Homotopy Analysis Method) has been utilized to solve the modified nonlinear SIR epidemiological model of computer viruses [Noeiaghdam, Suleman and Budak (2018)]. The propagation mechanism of computer viruses is explored by the node-based models. To examine the dynamic behavior of a computer virus a model named SLIS which is node-based has also been proposed which demonstrated that the virus-free equilibrium is asymptotically or exponentially stable [Yu, Hu and Zeng (2019)].

However, the influence of installing anti-virus software and the period of inactivity was not taken into account. The interaction frequency of afresh entered computers on the internet from vulnerable status to unprotected status is the same as that of vulnerable status entering into infected status. This tabloid works on the stochastic model of computer virus namely SEIR model. It describes the vulnerability of susceptible computer and how they can get infected by other infected or exposed computers and thus changing to exposed status. This model based on fake immunity considers the bilinear incident rate for the latent period and infection status. We suppose that computers which freshly join the internet are susceptible. The computers interact with exposed computers, let their adequate contact rate is denoted by β_1 and computers also interact with infected computers, let their adequate interaction be denoted by β_2 Anti-virus software will compel the segments that newly entered the internet to enter the class $R(t)$, and the segments of computer that come in contact with exposed and infected computers will be in latent state before becoming infectious and enter the class $E(t)$. A threshold factor C^* is used to determine the dynamic characteristics of the suggested model.

Scientific demonstrating has appeared as an efficient tool for the extraction of comprehensive insight about widespread viruses. For inspecting the comparison and sensitivity of conjuncture paradigms, the construction and the likely imitations of the model are used. These models' outcomes are expected to predict certain parameters that are crucial to the public's health. The parameters include a biological factor, host and mediator. This critical information develops health services which are used by the authority that is responsible for the public health policy [Anwar, Goldberg, Fraser et al. (2014)]. Many types of research have been done on various computer virus transmission dynamics models [Cai and Li (2010); Peng, He, Huang et al. (2013)]. It had already been established that non-linear IVPs do not always hold analytical solutions. Runge-Kutta and Euler methods cause disorder and fraudulent oscillations for some parameters of the discretisation parameters [Zafar, Rehan and Mushtaq (2017); Zafar, Rehan, Mushtaq et al. (2017); Zafar,

Rehan and Mushtaq (2017); Bayram, Partal and Buyukoz (2018)]. Such models prove to be less advantaged choices, due to uncertainties.

Stochastic differential equation models play an essential role in many branches of applied sciences such as industries, including population dynamics, finance, mechanics, medicine and biology as they provide an extra degree of realism compared to their deterministic counterpart. [Bayram, Partal and Buyukoz (2018)].

Generally, the elasticity of stochastic differential equations (SDEs) is difficult, and the solutions of stochastic differential equations do not exist explicitly. Different numerical schemes utilized to join the indicated equations in understanding convergence is difficult [Mickens (1994, 2005); Cresson and Pierret (2014); Pierret (2015)]. An obvious question can be raised on numerical schemes despite the convergence analysis: Are the dynamical characteristics of the original system protected by the numerical scheme [Mickens (2005)]?

In the case of deterministic modelling, Euler and Runge-Kutta- usual pragmatic numerical schemes do not protect the dynamical characteristics of the initial system. Neither is it protected by stochastic Euler, stochastic Runge-Kutta and Euler Maruyama scheme which begs the question: Is there any stochastic numerical method that can protect all dynamical properties?

Our foremost persistence in this paper is to propose a method which we call stochastic non-standard finite difference scheme (SNSFD). It is built on the model proposed by Mickens in the deterministic case [Mickens (1994, 2005)].

This paper is further divided into the following segments:

In Section 2, we have given all the basic details of SDEs. Section 3 deals with the invention of stochastic models. Section 4 is dedicated to the discussion of deterministic computer virus paradigm and the points of equilibrium. In Section 5, we look for the construction of stochastic computer virus model. In Section 6, different stochastic numerical schemes' outcomes are compared with deterministic results. Finally, in Section 7, we will reach our deduction and provide our forthcoming work.

2 Preliminaries

Einstein gave the idea of stochastic differential equations in (1905) [Gard (1988); Karatzas and Shreve (1991); Platen (1991); Mickens (2005); Allen (2007); Britton (2010)]. These days the stochastic differential equations are catching much attention because of their growth in systems of our daily life. One of the reasons for their growth is that the ODEs (Ordinary Differential Equations) do not support randomness and stochastic ideas. A stochastic calculus distributes a mathematical constituent for the manner of SDEs. Generally, the stochastic differential equation with continuous time t and variable C_t can be written as

$$\mathrm{dC_t} = \mathrm{u(t, C_t)dt} + \mathrm{v(t, C_t)dB(t)}. \tag{1}$$

moreover, the integral form is

$$\mathrm{C(t)} = \mathrm{c} + \int_{\mathrm{t_o}}^{\mathrm{t}} \mathrm{u(s, C_s)ds} + \int_{\mathrm{t_o}}^{\mathrm{t}} \mathrm{v(s, C_s)dB_s}. \tag{2}$$

The differential Eq. (1) is termed as the Ito stochastic differential equation. Here $\mathrm{u(t, T_t)}$ and $\mathrm{v(t, T_t)}$ are the drift coefficient and diffusion coefficient. The casual variable c at

an instant t_o is utilised as an initial value. An outcome T_t of equation one and two is known as a stochastic process.

3 The building of stochastic models

Epidemics are usually twisted by non-linear systems pragmatic through patchy noisy data. There are two types of epidemic models as deterministic and stochastic models. The deterministic epidemic models do not preserve the natural uncertainty of virus dynamics, but the idea of stochastic epidemic models preserves all types of the uncertainty of virus dynamics. Deterministic epidemic models can be diffused to stochastic epidemic models by numerous conducts [Allen, Allen, Arciniega et al. (2008)]. Ito SDEs did the stochastic epidemic modelling. The theme of Ito SDEs gives a more convenient way to study the stochastic epidemic models. The idea of the Ito stochastic differential equation can be pronounced by methods such as parametric and non-parametric perturbations. In the former technique, we select a parameter from the model and transform it into the model's random variables. In the latter, we propose the Brownian motion in each differential equation (or propose the extra stochasticity parameter). In comparison, the non-parametric perturbation is more convenient by Allen [Karatzas and Shreve (1991); Platen (1991); Allen and Burgin (2000); Holt, Davis and Leirs (2006); Allen (2007); Britton (2010)]. We will simulate the way of non-parametric perturbation into deterministic epidemic models and will check its efficacy by using different numerical models on stochastic epidemic models. Here, the idea is to examine the relationship between deterministic and stochastic models.

4 Deterministic computer virus model

Figures and tables should be inserted in the text of the manuscript.

Here, we consider the deterministic computer virus model [Peng, He, Huang et al. (2013)]. Let at any non-specific time t, the defined variables are $S(t)$(exemplifies susceptible computers' fraction), $E(t)$ (exemplifies exposed computers' fraction), $I(t)$(exemplifies infected computers' fraction) and $R(t)$(exemplifies recovered computers' fraction). The communication dynamics of computer virus model is illustrated below.

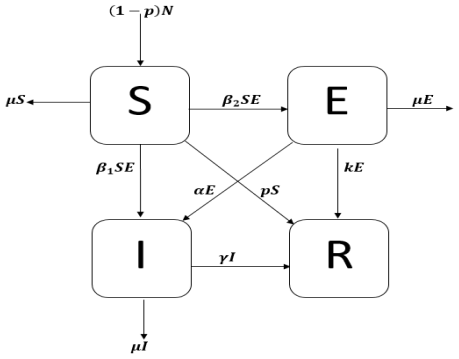


Figure 1: Flow map of computer virus model

The parameters of model are pronounced as p (pronounces the susceptible computer recovery rate under the influence of antivirus capability), N (pronounces the external computers connection rate to the network), β_1 (pronounces the susceptible computers contact rate to the infected computer, which ultimates their transformation to exposed status. However the computer has not crashed), β_2 (pronounces the susceptible computers contact rate to exposed computer, which results its transformation to exposed status), μ (pronounces the withdrawn computer rate from the network), k (pronounces the exposed computer recovery rate in network, under the influence of anti-virus capability) α (pronounces the exposed computer rate that cannot be treated by anti-virus software and crashed), r (pronounces the infected computers recovery rate that are treated).

The governing equations of the computer virus model as follows:

$$\left.\begin{aligned}
\frac{dS(t)}{dt} &= (1-p)N - \beta_1 S(t)I(t) - \beta_2 S(t)E(t) - pS(t) - \mu S(t) \\
\frac{dE(t)}{dt} &= \beta_1 S(t)I(t) + \beta_2 S(t)E(t) - kE(t) - \alpha E(t) - \mu E(t) \\
\frac{dI(t)}{dt} &= \alpha E(t) - rI(t) - \mu I(t) \\
\frac{dR(t)}{dt} &= pS(t) + kE(t) + rI(t)
\end{aligned}\right\} \quad (3)$$

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

with conditions $S(t) \geq 0, E(t) \geq 0, I(t) \geq 0, R(t) \geq 0$

The reduced form of computer virus model is

$$\left.\begin{aligned}
\frac{dS(t)}{dt} &= (1-p)N - \beta_1 S(t)I(t) - \beta_2 S(t)E(t) - pS(t) - \mu S(t) \\
\frac{dE(t)}{dt} &= \beta_1 S(t)I(t) + \beta_2 S(t)E(t) - kE(t) - \alpha E(t) - \mu E(t) \\
\frac{dI(t)}{dt} &= \alpha E(t) - rI(t) - \mu I(t)
\end{aligned}\right\} \quad (5)$$

4.1 Steady states of the computer virus model

Given below are two ways of equilibrium point to categorize the steady states of computer virus model (3) as shadows:

Virus-free equilibrium is $V_1 = (S^o, E^o, I^o) = \left(\frac{A}{a}, 0, , 0\right)$

Endemic equilibrium is $E_1 = (S^o, E^o, I^o) = \left(\frac{A}{aC^*}, \frac{A(C^*-1)}{bC^*}, \frac{A\alpha(C^*-1)}{bcC^*}\right)$

where,

$C^* = \frac{A(\beta_1\alpha+\beta_2 c)}{abc}$, $a = p + \mu$, $b = k + \alpha + \mu$, $c = r + \mu$, $A = (1-p)N$

Note that C^* is the reproductive number of the computer virus model (5). It has an important part in virus dynamics. If $C^* < 1$ then this helps us to control the virus and if $C^* > 1$ then this will be an alarming situation of virus in the computer population.

5 Stochastic computer virus model

Let $C(t) = [S(t), E(t), I(t)]^T$ tformulates the SDEs of computer virus model (1). We want to calculate the expectations $E^*[\Delta C]$ and $E^*[\Delta C \Delta C^T]$. In order to find them the likely changes and their related transition probabilities are in the following table (Tab. 1).

Table 1: Possible changes in the process for the computer virus model (5)

Transition	Probabilities
$(\Delta C)_1 = [1 \quad 0 \quad 0]^T$	$P_1 = (1-p)N\Delta t$
$(\Delta C)_2 = [-1 \quad 1 \quad 0]^T$	$P_2 = \left(\beta_1 S(t)I(t) + \beta_2 S(t)E(t)\right)\Delta t$
$(\Delta C)_3 = [-1 \quad 0 \quad 0]^T$	$P_3 = (p+\mu)S(t)\Delta t$
$(\Delta C)_4 = [0 \quad -1 \quad 1]^T$	$P_4 = \alpha E(t)\,\Delta t$
$(\Delta C)_5 = [0 \quad -1 \quad 0]^T$	$P_5 = (k+\mu)E(t)\,\Delta t$
$(\Delta C)_6 = [0 \quad 0 \quad -1]^T$	$P_6 = (\gamma+\mu)I(t)\Delta t$

The expectation of computer virus model (5) is defined as

$E^*[\Delta C] = \sum_{i=1}^{6} P_i\,(\Delta C)_i$

.Expectation $= E^*[\Delta C] = \begin{bmatrix} (1-p)N - \left(\beta_1 S(t)I(t) + \beta_2 S(t)E(t)\right) - (p+\mu)S(t) \\ \left(\beta_1 S(t)I(t) + \beta_2 S(t)E(t)\right) - \alpha E(t) - (k+\mu)E(t) \\ \alpha E(t) - (\gamma+\mu)I(t) \end{bmatrix}\Delta t$

The variance of the computer virus model is defined as Var= $E^*[\Delta C \Delta C^T] = \sum_{i=1}^{6} P_i\,[(\Delta C)_i][(\Delta C)_i]^T$.

$E^*[\Delta C\,\Delta C^T] = \begin{bmatrix} W_{11} & W_{12} & W_{13} \\ W_{21} & W_{22} & W_{23} \\ W_{31} & W_{32} & W_{33} \end{bmatrix}\Delta t$.

where,

$.W_{11} = (1-p)N + \left(\beta_1 S(t)I(t) + \beta_2 S(t)E(t)\right) + (p+\mu)S(t), W_{12} = -\left(\beta_1 S(t)I(t) + \beta_2 S(t)E(t)\right), W_{13} = 0$, $W_{21} = -\left(\beta_1 S(t)I(t) + \beta_2 S(t)E(t)\right), W_{22} = \left(\beta_1 S(t)I(t) + \beta_2 S(t)E(t)\right) + \alpha E(t) + (k+\mu)E(t), W_{23} = -\alpha E(t), .W_{31} = 0, W_{32} = -\alpha E(t), W_{33} = \alpha E(t) + (r+\mu)I(t).$

The SDE satisfy the diffusion processes, therefore,

$\frac{dC(t)}{dt} = G(C(t), t) + H(C(t), t)\frac{dB(t)}{dt}$.

If $\text{drift} = G(C(t), t) = \frac{E^*[\Delta C]}{\Delta t}$ and $\text{diffusion} = H(C(t), t) = \sqrt{\frac{E^*[\Delta C\,\Delta C^T]}{\Delta t}}$, then the SDE of computer virus model (5) is

$$dC(t) = G(C(t), t)dt + H(C(t), t)dB(t). \tag{6}$$

with initial conditions $C(0) = C_o = [50, 40, 20]^T$, $0 \le t \le C$ and $B(t)$ is the Brownian motion.

5.1 Euler maruyama scheme

The Euler Maruyama scheme [Maruyama (1955)] to determine the numerical result of SDE (6) by using the parameters values given in literature [Peng, He, Huang et al. (2013)] (Tab. 2).

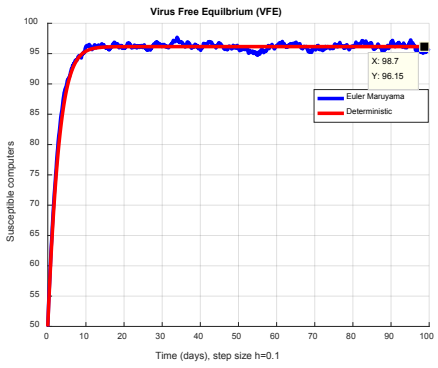
Table 2: Values of Parameter [Peng, He, Huang et al. (2013)]

	Values (Days)	
Parameters	**VFE**	**EE**
μ	0.001	0.02
p	0.7	0.5
k	0.02	0.4
A	0.09	0.6
r	0.04	0.6
N	10	100
β_1	0.002	0.7
β_2	0.003	0.8
σ_1	0.9	0.9
σ_2	0.8	0.8
σ_3	0.7	0.7

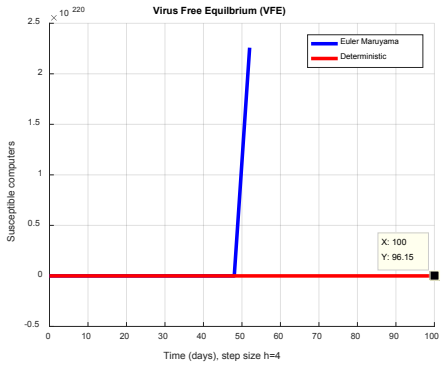
The Euler Maruyama scheme of stochastic differential Eq. (6) shadows:

$$C_{n+1} = C_n + f(C_n, t)\Delta t + L(C_n, t)dB(t).$$

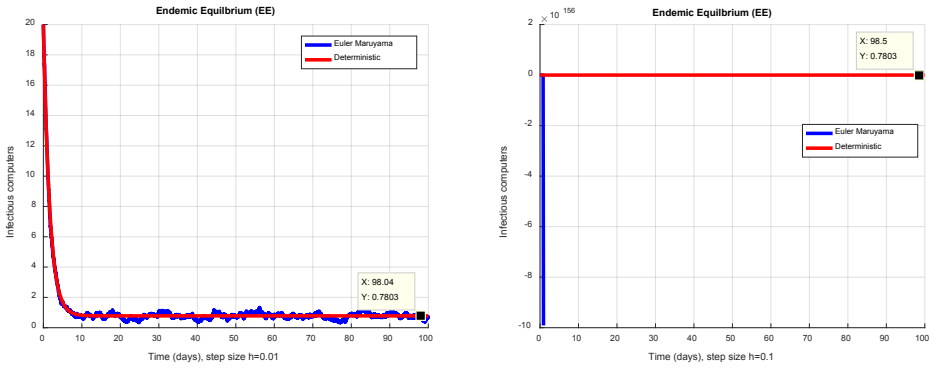
where 'Δt ' is the time step size. The confidence interval holds the solution to stochastic differential equations for both equilibriums as presented in the above numerical experiments. The solution of deterministic computer virus model for the virus-free symmetry $V_1^* = (96.15,0,0)$ and the procreative number $C^* = 0.2858 < 1$ helps us to control this virus in the computer population. The endemic equilibrium $E_1^* = (1.2573, 48.3787, 0.7803)$ and the reproductive number $C^* = 76.4791 > 1$ shows that the virus is endemic in the computer population. The graphical behaviour of Euler Maruyama scheme for both virus-free equilibrium and endemic equilibrium at different sub-computers as shown in Fig. 2.



(a)



(b)



(c) **(d)**

Figure 2: Comparison in solutions of euler maruyama and deterministic **(a)** Susceptible computers fraction at VFE Point for h=0.1 **(b)** Susceptible computers fraction at VFE Point for h=4 **(c)** infectious computers fraction at EE Point for h=0.01 **(d)** infectious computers fraction at EE Point for h=0.1

5.2 Non-parametric perturbation of stochastic computer virus model

An additional way to establish the stochastic differential equations from the deterministic ordinary differential equations is to instigate the non-parametric perturbation in every single differential equation of computer virus model (5) as shadows [Raza, Arif and Rafiq (2019)]:

$$\left.\begin{aligned} dS(t) &= \big((1-p)N - \beta_1 S(t)I(t) - \beta_2 S(t)E(t) - (p+\mu)S(t) + \sigma_1 dB_1(t)S(t)\big)dt \\ dE(t) &= \big(\beta_1 S(t)I(t) + \beta_2 S(t)E(t) - \alpha E(t) - (k+\mu)E(t) + \sigma_2 dB_2(t)E(t)\big)dt \\ dI(t) &= \big(\alpha E(t) - (\gamma+\mu)I(t) + \sigma_3 dB_3(t)I(t)\big)dt \end{aligned}\right\} \quad (7)$$

with initial conditions $C(0) = [S(0), E(0), I(0),]^T = [50, 40, 20]^T$ where $\sigma_1, \sigma_2,$ and σ_3 is casualness of each cubicle of the computer virus model and $B_j(t), (j = 1,2,3)$ are the sovereign Brownian gestures. This type of computer virus model does not have a specific result because of a non-differentiability span of Brownian gesture. For this, we shall introduce the new stochastic numerical methods.

5.2.1 Stochastic Euler scheme

The designed form of stochastic Euler scheme for the model (7) as shadows [Raza, Arif and Rafiq (2019)]:

$$\left.\begin{aligned} S^{n+1}(t) &= S^n(t) + h[(1-p)N - \beta_1 S^n(t)I^n(t) - \beta_2 S^n(t)E^n(t) - (p+\mu)S^n(t) + \sigma_1 dB_1(t)S^n(t)] \\ E^{n+1} &= E^n(t) + h[\beta_1 S^n(t)I^n(t) + \beta_2 S^n(t)E^n(t) - \alpha E^n(t) - (k+\mu)E^n(t) + \sigma_2 dB_2(t)E^n(t)] \\ I^{n+1} &= I^n(t) + h[\alpha E^n(t) - (r-\mu)I^n(t) + \sigma_3 dB_3(t)I^n(t)] \end{aligned}\right\} \quad (8)$$

We pretend the solutions of the model (8) by using the Matlab database and parameters values assumed in Peng et al. [Peng, He, Huang et al. (2013)] (Tab. 2) and h is any time step size.

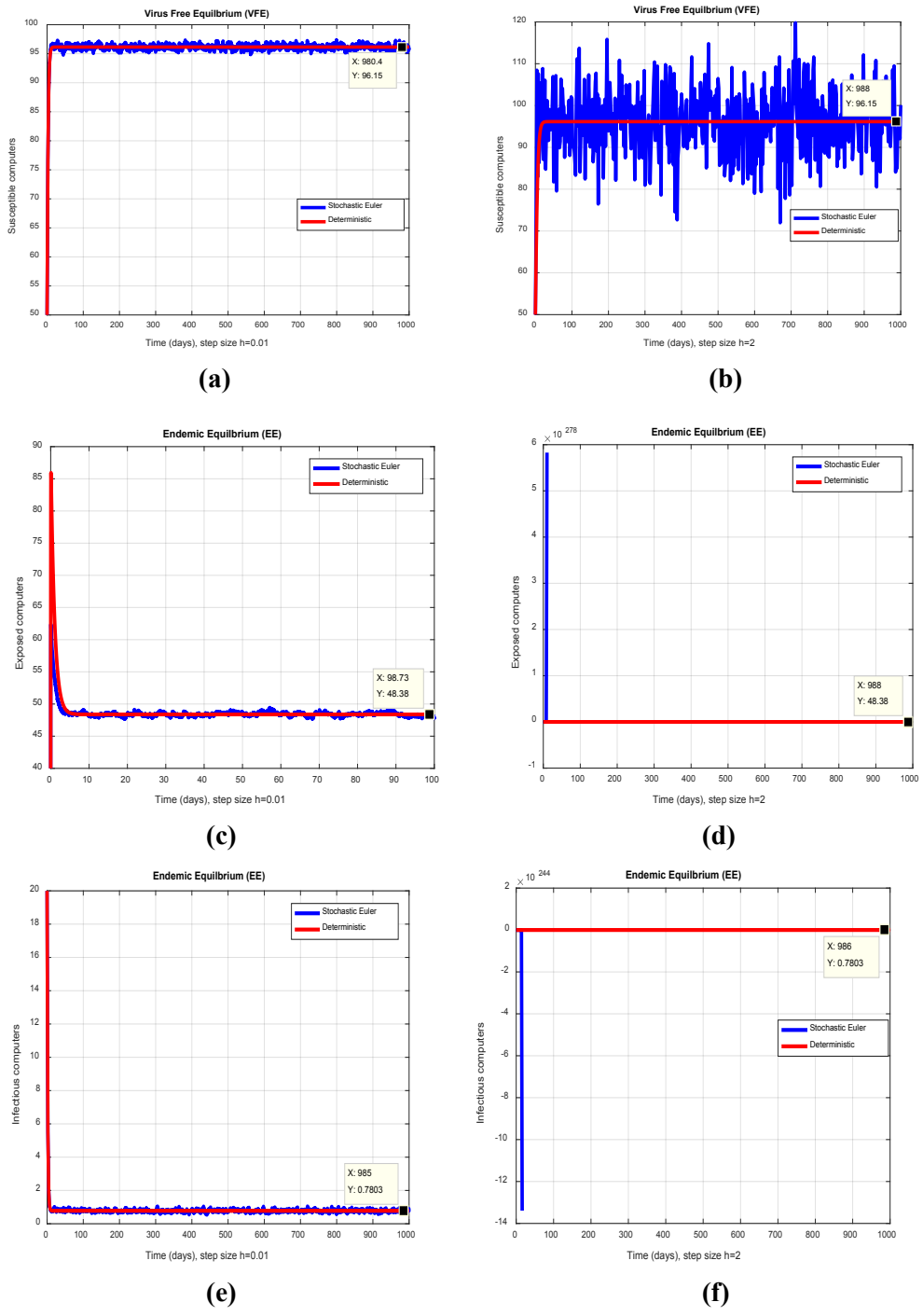


Figure 3: Comparison in solutions of stochastic euler and deterministic **(a)** Susceptible computers fraction at VFE Point for h=0.01 **(b)** Susceptible computers fraction at VFE Point for h=2 **(c)** Exposed computers fraction at EE Point for h=0.01 **(d)** Exposed

computers fraction at EE Point for h=2 **(e)** Infectious computers fraction at EE Point for h=0.01 **(f)** Infectious computers fraction at EE Point for h=2

5.2.2 Stochastic runge-kutta scheme

The designed form of stochastic runge-kutta scheme for the model (7) as shadows [Raza, Arif and Rafiq (2019)]:

First Stage

$A_1 = h[(1-p)N - \beta_1 S^n(t) I^n(t) - \beta_2 S^n(t) E^n(t) - (p+\mu) S^n(t) + \sigma_1 dB_1(t) S^n(t)].$

. $B_1 = h[\beta_1 S^n(t) I^n(t) + \beta_2 S^n(t) E^n(t) - \alpha E^n(t) - (k+\mu) E^n(t) + \sigma_2 dB_2(t) E^n(t)].$

. $C_1 = h[\alpha E^n(t) - (r-\mu) I^n(t) + \sigma_3 dB_3(t) I^n(t)].$

Second Stage

. $A_2 = h\left[(1-p)N - \beta_1 (S^n(t) + \frac{A_1}{2})\left(I^n(t) + \frac{C_1}{2}\right) - \beta_2 (S^n(t) + \frac{A_1}{2})(E^n(t) + \frac{B_1}{2}) - (p + \mu)(S^n(t) + \frac{A_1}{2}) + \sigma_1 dB_1(t)(S^n(t) + \frac{A_1}{2})\right].$

. $B_2 = h[\beta_1 (S^n(t) + \frac{A_1}{2})(I^n(t) + \frac{C_1}{2}) + \beta_2 (S^n(t) + \frac{A_1}{2})(E^n(t) + \frac{B_1}{2}) - \alpha (E^n(t) + \frac{B_1}{2}) - (k+\mu)(E^n(t) + \frac{B_1}{2}) + \sigma_2 dB_2(t)(E^n(t) + \frac{B_1}{2})].$

. $C_2 = h\left[\alpha\left(E^n(t) + \frac{B_1}{2}\right) - (r-\mu)\left(I^n(t) + \frac{C_1}{2}\right) + \sigma_3 dB_3(t)\left(I^n(t) + \frac{C_1}{2}\right)\right].$

Third Stage

. $A_3 = h\left[(1-p)N - \beta_1 (S^n(t) + \frac{A_2}{2})\left(I^n(t) + \frac{C_2}{2}\right) - \beta_2 (S^n(t) + \frac{A_2}{2})(E^n(t) + \frac{B_2}{2}) - (p + \mu)(S^n(t) + \frac{A_2}{2}) + \sigma_1 dB_1(t)(S^n(t) + \frac{A_2}{2})\right]$.

. $B_3 = h[\beta_1 (S^n(t) + \frac{A_2}{2})(I^n(t) + \frac{C_2}{2}) + \beta_2 (S^n(t) + \frac{A_2}{2})(E^n(t) + \frac{B_2}{2}) - \alpha (E^n(t) + \frac{B_2}{2}) - (k+\mu)(E^n(t) + \frac{B_2}{2}) + \sigma_2 dB_2(t)(E^n(t) + \frac{B_2}{2})].$

. $C_3 = h\left[\alpha\left(E^n(t) + \frac{B_2}{2}\right) - (r-\mu)\left(I^n(t) + \frac{C_2}{2}\right) + \sigma_3 dB_3(t)\left(I^n(t) + \frac{C_2}{2}\right)\right].$

Fourth Stage

. $A_4 = h\left[(1-p)N - \beta_1 (S^n(t) + \frac{A_3}{2})\left(I^n(t) + \frac{C_3}{2}\right) - \beta_2 (S^n(t) + \frac{A_3}{2})(E^n(t) + \frac{B_3}{2}) - (p + \mu)(S^n(t) + \frac{A_3}{2}) + \sigma_1 dB_1 (S^n(t) + \frac{A_3}{2})\right].$

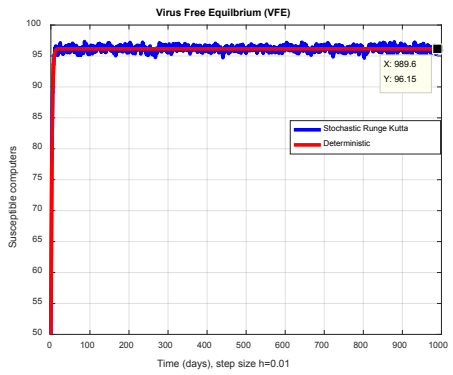
. $B_4 = h[\beta_1 (S^n(t) + \frac{A_3}{2})(I^n(t) + \frac{C_3}{2}) + \beta_2 (S^n(t) + \frac{A_3}{2})(E^n(t) + \frac{B_3}{2}) - \alpha (E^n(t) + \frac{B_3}{2}) - (k+\mu)(E^n(t) + \frac{B_3}{2}) + \sigma_2 dB_2 (E^n(t) + \frac{B_3}{2})].$

. $C_4 = h\left[\alpha\left(E^n(t) + \frac{B_3}{2}\right) - (\gamma+\mu)\left(I^n(t) + \frac{C_3}{2}\right) + \sigma_3 dB_3\left(I^n(t) + \frac{C_3}{2}\right)\right].$

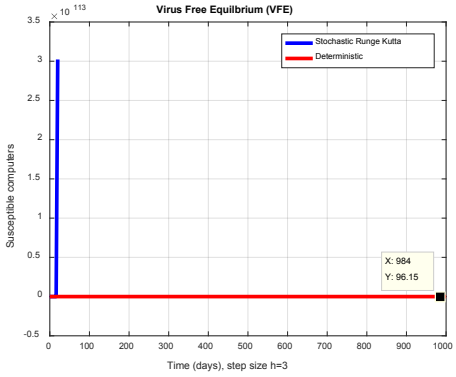
Final Stage

$$\left.\begin{aligned} S^{n+1}(t) &= S^{n}(t) + \frac{1}{6}[A_1 + 2A_2 + 2A_3 + A_4] \\ E^{n+1}(t) &= E^{n}(t) + \frac{1}{6}[B_1 + 2B_2 + 2B_3 + B_4] \\ I^{n+1}(t) &= I^{n}(t) + \frac{1}{6}[C_1 + 2C_2 + 2C_3 + C_4] \end{aligned}\right\} \tag{9}$$

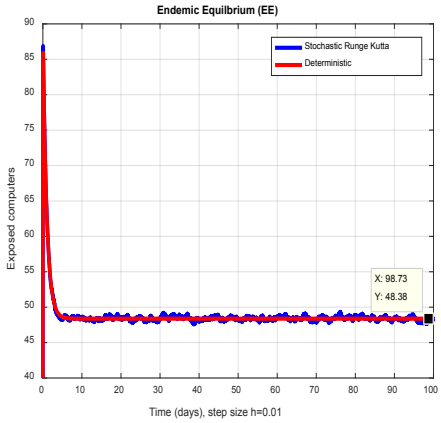
We pretend the solutions of the model (9) by using the Matlab database and parameters values assumed in Peng et al. [Peng, He, Huang et al. (2013)] (Tab. 2) and h is any time step size.



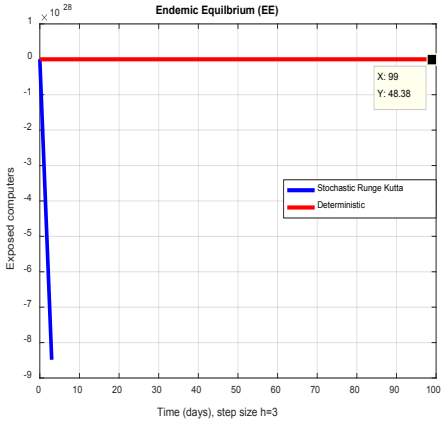
(a)



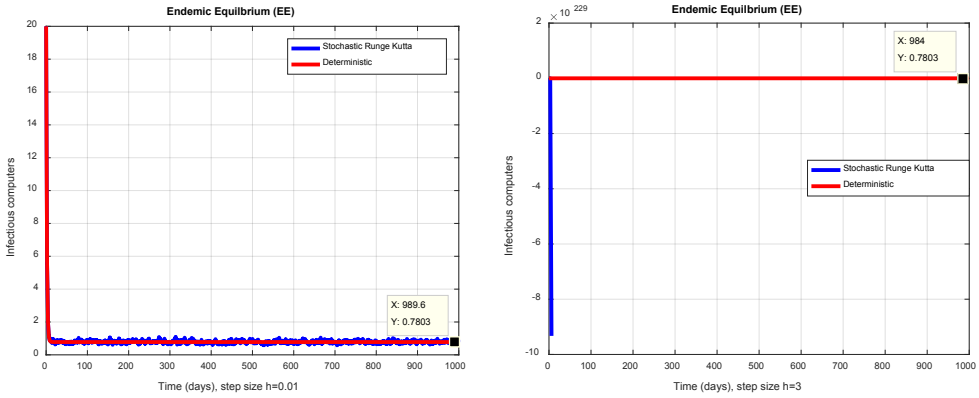
(b)



(c)



(d)



(e) **(f)**

Figure 4: Comparison in solutions of stochastic runge kutta and deterministic **(a)** Susceptible computers fraction at VFE Point for h=0.01 **(b)** Susceptible computers fraction at VFE Point for h=3 **(c)** Exposed computers fraction at EE Point for h=0.01 **(d)** Exposed computers fraction at EE Point for h=3 **(e)** Infectious computers fraction at EE Point for h=0.01 **(f)** Infectious computers fraction at EE Point for h=3

5.2.3 Stochastic NSFD scheme

The recommended frame works of SNSFD for the model (7) as shadows [Raza, Arif and Rafiq (2019)]:

$$\left.\begin{aligned} S^{n+1}(t) &= \frac{S^n(t)+\varphi(h)[(1-p)N+\sigma_1 dB_1(t)S^n(t)]}{(1+\varphi(h)\beta_1 I^n(t)+\varphi(h)\beta_2 E^n(t)+\varphi(h)(p+\mu))} \\ E^{n+1}(t) &= \frac{E^n(t)+\varphi(h)[\beta_1 S^n(t)I^n(t)+\beta_2 S^n(t)E^n(t)+\sigma_2 dB_2(t)E^n(t)]}{(1+\varphi(h)\alpha+\varphi(h)(k+\mu))} \\ I^{n+1}(t) &= \frac{I^n(t)+\varphi(h)[\alpha E^n(t)+\sigma_3 dB_3(t)I^n(t)]}{(1+\varphi(h)(r-\mu))} \end{aligned}\right\} \quad (10)$$

We pretend the solutions of the model (8) by using the Matlab database and parameters values assumed in Peng et al. [Peng, He, Huang et al. (2013)] (Tab. 2) and h is any time step size.

5.2.4 Stability Analysis

We consider the suggested framework of stochastic NSFD scheme as follows:

$$F = \frac{S(t)+hA+h\sigma_1 dB_1(t)S(t)}{1+h\beta_1 I(t)+h\beta_2 E(t)+ah}$$

$$G = \frac{E(t)+h\beta_1 S(t)I(t)+h\beta_2 S(t)E(t)+\sigma_2 dB_2(t)E(t)}{1+hb}$$

$$H = \frac{I+\alpha hE(t)+\sigma_3 dB_3(t)I(t)}{1+hc}$$

We define, The Jacobian matrix J as follows:

$$J=\begin{bmatrix}\frac{\partial F}{\partial S(t)} & \frac{\partial F}{\partial E(t)} & \frac{\partial F}{\partial I(t)}\\ \frac{\partial G}{\partial S(t)} & \frac{\partial G}{\partial E(t)} & \frac{\partial G}{\partial I(t)}\\ \frac{\partial H}{\partial S(t)} & \frac{\partial F}{\partial E(t)} & \frac{\partial H}{\partial I(t)}\end{bmatrix}$$

where, $\frac{\partial F}{\partial S}=\frac{h\sigma_1 dB_1(t)}{1+h\beta_1 I+h\beta_2 E+ah}$, $\frac{\partial G}{\partial S}=\frac{h\beta_1 I+h\beta_2 E}{1+hb}$ and $\frac{\partial H}{\partial S}=0$.

$\frac{\partial F}{\partial E}=-\frac{(S+hA)h\beta_2}{(1+h\beta_1 I+h\beta_2 E+ah)^2}$, $\frac{\partial G}{\partial E}=\frac{1+h\beta_2 S}{1+hb}$ and $\frac{\partial H}{\partial E}=\frac{\alpha h}{1+hc}$.

$\frac{\partial F}{\partial I}=-\frac{(S+hA)h\beta_1}{(1+h\beta_1 I+h\beta_2 E+ah)^2}$, $\frac{\partial G}{\partial I}=\frac{h\beta_1 S}{1+hb}$ and $\frac{\partial H}{\partial I}=\frac{1}{1+hc}$

$$J=\begin{bmatrix}\frac{1}{1+h\beta_1 I+h\beta_2 E+ah} & -\frac{(S+hA)h\beta_2}{(1+h\beta_1 I+h\beta_2 E+ah)^2} & -\frac{(S+hA)h\beta_1}{(1+h\beta_1 I+h\beta_2 E+ah)^2}\\ \frac{h\beta_1 I+h\beta_2 E}{1+hb} & \frac{1+h\beta_2 S}{1+hb} & \frac{h\beta_1 S}{1+hb}\\ 0 & \frac{\alpha h}{1+hc} & \frac{1}{1+hc}\end{bmatrix}$$

By using the virus-free equilibrium $\left(\frac{A}{\alpha},0,0\right)$ we have

$$J\left(\frac{A}{\alpha},0,0\right)=\begin{bmatrix}\frac{1}{1+ah} & -\frac{\left(\frac{A}{\alpha}+hA\right)h\beta_2}{(1+ah)^2} & -\frac{\left(\frac{A}{\alpha}+hA\right)h\beta_1}{(1+ah)^2}\\ 0 & \frac{1+\frac{h\beta_2 A}{\alpha}}{1+hb} & \frac{\frac{h\beta_1 A}{\alpha}}{1+hb}\\ 0 & \frac{\alpha h}{1+hc} & \frac{1}{1+hc}\end{bmatrix}$$

The eigen value of the Jacobean matrix as follows:

$\lambda_1=\frac{1}{1+ah}<1$,

Because the stochasticity like as $\sigma_1,\sigma_2,$ and σ_3 is small noise disturbance with Brownian motions $B_j(t),(j=1,2,3)$ in each compartment of the computer virus model. So, each stochastic term $\sigma_j.(j=1,2,3)<a$, where the parameter a is the sum of the recovery rate of susceptible computer due to the antivirus ability of network and rate of computer removed from network [Peng, He, Huang et al. (2013)].

$$J=\begin{bmatrix}\frac{a+h\beta_2 A+ah\sigma_2 dB_2}{a(1+hb)} & \frac{h\beta_1 A}{a(1+hb)}\\ \frac{\alpha h}{1+hc} & \frac{1+h\sigma_3 dB_3}{1+hc}\end{bmatrix}.$$

A = Trace of the Jacobean matrix.

B = The determinant of the Jacobean matrix.

$A=\frac{a+h\beta_2 A+ah\sigma_2 dB_2}{a(1+hb)}+\frac{1+h\sigma_3 dB_3}{1+hc}$

$$B = \frac{(a+h\beta_2 A+ah\sigma_2 dB_2)(1+h\sigma_3 dB_3)}{a(1+hb)(1+hc)} - \frac{ah^2\beta_1 A}{a(1+hb)(1+hc)}$$

Lemma 5.2.5

For the quadratic equation $\lambda^2 - C_1\lambda + C_2 == 0$, $|\lambda_i| < 1, i = 1,2$; if and only if succeeding conditions are satisfied [Brauer and Chavez (2001)]:

(i) $1 + C_1 + C_2 > 0$

(ii) $1 - C_1 + C_2 > 0$

(iii) $C_2 < 1$

(i). $1 + C_1 + C_2 > 0$

$\because 1 > 0 , C_1 > 0 ,$ To prove $C_2 > 0$.

$$\Rightarrow \frac{(a+h\beta_2 A+ah\sigma_2 dB_2)(1+h\sigma_3 dB_3)}{a(1+hb)(1+hc)} - \frac{ah^2\beta_1 A}{a(1+hb)(1+hc)} > 0$$

$$\Rightarrow (a + h\beta_2 A + ah\sigma_2 dB_2)(1 + h\sigma_3 dB_3) - ah^2\beta_1 A > 0.$$

$$\Rightarrow h^2(a\beta_1 A - \beta_2 A\sigma_3 dB_3 - a\sigma_2\sigma_3 dB_2 dB_3) - h\,(a\sigma_3 dB_3 + a\sigma_2 dB_2 + \beta_2 A) < a.$$

$$\Rightarrow h^2 - h\,\frac{(a\sigma_3 dB_3+a\sigma_2 dB_2+\beta_2 A)}{(a\beta_1 A-\beta_2 A\sigma_3 dB_3-a\sigma_2 dB_2 dB_3)} < \frac{a}{(a\beta_1 A-\beta_2 A\sigma_3 dB_3-a\sigma_2\sigma_3 dB_2 dB_3)}$$

$$\Rightarrow h^2 - 2h\,\frac{(a\sigma_3 dB_3+a\sigma_2 dB_2+\beta_2 A)}{2(a\beta_1 A-\beta_2 A\sigma_3 dB_3-a\sigma_2 dB_2 dB_3)} + \left(\frac{(a\sigma_3 dB_3+a\sigma_2 dB_2+\beta_2 A)}{2(a\beta_1 A-\beta_2 A\sigma_3 dB_3-a\sigma_2 dB_2 dB_3)}\right)^2 <$$

$$\frac{a}{(a\beta_1 A-\beta_2 A\sigma_3 dB_3-a\sigma_2\sigma_3 dB_2 dB_3)} + \left(\frac{(a\sigma_3 dB_3+a\sigma_2 dB_2+\beta_2 A)}{2(a\beta_1 A-\beta_2 A\sigma_3 dB_3-a\sigma_2 dB_2 dB_3)}\right)^2$$

$$\Rightarrow \left(\frac{(a\sigma_3 dB_3+a\sigma_2 dB_2+\beta_2 A)}{2(a\beta_1 A-\beta_2 A\sigma_3 dB_3-a\sigma_2 dB_2 dB_3)} - h\right)^2 < \left(\frac{(a\sigma_3 dB_3+a\sigma_2 dB_2+\beta_2 A)}{2(a\beta_1 A-\beta_2 A\sigma_3 dB_3-a\sigma_2 dB_2 dB_3)}\right)^2 +$$

$$\frac{a}{(a\beta_1 A-\beta_2 A\sigma_3 dB_3-a\sigma_2\sigma_3 dB_2 dB_3)}$$

where "h" is any step size and always positive.

(ii). $1 - C_1 + C_2 > 0$

$$\Rightarrow 1 - \frac{a+h\beta_2 A+ah\sigma_2 dB_2}{a(1+hb)} - \frac{1+h\sigma_3 dB_3}{(1+hc)} + \frac{(a+h\beta_2 A+ah\sigma_2 dB_2)(1+h\sigma_3 dB_3)-ah^2 A\beta_1}{a(1+hb)(1+hc)} > 0$$

$$\Rightarrow a(1 + hb)(1 + hc) - (1 + hc)(a + h\beta_2 A + ah\sigma_2 dB_2) - a(1 + h\sigma_3 dB_3)(1 + hb) + h + (1 + h\sigma_3 dB_3)(a + h\beta_2 A + ah\sigma_2 dB_2) > 0$$

$$\Rightarrow h^2(abc + \beta_2 A\sigma_3 dB_3 + a\sigma_2\sigma_3 dB_2 dB_3 - cA\beta_2 - ac\sigma_2 dB_2] > 0$$

$$\Rightarrow h^2 > 0$$

$$\Rightarrow h > 0$$

where "h" is any step size and always positive.

(iii). $C_2 < 1$

$$\Rightarrow \frac{(a+h\beta_2 A+ah\sigma_2 dB_2)(1+h\sigma_3 dB_3)}{a(1+hb)(1+hc)} - \frac{ah^2\beta_1 A}{a(1+hb)(1+hc)} < 1$$

$$\Rightarrow (a + h\beta_2 A + ah\sigma_2 dB_2)(1 + h\sigma_3 dB_3) - ah^2\beta_1 A < a(1 + hb)(1 + hc)$$

$$\Rightarrow h^2(abc + a\beta_1 A - \beta_2 A\sigma_2 dB_2 - a\sigma_2\sigma_3\, dB_2 dB_3 + h(ab + ac - \beta_2 A - a\sigma_2\, dB_2 - a\sigma_3\, dB_3) > 0$$

$$\Rightarrow h^2 + 2\frac{h(ab+ac-\beta_2 A-a\sigma_2 dB_2-a\sigma_3\, dB_3)}{2(abc+a\beta_1 A-\beta_2 A\sigma_2 dB_2-a\sigma_2\sigma_3\, dB_2 dB_3)} + \left(\frac{(ab+ac-\beta_2 A-a\sigma_2 dB_2-a\sigma_3\, dB_3)}{2(abc+a\beta_1 A-\beta_2 A\sigma_2 dB_2-a\sigma_2\sigma_3\, dB_2 dB_3)}\right)^2 >$$

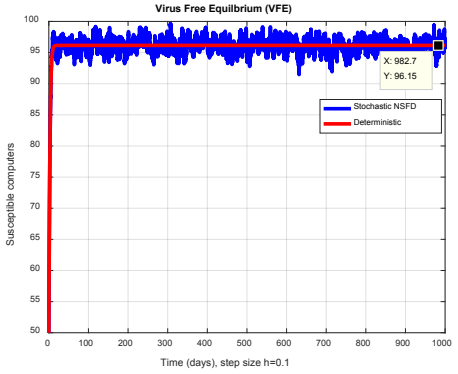
$$+\left(\frac{(ab+ac-\beta_2 A-a\sigma_2 dB_2-a\sigma_3\, dB_3)}{2(abc+a\beta_1 A-\beta_2 A\sigma_2 dB_2-a\sigma_2\sigma_3\, dB_2 dB_3)}\right)^2$$

$$\Rightarrow \left(\frac{(ab+ac-\beta_2 A-a\sigma_2 dB_2-a\sigma_3\, dB_3)}{2(abc+a\beta_1 A-\beta_2 A\sigma_2 dB_2-a\sigma_2\sigma_3\, dB_2 dB_3)} + h\right)^2 > \left(\frac{(ab+ac-\beta_2 A-a\sigma_2 dB_2-a\sigma_3\, dB_3)}{2(abc+a\beta_1 A-\beta_2 A\sigma_2 dB_2-a\sigma_2\sigma_3\, dB_2 dB_3)}\right)^2$$

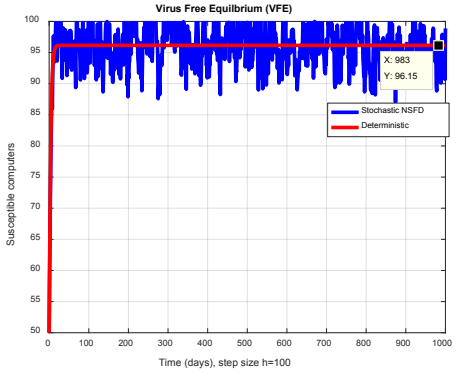
$$\Rightarrow \frac{(ab+ac-\beta_2 A-a\sigma_2 dB_2-a\sigma_3\, dB_3)}{2(abc+a\beta_1 A-\beta_2 A\sigma_2 dB_2-a\sigma_2\sigma_3\, dB_2 dB_3)} + h > \frac{(ab+ac-\beta_2 A-a\sigma_2 dB_2-a\sigma_3\, dB_3)}{2(abc+a\beta_1 A-\beta_2 A\sigma_2 dB_2-a\sigma_2\sigma_3\, dB_2 dB_3)}$$

$$\Rightarrow h > 0.$$

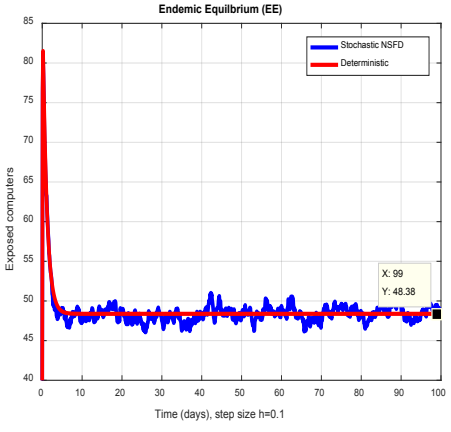
This condition is always valid [Peng, He, Huang et al. (2013)]. So, the suggested framework of stochastic nonstandard finite difference method is locally asymptotical stable (LAS).



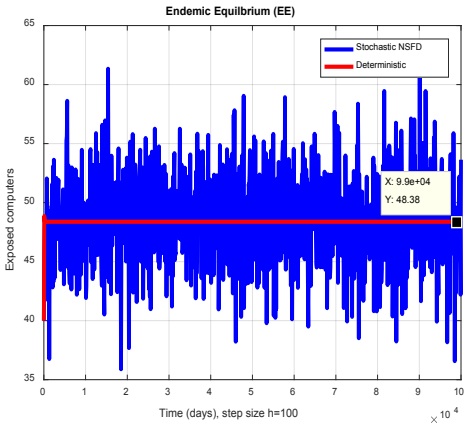
(a)



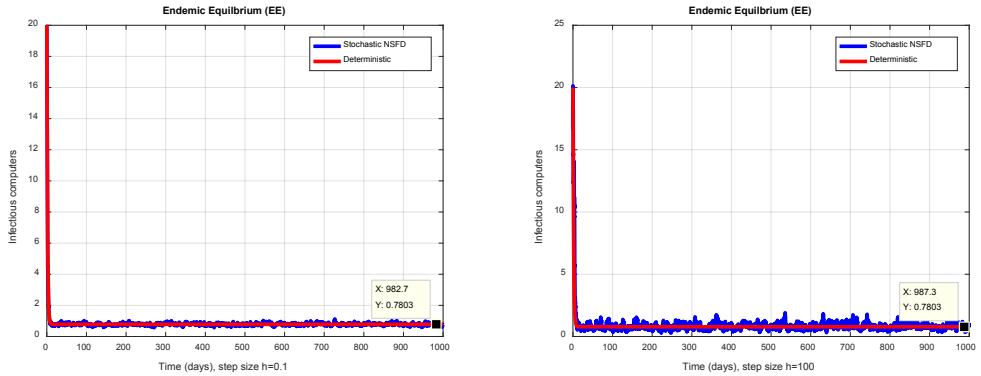
(b)



(c)



(d)



(e) **(f)**

Figure 5: Comparison in solutions of stochastic NSFD and deterministic **(a)** Susceptible computers fraction at VFE Point for h=0.1 **(b)** Susceptible computers fraction at VFE Point for h=100 **(c)** Exposed computers fraction at EE Point for h=0.1 **(d)** Exposed computers fraction at EE Point for h=100 **(e)** Infectious computers fraction at EE Point for h=0.1 **(f)** Infectious computers fraction at EE Point for h=100

6 Outcomes and analysis

The Euler Maruyama scheme meets the factual steady states of the computer virus model whereas Fig. 2, also illustrates that a deterministic outcome is the mean of Euler Maruyama outcome for h=0.01 at different sub-computer fractions respectively. In Fig. 2, if we enlarge the time step size, the Euler Maryuama scheme is unable to keep boundedness and positivity for virus free equilibrium and endemic equilibrium at different sub-computer fractions. Consequently, for any time step size, Euler Maryuama scheme fails to work.

Fig. 3 depicts that the stochastic Euler scheme converges the factual steady states equilibrium whereas the mean of the stochastic Euler solution is the deterministic outcome for discretization h=0.01 at different sub-computer fractions. In Fig. 3, if we enlarge time step size, the stochastic Euler scheme is unable to keep positivity and boundedness for virus free and endemic equilibrium at different sub-computer fractions as well. Ultimately for obtaining the solutions of stochastic computer virus model the stochastic Euler scheme is not a reliable method.

Fig. 4 represents that the stochastic Runge-Kutta scheme converges the virus-free equilibrium and endemic equilibrium whereas the mean of the stochastic Runge-Kutta solution is the deterministic outcome for discretization h=0.01 at different sub-computer fractions respectively. In Fig. 4, if we enlarge the time step size, the stochastic Runge-Kutta scheme is unable to keep boundedness and positivity for virus free equilibrium and also for endemic equilibrium at different sub-computer fractions. Finally, the stochastic Runge-Kutta scheme fails for any time step size. Hence aforesaid stochastic schemes do not support all dynamical properties [Mickens (1994, 2005)].

In Fig. 5, we have concluded that the stochastic NSFD scheme converges both virus free equilibrium and endemic equilibrium whereas the mean of stochastic NSFD solution is the deterministic outcome for any discretization like h=0.1 and h=100 at different sub-

computer fractions respectively. Hence the stochastic NSFD scheme supports all dynamical properties like dynamical consistency, boundedness and positivity characterised by Mickens in a stochastic milieu. The projected framework stochastic NSFD scheme has successfully worked for any time step size.

7 Conclusion and future framework

For comprehending computer virus dynamics incorporating protection against virus, the stochastic epidemic model is a more beneficial approach in contrast to the deterministic epidemic model in terms of numerical analysis. The Euler Maruyama scheme, stochastic Euler scheme and stochastic Runge-Kutta scheme converge right equilibrium points, but for very little time step size. Those above stochastic numerical schemes diverge and lose dynamical properties. However, as we increase the time, these schemes diverge and fail to obey the above-mentioned dynamical properties. The suggested structure of (SNSFD) of computer virus model performs for any time step size defined by Mickens [Mickens (1994, 2005)] in the stochastic framework. This framework (SNSFD) is appropriate for all non-linear and complex stochastic epidemic models. The deterministic ODEs outcomes and the stochastic outcomes are quite close to each other. The stochastic model's study shows a crucial part of virus dynamics. We have detected that stochastic models are more practical rather than deterministic epidemic models. For forthcoming work, we shall extend this stochastic analysis on all types of complicated computer virus models. The proposed (SNSFD) can be executed to the complicated stochastic diffusion and stochastic delay epidemic models. Moreover, in the extension of fractional order dynamical system [Jajarmi and Baleanu (2018); Jajarmi, Baleanu, Bonyah et al. (2018)], the proposed numerical analysis of this work might also be used. We plan to construct an authentic numerical scheme for the fractional order stochastic epidemic model for different viruses.

Acknowledgement: We would like to thank the referees for their valuable comments, and also the authors are grateful to Vice Chancellor, Air vice Marshal Faaiz Amir (Retd.), Air University, Islamabad and Dr Raheel Qamar, Rector COMSATS University, Islamabad, Pakistan for providing excellent research environment and facilities.

Declaration of conflicting interests: We have no competing interest for this article.

References

Albazzaz, J. M. A.; Almuhanna, N. E. (2016). Avoiding computer viruses and malware threats. *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 11, pp. 288-291.

Allen, E. (2007): *Modeling with Ito Stochastic Differential Equations*. Springer Dordrecht, Netherlands.

Allen, E. J.; Allen, L. J. S.; Arciniega, A.; Greenwood, P. E. (2008): Construction of equivalent stochastic differential equation models. *Stochastic Analysis and Applications*, vol. 26, no. 2, pp. 274-297.

Allen, L. J.; Burgin, A. (2000): Comparison of deterministic and stochastic sis and sir

models in discrete time. *Mathematical Biosciences*, vol. 163, no. 1, pp. 1-33.

Anwar, E.; Goldberg, E.; Fraser, A.; Acosta, J.; Paul, M. et al. (2014): Vaccination for preventing typhoid fever disease. *Cochrane Database of Systematic Reviews*, vol. 2, no. 1, pp. 1465-1858.

Baleanu, D.; Jajarmi, A.; Bonyah, E.; Hajipour, M. (2018): New aspects of poor nutrition in the life cycle within the fractional calculus. *Advances in Difference Equations*, vol.18, no. 230, pp. 1684-1698.

Bayram, M.; Partal, T.; Buyukoz, G. O. (2018): Numerical methods for simulation of stochastic differential equations. *Advances in Difference Equations*, vol. 17, no. 5, pp. 1466-1476.

Billings, L.; Spears, W. M.; Schwartz, I. B. (2002): A unified prediction of computer virus spread in connected networks. *Physics Letters A*, vol. 297, no. 3, pp. 261-266.

Brauer, F.; Chavez, C. C. (2001): *Mathematical Models in Population Biology and Epidemiology*. Springer, New York.

Britton, T. (2010): Stochastic epidemic models a survey. *Mathematical Biosciences*, vol. 225, no. 1, pp. 24-35.

Cai, L.; Li, X. Z. (2010): Global analysis of a vector-host epidemic model with nonlinear incidences. *Applied Mathematics and Computation*, vol. 217, no. 7, pp. 3531-3541.

Cohen, F. (1987): Computer viruses. *Computers and Security*, vol. 6, no. 1, pp. 22-35.

Cresson, J.; Pierret, F. (2014): Nonstandard finite difference scheme preserving dynamical properties. *Journal of Computational and Applied mathematics*, vol. 303, no. 1, pp. 15-30.

Cui, J. A.; Tao, X.; Zhu, H. (2008): An sis infection model incorporating media coverage. *Rocky Mountain Journal of Mathematics*, vol. 38, no. 5, pp. 1323-1334.

Fatima, U.; Ali, M.; Ahmed, N.; Rafiq, M. (2018): Numerical modeling of susceptible latent breaking-out quarantine computer virus epidemic dynamics. *Heliyon*, vol. 5, no. 5, pp. 631-652.

Gard, T. C. (1988): *Introduction to Stochastic Differential Equations*. Marcel Dekker, New York.

Han, X.; Tan, Q. (2010): Dynamical behavior of computer virus on Internet. *Applied Mathematics and Computation*, vol. 2, no. 17, pp. 2520-2526.

Holt, J.; Davis, S.; Leirs, H. (2006): A model of leptospirosis infection in an african rodent to determine risk to human seasonal fluctuations and the impact of rodent control. *Acta Tropica*, vol. 99, no. 2, pp. 218-225.

Jajarmi, A.; Baleanu, D. (2018): A new fractional analysis on the interaction of HIV with CD4+T-cells. *Chaos, Solitons & Fractals*, vol. 113, no. 1, pp. 221-229.

Karatzas, I.; Shreve, S. E. (1991): *Brownian Motion and Stochastic Calculus*, 2nd Edition. Springer Verlag, Berlin.

Kloeden, P. E.; Platen, E. (1992): *Numerical Solution of Stochastic Differential Equations*. Springer Verlag, Berlin.

Kloeden, P. E.; Platen, E.; Schurz, H. (1994): *Numerical Solution of SDE Through*

Computer Experiments. Springer Verlag, Berlin.

Maruyama, G. (1955): Continuous Markov processes and stochastic equations. *Rendiconti Del Circolo Matematico Di Palermo*, vol. 4, no. 1, pp. 48-90.

Mickens, R. E. (1994): *Nonstandard Finite Difference Models of Differential Equations*. World Scientific, Singapore.

Mickens, R. E. (2005): A fundamental principle for constructing nonstandard finite difference schemes for differential equations. *Journal of Difference Equations and Applications*, vol. 11, no. 7, pp. 645-653.

Mickens, R. E. (2005): *Advances in Applications of Nonstandard Finite Difference Schemes*. World Scientific, Singapore.

Mishra, B. K.; Jha, N. (2007): Fixed period of temporary immunity after run of anti-malicious software on computer nodes. *Applied Mathematics and Computation*, vol. 190, no. 2, pp. 1207-1212.

Murray, W. H. (1988): The application of epidemiology to computer viruses. *Computers and Security*, vol. 7, no. 2, pp. 139-150.

Noeiaghdam, S.; Suleman, M.; Budak, H. (2018): Solving a modified nonlinear epidemiological model of computer viruses by homotopy analysis method. *Mathematical Sciences*, vol. 12, no. 3, pp. 211-222.

Patil, B. V.; Jadhav, R. J. (2014). Computer virus and antivirus software a brief review. *International Journal of Advances in Management and Economics*, vol. 4, no. 2, pp. 1-4.

Peng, M.; He, X.; Huang, J.; Dong, T. (2013): Modeling computer virus and its dynamics. *Mathematical problems in Engineering*, vol. 1, no. 6, pp. 1-5.

Pierret, F. (2015): A non-standard Euler Maruyama scheme. *Journal of Difference Equations and Applications*, vol. 22, no. 1, pp. 75-98.

Piqueira, J. R. C.; Araujo, V. O. (2009): A modified epidemiological model for computer viruses. *Applied Mathematics and Computation*, vol. 2, no. 13, pp. 355-360.

Piqueira, J. R. C.; Vasconcelos, A. A. D.; Gabriel C. E. C. J.; Araujo, V. O. (2008): Dynamic models for computer viruses. *Computers and Security*, vol. 27, no. 7-8, pp. 355-359.

Platen, E. (1991): An introduction to numerical methods for stochastic differential equations. *Acta Numerica*, vol. 8, no. 1, pp. 197-246.

Raza, A.; Arif, M. S.; Rafiq, M. (2019). A reliable numerical analysis for stochastic dengue epidemic model with incubation period of virus. *Advances in Difference Equations*, vol. 3, no. 2, pp. 1958-1977.

Ren, J.; Yang, X.; Yang, L. X.; Xu, Y.; Yang, F. (2012): A delayed computer virus propagation model and its dynamics. *Chaos Soliton and Fractals*, vol. 45, no. 1, pp. 74-79.

Ren, J.; Yang, X.; Zhu, Q.; Yang, L. X.; Zhang, C. (2012): A novel computer virus model and its dynamics. *Nonlinear Analysis Real World Applications*, vol. 13, no. 1, pp. 376-384.

Shoji, I.; Ozaki, T. (1997): Comparative study of estimation methods for continuous time stochastic processes. *Journal of Time Series Analysis*, vol. 18, no. 5, pp. 485-506.

Shoji, I.; Ozaki, T. (1998): Estimation for nonlinear stochastic differential equations by a local linearization method. *Stochastic Analysis and Applications*, vol. 16, no. 4, pp. 733-752.

Wierman, J. C.; Marchette, D. J. (2004): Modeling computer virus prevalence with a susceptible infected susceptible model with reintroduction. *Computational Statistics and Data Analysis*, vol. 45, no. 1, pp. 3-23.

Yang, L. X.; Yang, X.; Wen, L.; Liu, J. (2012): A novel computer virus propagation model and its dynamics. *International Journal of Computer Mathematics*, vol. 89, no. 17, pp. 2307-2314.

Yang, L. X.; Yang, X.; Zhu, Q.; Wen, L. (2013): A computer virus model with graded cure rates. *Nonlinear Analysis Real World Applications*, vol. 14, no. 1, pp. 414-422.

Yao, Y.; Fu, Q.; Yang, W.; Wang, Y.; Sheng, C. (2018): An epidemic model of computer worms with time delay and variable infection rate. *Security and Communication Networks,* vol. 2, no. 1, pp. 982-993.

Yu, Y.; Hu, J.; Zeng, Y. (2019): On computer virus spreading using node-based model with time-delayed intervention strategies. *Science China Information Sciences*, vol. 62, no. 5, pp. 59201-59203.

Yuan, H.; Chen, G. (2008): Network virus epidemic model with the point to group information propagation. *Applied Mathematics and Computation*, vol. 206, no. 1, pp. 357-367.

Zafar, Z.; Rehan, K.; Mushtaq, M. (2017): Fractional-order scheme for bovine babesiosis disease and tick populations. *Advances in Difference Equations*, vol. 86, no. 1, pp. 1133-1152.

Zafar, Z.; Rehan, K.; Mushtaq, M. (2017): HIV/AIDS epidemic fractional-order model. *Journal of Difference Equations and Applications*, vol. 23, no. 7, pp. 1298-1315.

Zafar, Z.; Rehan, K.; Mushtaq, M.; Rafiq, M. (2017): Numerical treatment for nonlinear brusselator chemical model. *Journal of Difference Equations and Applications*, vol. 23, no. 3, pp. 521-538.

Zhang, C. (2018): Global behavior of a computer virus propagation model on multilayer networks. *Security and Communication Networks*, vol. 1, no. 1, pp. 195-204.

Zhu, Q.; Yang, X.; Ren, J. (2012). Modeling and analysis of the spread of computer virus. *Communication in Nonlinear Science and Numerical Simulation*, vol. 17, no. 12, pp. 5117-5124.