A Stochastic Numerical Analysis for Computer Virus Model with Vertical Transmission Over the Internet

Muhammad Shoaib Arif[1], Ali Raza[1], Wasfi Shatanawi[2, 3, *], Muhammad Rafiq[4] and Mairaj Bibi[5]

Abstract: We are presenting the numerical analysis for stochastic SLBR model of computer virus over the internet in this manuscript. We are going to present the results of stochastic and deterministic computer virus model. Outcomes of the threshold number C^* hold in stochastic computer virus model. If $\mathrm{C}^* < 1$ then in such a condition virus controlled in the computer population while $\mathrm{C}^* > 1$ shows virus spread in the computer population. Unfortunately, stochastic numerical techniques 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, bounded-ness and positivity as well-defined by Mickens. On this basis, we can suggest a collection of plans for eradicating viruses spreading across the internet effectively.

Keywords: Computer virus model, stochastic modelling, stochastic techniques, stability.

1 Literature survey

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 practise 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 virus, which was discovered in 2008, had infected millions of

[1] Department of Mathematics, Stochastic Analysis & Optimization Research Group, Air University, PAF Complex E-9, Islamabad, 44000, Pakistan.

[2] Department of Mathematics and General Courses Prince Sultan University Riyadh, Saudi Arabia.

[3] Department of Medical Research, China Medical University Hospital, China Medical University, Taichung, 40402, Taiwan.

[4] Faculty of Engineering, University of Central Punjab, Lahore, 54500, Pakistan.

[5] Department of Mathematics, Comsats University, Chak Shahzad Campus, Islamabad, 44000, Pakistan.

[*] Corresponding Author: Wasfi Shatanawi. Email: wshatanawi@psu.edu.sa.

CMC. doi: 10.32604/cmc.2019.08405

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. Next sub-routine, namely do-damage also called the virus payload, 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 risky viruses was proposed by Cohen et al. [Cohen (1987); Murray (1988)].

In 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 infected 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 the 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)]. 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 warm virus's 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 behaviour 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 a computer virus, namely SLBRS model. It describes the vulnerability of uninfected computers and how they can get infected from the internet. We suppose that computers which join the internet are categorized into four classes. A threshold factor $\mathtt{C}^*$ is used to determine the dynamic characteristics of the suggested model.

Mathematical modelling has become very advanced to understand the viruses thoroughly. Formation of models and simulation allows us to analyze the sensitivity and make a comparison of conclusive opinions originating out of examples. Lots of studies are present on computer virus transmission dynamics models. Nonlinear initial value problems (IVPs) do not always, provide analytical solutions to specific issues and classical explicit finite-difference schemes such as Runge-Kutta, and Euler methods can bring confusion and unexpected fluctuations for discretization parameters [Mickens (1994, 2005]. Many types of research have been done on various computer virus models [Cai and Li (2010); Peng, He, Huang et al. (2013)]. 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)]. The usual quantitative explicit techniques for ODEs never maintain dynamical possessions as we have seen in the deterministic modelling. We have also seen that in explicit stochastic techniques do not maintain the dynamical possessions in the stochastic case. So, from this a question arises and need to research more: Could we develop the random emphatical scheme which maintains all the dynamical possessions? A rule introduced in the deterministic case, which has been used to start the notion stochastic nonstandard finite difference technique (SNSFD). These regulations were given by Mickens. This is the primary point of this paper.

This paper is divided into the following sections:

In Section 2, we have explained the deterministic computer model and its equilibria. Next section is about the formulation of the stochastic computer model. Section 4 explains the stochastic numerical techniques for stochastic computer virus model and their convergence analysis. Section 5 deals with the comparison of deterministic and stochastic numerical outcomes. Finally, in the last section, we shall present our deduction and give the future work.

2 Deterministic computer virus model

Here, we observe the deterministic computer virus model presented by Yang et al. [Yang, Zhang, Li et al. (2012)]. Consider at any non-specific time t, the defined variables are S (exemplifies uninfected computers' fraction), L (exemplifies infected computers' fraction in latency), B (exemplifies infected computers' fraction which is broke-out) and R (exemplifies recovered computers' fraction with short-term immunity). The communication dynamics of computer virus model is illustrated below.

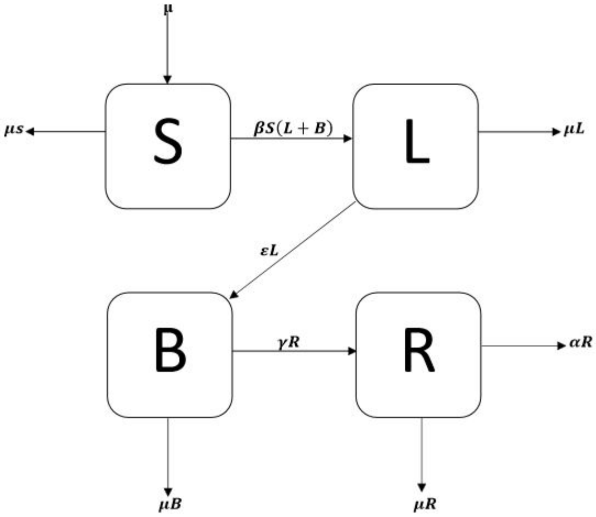


Figure 1: Flow map of computer virus model

The variables of the model are illustrated as μ (depicts the connected and withdrawn computer rate from the internet), β (pronounces the bilinear incidence rate of virus-free computers with infected computers), ε (pronounces the latent computers break out rate), r (pronounces the breaking out computers recovery rate) and α (pronounces the recovered computer rate that become virus-free).

The governing equations of the computer virus model as follows:

$$\left.\begin{aligned}\frac{dS}{dt} &= \mu - \beta S(L+B) + \alpha R - \mu S\\ \frac{dL}{dt} &= \beta S(L+B) - \varepsilon L + \mu L\\ \frac{dB}{dt} &= \varepsilon L - \gamma B - \mu B\\ \frac{dR}{dt} &= \gamma B - \alpha B - \mu R\end{aligned}\right\} \tag{1}$$

$$S + L + B + R \leq 1 \tag{2}$$

with conditions $S \geq 0, L \geq 0, B \geq 0, R \geq 0$

The reduced form of computer virus model is

$$\left.\begin{aligned} \frac{dS}{dt} &= \mu(1-S) - \beta S(L+B) + \alpha(1-S-L-B) \\ \frac{dL}{dt} &= \beta S(L+B) - (\varepsilon+\mu)L \\ \frac{dB}{dt} &= \varepsilon L - (\gamma+\mu)B \end{aligned}\right\} \qquad (3)$$

with conditions $S \geq 0, L \geq 0, B \geq 0$ and $S + L + B \leq 1$.

2.1 Equilibria of the computer virus model

Given below are two ways of equilibrium points of computer virus model (3) as:

Virus-free equilibrium is $V_1 = (S, L, B) = (1,0,,0)$

Virus existence equilibrium is

$E_1 = (S^o, L^o, B^o) =$

$$\left(\frac{(\gamma+\mu)(\mu+\varepsilon)}{\beta(\mu+\gamma+\varepsilon)}, \frac{(\gamma+\mu)(\mu+\alpha)\beta(\mu+\gamma+\varepsilon)-(\gamma+\mu)(\gamma+\mu)(\mu+\varepsilon)(\mu+\alpha)}{\beta(\mu+\gamma+\varepsilon)(\alpha+\mu+\varepsilon)(\gamma+\mu)+\alpha\varepsilon}, \frac{\varepsilon}{(1-\gamma-\mu)}\left[\frac{(\gamma+\mu)(\mu+\alpha)\beta(\mu+\gamma+\varepsilon)-(\gamma+\mu)(\gamma+\mu)(\mu+\varepsilon)(\mu+\alpha)}{\beta(\mu+\gamma+\varepsilon)(\alpha+\mu+\varepsilon)(\gamma+\mu)+\alpha\varepsilon}\right]\right)$$

$C^* = \frac{\beta(\mu+\gamma+\varepsilon)}{(\mu+\varepsilon)(\mu+\gamma)}$, C^* is the computer virus transmission generation number of model (3). It has an important part in virus dynamics.

3 Stochastic computer virus model

Let $C(t) = [S, L, B]^T$ formulates the SDEs of computer virus model (3). We will determine 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 as follows (see Tab. 1).

Table 1: Changes that may occur in the computer virus model

T_i=Transition	P_i= Probabilities
$(\Delta C)_1 = [1 \quad 0 \quad 0]^T$	$P_1 = \mu(1-S)\Delta t$
$(\Delta C)_2 = [-1 \quad 1 \quad 0]^T$	$P_2 = \beta S(L+B)\Delta t$
$(\Delta C)_3 = [1 \quad 0 \quad 0]^T$	$P_3 = \alpha(1-S-L-B)\Delta t$
$(\Delta C)_4 = [0 \quad -1 \quad 1]^T$	$P_4 = \varepsilon L\, \Delta t$
$(\Delta C)_5 = [0 \quad -1 \quad 0]^T$	$P_5 = \mu L\, \Delta t$
$(\Delta C)_6 = [0 \quad 0 \quad -1]^T$	$P_6 = (\gamma+\mu)B\Delta t$

Following is the expectation of computer virus model (3):

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

$$.\text{Expectation} = E^*[\Delta C] = \begin{bmatrix} \mu(1-S) - \beta S(L+B) + \alpha(1-S-L-B) \\ \beta S(L+B) - (\varepsilon+\mu)L \\ \varepsilon L - (\gamma+\mu)B \end{bmatrix} \Delta t$$

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

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

where

$\mathrm{W}_{11} = \mu(1 - \mathrm{S}) + \beta\mathrm{S}(\mathrm{L} + \mathrm{B}) + \alpha(1 - \mathrm{S} - \mathrm{L} - \mathrm{B}), \mathrm{W}_{12} = -\beta\mathrm{S}(\mathrm{L} + \mathrm{B}), \mathrm{W}_{13} = 0$, $\mathrm{W}_{21} = -\beta\mathrm{S}(\mathrm{L} + \mathrm{B}), \mathrm{W}_{22} = \beta\mathrm{S}(\mathrm{L} + \mathrm{B}) + (\varepsilon + \mu)\mathrm{L}, \mathrm{W}_{23} = -\varepsilon\mathrm{L}$, $.\, \mathrm{W}_{31} = 0, \mathrm{W}_{32} = -\varepsilon\mathrm{L}, \mathrm{W}_{33} = \varepsilon\mathrm{L} + (\gamma + \mu)\mathrm{B}$.

The SDE satisfy the diffusion processes, therefore,

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

where, $(\mathrm{C}, \mathrm{t}) = \frac{\mathrm{E}^*[\Delta \mathrm{C}]}{\Delta \mathrm{t}}$ and $\mathrm{H}(\mathrm{C}, \mathrm{t}) = \sqrt{\frac{\mathrm{E}^*[\Delta \mathrm{C}\, \Delta \mathrm{C}^{\mathrm{T}}]}{\Delta \mathrm{t}}}$, then the SDE of computer virus model (3) is

$$\mathrm{dC} = \quad (\mathrm{C}, \mathrm{t})\mathrm{dt} + \mathrm{H}(\mathrm{C}, \mathrm{t})\mathrm{dB}. \tag{4}$$

Here, we have $\mathrm{C}(0) = \mathrm{C}_{\mathrm{o}} = [0.2, 0.7, 0.1]^{\mathrm{T}}$, $0 \leq \mathrm{t} \leq \mathrm{C}$ as initial conditions and B as Brownian motion.

3.1 Euler maruyama technique

We used the parameters given by Yang et al. [Yang, Zhang, Li et al. (2012)] and euler maruyama technique presented in Maruyama [Maruyama (1955)], to analyze the numerical outcome of SDE (4).

The euler maruyama technique of (4) as:

$$\mathrm{C}_{\mathrm{n}+1} = \mathrm{C}_{\mathrm{n}} + \mathrm{f}(\mathrm{C}_{\mathrm{n}}, \mathrm{t})\Delta \mathrm{t} + \mathrm{L}(\mathrm{C}_{\mathrm{n}}, \mathrm{t})\Delta \mathrm{B}_{\mathrm{n}}. \tag{5}$$

where $\Delta \mathrm{t}$ and $\Delta \mathrm{B}_{\mathrm{n}}$ is normally distributed between stochastic drift and stochastic diffusion, i.e., $\Delta \mathrm{B}_{\mathrm{n}} \sim \mathrm{N}(0, 1)$. The confidence interval holds the solution to stochastic differential equations for both equilibria as presented in the above numerical investigations. The outcome of deterministic computer virus model for the virus-free symmetry $\mathrm{V}_1{}^* = (1{,}0{,}0)$ and $\mathrm{C}^* = 0.0300 < 1$ may control the virus in the computer population through the internet. The viral equilibrium $\mathrm{E}_1{}^* = (0.4353, 0.5625, 0.001607)$ and $\mathrm{C}^* = 2.2974 > 1$ shows that the virus rapidly infects to the computer population through the internet.

4 Parametric perturbation of stochastic computer virus model

In this technique, we shall choose parameters from the system (3) and change into the random parameters with small noise as $\beta\mathrm{dt} = \beta\mathrm{dt} + \sigma\mathrm{dB}$. So, the stochastic system (3) is as follows [Allen, Allen, Arciniega et al. (2008)].

$$\left.\begin{aligned} &\mathrm{dS} = [\mu(1 - \mathrm{S}) - \beta\mathrm{S}(\mathrm{L} + \mathrm{B}) + \alpha(1 - \mathrm{S} - \mathrm{L} - \mathrm{B})]\mathrm{dt} - \sigma\mathrm{S}(\mathrm{L} + \mathrm{B})\mathrm{dB} \\ &\mathrm{dL} = [\beta\mathrm{S}(\mathrm{L} + \mathrm{B}) - (\mathcal{E} + \mu)\mathrm{L}]\mathrm{dt} + \sigma\mathrm{S}(\mathrm{L} + \mathrm{B})\mathrm{dB} \\ &\mathrm{dB} = [\mathcal{E}\mathrm{L}(\mathrm{t}) - (\gamma + \mu)\mathrm{B}]\mathrm{dt} \end{aligned}\right\} \tag{6}$$

with initial conditions $\mathrm{C}(0) = [\mathrm{S}(0), \mathrm{L}(0), \mathrm{B}(0)]^{\mathrm{T}} = [0.2, 0.7, 0.1]^{\mathrm{T}}$ where σ is casualness of each compartment of the computer virus model.

4.1 Equilibria of stochastic computer virus model

Two equilibria of the stochastic computer virus model (6) are as follows:
Virus-free equilibrium = (VFE) = $(S, L, B) = (1,0,0)$.
Virus existence equilibrium= (VEE)= (S^o, L^o, B^o)
where,

$$S^o = \frac{(\gamma+\mu)(\mu+\varepsilon)}{\beta(\mu+\gamma+\varepsilon)},\ L^o = \frac{(\gamma+\mu)(\mu+\alpha)\beta(\mu+\gamma+\varepsilon)-(\gamma+\mu)(\gamma+\mu)(\mu+\varepsilon)(\mu+\alpha)}{\beta(\mu+\gamma+\varepsilon)(\alpha+\mu+\varepsilon)(\gamma+\mu)+\alpha\varepsilon},$$

$$B^o = \frac{\varepsilon}{(1-\gamma-\mu)}\left[\frac{(\gamma+\mu)(\mu+\alpha)\beta(\mu+\gamma+\varepsilon)-(\gamma+\mu)(\gamma+\mu)(\mu+\varepsilon)(\mu+\alpha)}{\beta(\mu+\gamma+\varepsilon)(\alpha+\mu+\varepsilon)(\gamma+\mu)+\alpha\varepsilon}\right]$$

4.2 Stochastic euler technique

The designed form of the model (6) as presented in Raza et al. [Raza, Arif and Rafiq (2019)]:

$$\left.\begin{aligned}
S^{n+1} &= S^n + h[\mu(1-S^n) - \beta S^n(L^n+B^n) + \alpha(1-S^n-L^n-B^n) - \sigma S^n(L^n+B^n)\Delta B_n] \\
L^{n+1} &= L^n + h[\beta S^n(L^n+B^n) - (\mathcal{E}+\mu)L^n + \sigma S^n(L^n+B^n)\Delta B_n] \\
B^{n+1} &= B^n + h[\mathcal{E}L^n - (\gamma+\mu)B^n]
\end{aligned}\right\} \tag{7}$$

where "h" is represented as the discretized parameter of the method and i.e., $\Delta B_n \sim N(0,1)$.

4.3 Stochastic runge-kutta technique

The designed form of the model (6) as presented in Raza et al. [Raza, Arif and Rafiq (2019)]:
First Stage

$$A_1 = h[\mu(1-S^n) - \beta S^n(L^n+B^n) + \alpha(1-S^n-L^n-B^n) - \sigma S^n(L^n+B^n)\Delta B_n]$$

$$B_1 = h[\beta S^n(L^n+B^n) - (\mathcal{E}+\mu)L^n + \sigma S^n(L^n+B^n)\Delta B_n]$$

$$C_1 = h[\mathcal{E}L^n - (\gamma+\mu)B^n]$$

Second Stage

$$A_2 = h[\mu\Big(1-(S^n+\frac{A_1}{2}\Big) - \beta\Big(S^n+\frac{A_1}{2}\Big)\Big(\Big(L^n+\frac{B_1}{2}\Big)+\Big(B^n+\frac{C_1}{2}\Big)\Big) + \alpha\Big(1-(S^n+\frac{A_1}{2}) - (L^n+\frac{B_1}{2}) - (B^n+\frac{C_1}{2})\Big) - \sigma(S^n+\frac{A_1}{2})\Big(\Big(L^n+\frac{B_1}{2}\Big)+\Big(B^n+\frac{C_1}{2}\Big)\Big)\Delta B_n]$$

$$B_2 = h\Big[\beta(S^n+\frac{A_1}{2})\Big((L^n+\frac{B_1}{2})+(B^n+\frac{C_1}{2})\Big) - (\mathcal{E}+\mu)(L^n+\frac{B_1}{2}) + \sigma(S^n+\frac{A_1}{2})\Big((L^n+\frac{B_1}{2})+(B^n+\frac{C_1}{2})\Big)\Delta B_n\Big]$$

$$C_2 = h\Big[\mathcal{E}(L^n+\frac{B_1}{2}) - \Big(\gamma+\mu)(B^n+\frac{C_1}{2})\Big)\Big]$$

Third Stage

$$A_3 = h[\mu\Big(1-(S^n+\frac{A_2}{2}\Big) - \beta\Big(S^n+\frac{A_2}{2}\Big)\Big(\Big(L^n+\frac{B_2}{2}\Big)+\Big(B^n+\frac{C_2}{2}\Big)\Big) + \alpha\Big(1-(S^n+\frac{A_2}{2}) - (L^n+\frac{B_2}{2}) - (B^n+\frac{C_2}{2})\Big) - \sigma(S^n+\frac{A_2}{2})\Big(\Big(L^n+\frac{B_2}{2}\Big)+\Big(B^n+\frac{C_2}{2}\Big)\Big)\Delta B_n]$$

$$B_3 = h\Big[\beta(S^n + \tfrac{A_2}{2})\Big((L^n + \tfrac{B_2}{2}) + (B^n + \tfrac{C_2}{2})\Big) - (\mathcal{E} + \mu)(L^n + \tfrac{B_2}{2}) + \sigma(S^n + \tfrac{A_2}{2})\Big((L^n + \tfrac{B_2}{2}) + (B^n + \tfrac{C_2}{2})\Big)\Delta B_n\Big]$$

$$C_3 = h\Big[\mathcal{E}(L^n + \tfrac{B_2}{2}) - \Big(\gamma + \mu)(B^n + \tfrac{C_2}{2})\Big)\Big]$$

Fourth Stage

$$A_4 = h[\mu\Big(1 - (S^n + \tfrac{A_3}{2}\Big) - \beta\Big(S^n + \tfrac{A_3}{2}\Big)\Big(\Big(L^n + \tfrac{B_3}{2}\Big) + \Big(B^n + \tfrac{C_3}{2}\Big)\Big) + \alpha\Big(1 - (S^n + \tfrac{A_3}{2}) - (L^n + \tfrac{B_3}{2}) - (B^n + \tfrac{C_3}{2})\Big) - \sigma(S^n + \tfrac{A_3}{2})\Big(\Big(L^n + \tfrac{B_3}{2}\Big) + \Big(B^n + \tfrac{C_3}{2}\Big)\Big)\Delta B_n]$$

$$B_4 = h\Big[\beta(S^n + \tfrac{A_3}{2})\Big((L^n + \tfrac{B_3}{2}) + (B^n + \tfrac{C_3}{2})\Big) - (\mathcal{E} + \mu)(L^n + \tfrac{B_3}{2}) + \sigma(S^n + \tfrac{A_3}{2})\Big((L^n + \tfrac{B_3}{2}) + (B^n + \tfrac{C_3}{2})\Big)\Delta B_n\Big]$$

$$C_4 = h\Big[\mathcal{E}\Big(L^n + \tfrac{B_3}{2}\Big) - \Big(\gamma + \mu)(B^n + \tfrac{C_3}{2})\Big)\Big]$$

Final Stage

$$\left.\begin{aligned} S^{n+1} &= S^n + \frac{1}{6}[A_1 + 2A_2 + 2A_3 + A_4] \\ L^{n+1} &= L^n + \frac{1}{6}[B_1 + 2B_2 + 2B_3 + B_4] \\ B^{n+1} &= B^n + \frac{1}{6}[C_1 + 2C_2 + 2C_3 + C_4] \end{aligned}\right\} \qquad (8)$$

where “h” is represented as the discretized parameter of the method and i.e., $\Delta B_n \sim N(0,1)$.

4.4 Stochastic NSFD technique

The recommended frameworks of SNSFD for the model (6) as presented in Raza et al. [Raza, Arif and Rafiq (2019)]:

$$\left.\begin{aligned} S^{n+1} &= \frac{S^n + h[\mu + \alpha(1 - L^n - B^n)]}{1 + h[(\alpha + \mu) + \beta(L^n + B^n) + \sigma\Delta B_n(L^n + B^n)]} \\ L^{n+1} &= \frac{L^n + hS^n[\beta(L^n + B^n) + \sigma\Delta B_n(L^n + B^n)]}{1 + h(\mathcal{E} + \mu)} \\ B^{n+1} &= \frac{B^n + h\mathcal{E}L^n}{1 + h(\gamma + \mu)} \end{aligned}\right\} \qquad (9)$$

where “h” is represented as the discretized parameter of the method and i.e., $\Delta B_n \sim N(0,1)$.

4.4.1 Convergence analysis

Here we are to discuss the following theorems:

Theorem 1

For any given initial value (S^n (0), L^n (0), B^n (0)) $\in R^3_+$ system (9) has a unique non-negative solution (S^n, L^n, B^n) $\in R^3_+$ on n ≥ 0, almost surely.

Theorem 2

For all $n \geq 0$ is a non-negative invariant set for the system (9).

Proof: Rewriting the system (9) as follows:

$$\frac{S^{n+1}-S^{n}}{h}=[\mu(1-S^{n})-\beta S^{n}(L^{n}+B^{n})+\alpha(1-S^{n}-L^{n}-B^{n})-\sigma S^{n}(L^{n}+B^{n})\Delta B_{n}]$$

$$\frac{L^{n+1}-L^{n}}{h}=[\beta S^{n}(L^{n}+B^{n})-(\mathcal{E}+\mu)L^{n}+\sigma S^{n}(L^{n}+B^{n})\Delta B_{n}]$$

$$\frac{B^{n+1}-B^{n}}{h}=[\mathcal{E}L^{n}-(\gamma+\mu)B^{n}]$$

Adding the corresponding sides, we have

$$\frac{(S^{n+1}+L^{n+1}+B^{n+1})-(S^{n}+L^{n}+B^{n})}{h}=\mu-\mu(S^{n}+L^{n}+B^{n})$$

$$(S^{n+1}+L^{n+1}+B^{n+1})-(S^{n}+L^{n}+B^{n})=h\mu-h\mu(S^{n}+I^{n}+Z^{n})$$

$$(S^{n+1}+L^{n+1}+B^{n+1})\leq 1$$

almost surely.

Theorem 3

The discrete dynamical system (9) has the same equilibria as that of the continuous dynamical system (6) for all $n \geq 0$.

Proof: For solving the system (9), we get two states as follows:

VFE i.e., $V_3=(S^{n},L^{n},B^{n})=(1,0,0)$.

VPE i.e., $E_3=(S^{n},L^{n},B^{n})$.

where,

$$S^{n}=\frac{(\gamma+\mu)(\mu+\varepsilon)}{\beta(\mu+\gamma+\varepsilon)},\ L^{n}=\frac{(\gamma+\mu)(\mu+\alpha)\beta(\mu+\gamma+\varepsilon)-(\gamma+\mu)(\gamma+\mu)(\mu+\varepsilon)(\mu+\alpha)}{\beta(\mu+\gamma+\varepsilon)(\alpha+\mu+\varepsilon)(\gamma+\mu)+\alpha\varepsilon},$$

$$B^{n}=\frac{\varepsilon}{(1-\gamma-\mu)}\left[\frac{(\gamma+\mu)(\mu+\alpha)\beta(\mu+\gamma+\varepsilon)-(\gamma+\mu)(\gamma+\mu)(\mu+\varepsilon)(\mu+\alpha)}{\beta(\mu+\gamma+\varepsilon)(\alpha+\mu+\varepsilon)(\gamma+\mu)+\alpha\varepsilon}\right]$$

almost surely.

Theorem 4

The eigenvalues of the discrete dynamical system (9) lie in the unit circle for all $n \geq 0$.

Proof:

We consider F, G, and H from the system (9) as follows:

$$F=\frac{S+h\mu+h\alpha-h\alpha L-h\alpha B}{1+h\beta L+h\beta B+h\alpha+h\mu+h\sigma L\Delta B_{n}+h\sigma B\Delta B_{n}}$$

$$=\frac{L+hS\beta L+hS\beta B+hS\sigma L\Delta B_{n}+hS\sigma B\Delta B_{n}}{1+h(\varepsilon+\mu)}$$

$$H=\frac{\beta+h\varepsilon L}{1+h(\gamma+\mu)}$$

$$\frac{\partial F}{\partial S}=\frac{1}{1+h\beta(L+B)+h(\alpha+\mu)+h\sigma(L+B)\Delta B_{n}},$$

$$\frac{\partial F}{\partial L}=\frac{-h\alpha(1+h\beta L+h\beta B+h\alpha+h\mu+h\sigma L\Delta B_{n}+h\sigma B\Delta B_{n})-h\beta-h\sigma\Delta B_{n}(S+h\mu+h\alpha-h\alpha L-h\alpha B)}{(1+h\beta L+h\beta B+h\alpha+h\mu+h\sigma L\Delta B_{n}+h\sigma B\Delta B_{n})^{2}}$$

$$\frac{\partial F}{\partial B}=\frac{-h\alpha B(1+h\beta L+h\beta B+h\alpha+h\mu+h\sigma L\Delta B_{n}+h\sigma B\Delta B_{n})-h\beta-h\sigma\Delta B_{n}(S+h\mu+h\alpha-h\alpha L-h\alpha B)}{(1+h\beta L+h\beta B+h\alpha+h\mu+h\sigma L\Delta B_{n}+h\sigma B\Delta B_{n})^{2}}$$

$$\frac{\partial G}{\partial S}=\frac{h\beta L+h\beta B+h\sigma L\Delta B_{n}+h\sigma B\Delta B_{n}}{1+h(\varepsilon+\mu)}$$

$$\frac{\partial G}{\partial L}=\frac{1+hS\beta+hS\beta B+hS\sigma\Delta B_n}{1+h(\varepsilon+\mu)}$$

$$\frac{\partial G}{\partial B}=\frac{hS\beta+hS\sigma\Delta B_n}{1+h(\varepsilon+\mu)}$$

$$\frac{\partial H}{\partial S}=0$$

$$\frac{\partial H}{\partial L}=\frac{h\varepsilon}{1+h(\gamma+\mu)}$$

$$\frac{\partial H}{\partial B}=\frac{1}{1+h(\gamma+\mu)}$$

Now we want to linearize the model about the equilibria of the model for virus-free equilibrium $V_1=(S,L,B)=(1,0,0)$ and $C^*<1$.

The given Jacobean is

$$J=\begin{bmatrix}\frac{\partial F}{\partial S} & \frac{\partial F}{\partial L} & \frac{\partial F}{\partial B}\\ \frac{\partial G}{\partial S} & \frac{\partial G}{\partial L} & \frac{\partial G}{\partial B}\\ \frac{\partial H}{\partial S} & \frac{\partial H}{\partial L} & \frac{\partial H}{\partial B}\end{bmatrix}$$

$$J(1,0,0)=$$

$$\begin{bmatrix}\frac{1}{1+h\alpha+h\mu} & \frac{-h\alpha(+h\alpha+h\mu)-h\beta-h\sigma\Delta B_n(1+h\mu+h\alpha)}{(1+h\alpha+h\mu)^2} & \frac{-h\alpha B(1+h\alpha+h\mu)-h\beta-h\sigma\Delta B_n(1+h\mu+h\alpha)}{(1+h\alpha+h\mu)^2}\\ 0 & \frac{1+h\beta+h\sigma\Delta B_n}{1+h(\varepsilon+\mu)} & \frac{h\beta+h\sigma\Delta B_n}{1+h(\varepsilon+\mu)}\\ 0 & \frac{h\varepsilon}{1+h(\gamma+\mu)} & \frac{1}{1+h(\gamma+\mu)}\end{bmatrix}$$

The eigenvalues are

$$\lambda_1=\frac{1}{1+h\alpha+h\mu}<1,\ \lambda_2=\frac{1+h\beta+h\sigma\Delta B_n}{1+h(\varepsilon+\mu)}<1 \text{ when } C^*<1.$$

$$\lambda_3=\frac{1}{1+h(\gamma+\mu)}<1$$

This is guaranteed to the fact that all eigenvalues of the Jacobean lie in the unit circle. So, the system (9) is LAS around V_1.

4.5 Numerical trials

By using the values of parameters given in Yang et al. [Yang, Zhang, Li et al. (2012)], the numerical simulation is:

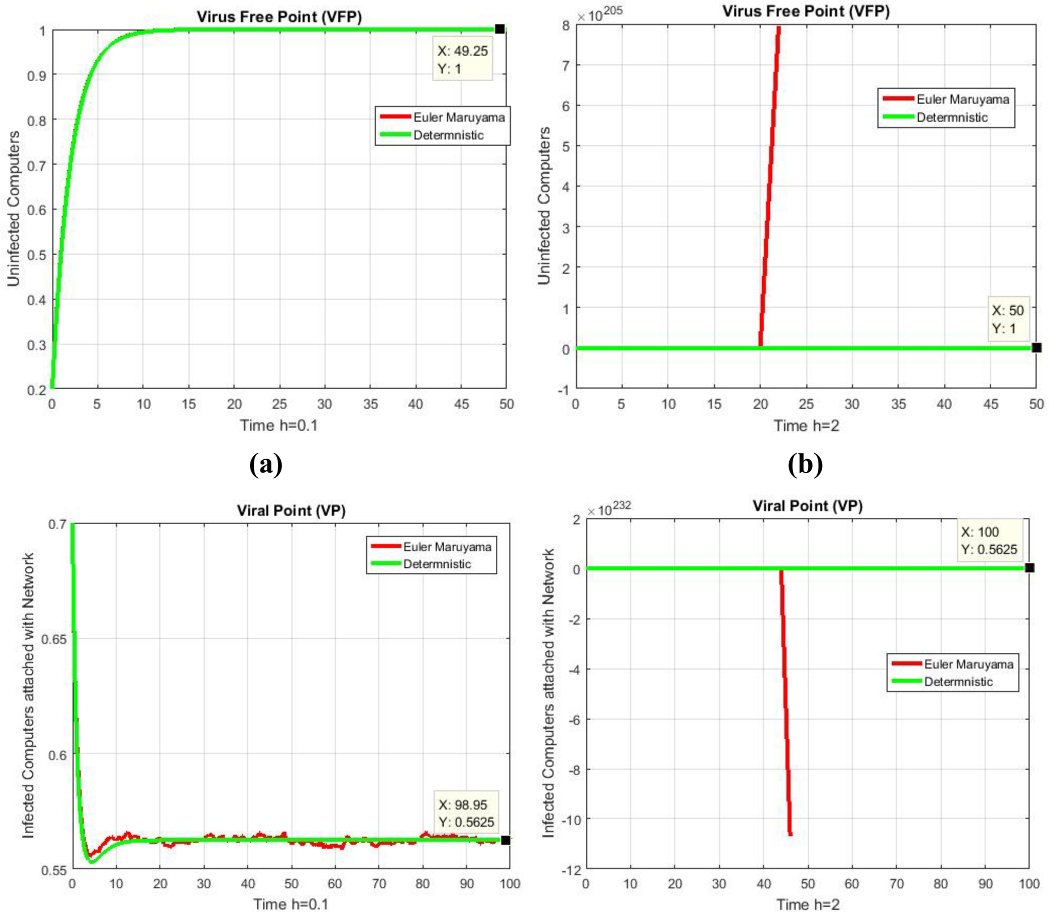
Table 2: Parameter values

	Values	
Parameters	**VFE**	**EE**
Α	0.01	0.01
Β	0.015	1.15
Γ	0.2	0.2
Ε	0.002	0.002

M	0.5	0.5
σ	0.05	Estimated

4.5.1 Euler maruyama technique

The simulation for the system (5) is as follows:



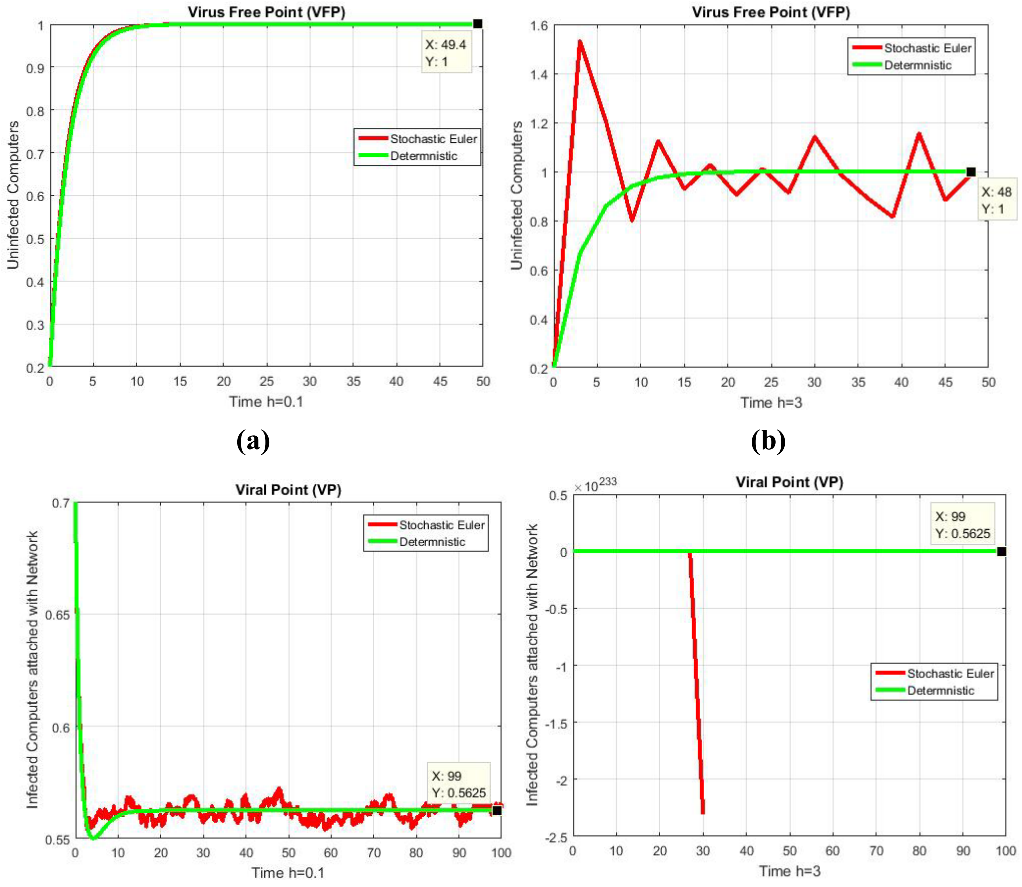
(a) **(b)**

(c) **(d)**

Figure 2: (a) Uninfected computers fraction for VFP at h=0.1 **(b)** Uninfected computers fraction for VFP at h=2 **(c)** Infected computers attached with network fraction for VP at h=0.1 **(d)** Infected computers attached with network fraction for VP at h=2

4.5.2 Stochastic euler technique

We pretend the solutions of the model (7) by utilizing Matlab database and parameters values assumed in Yang et al. [Yang, Zhang, Li et al. (2012)] (see Tab. 2)



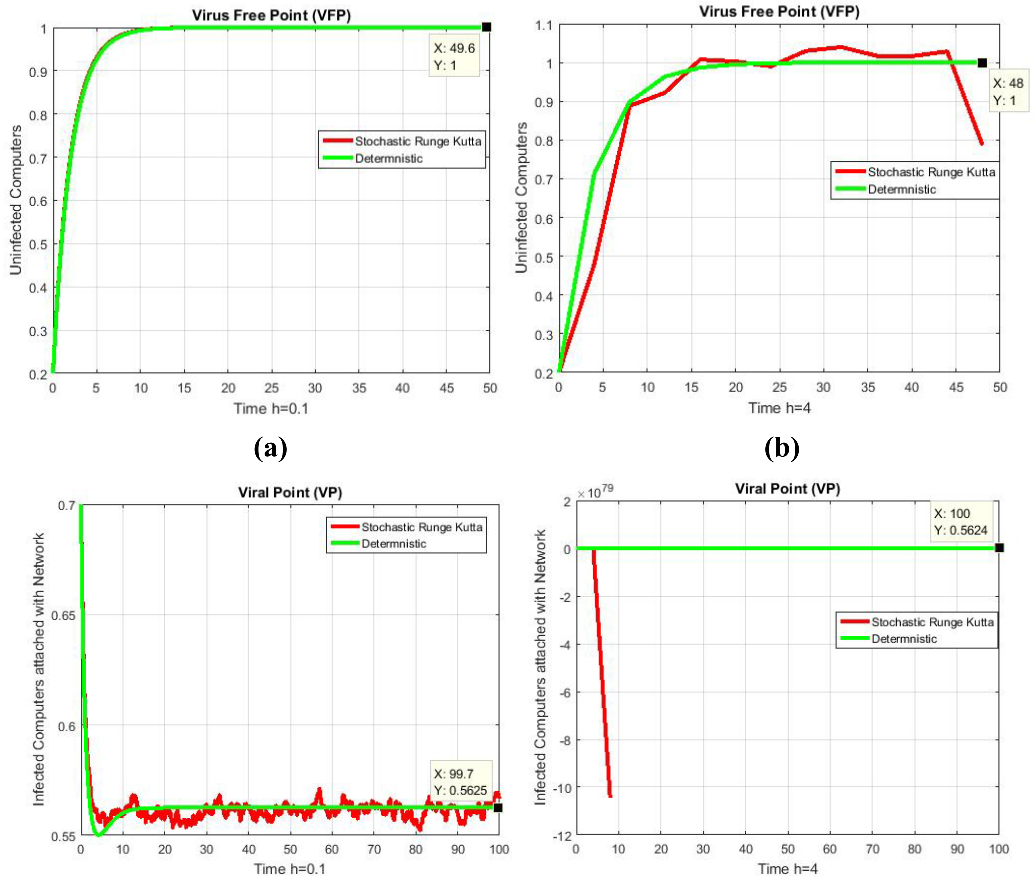
(a) **(b)**

(c) **(d)**

Figure 3: (a) Uninfected computers fraction for VFP at h=0.1 **(b)** Uninfected computers fraction for VFP at h=3 **(c)** Infected computers attached with network fraction for VP at h=0.1 **(f)** Infected computers attached with network fraction for VP at h=3

4.5.3 Stochastic runge kutta technique

We pretend the solutions of the model (8) by utilizing Matlab database and parameters values assumed in Yang et al. [Yang, Zhang, Li et al. (2012)] (see Tab. 2)



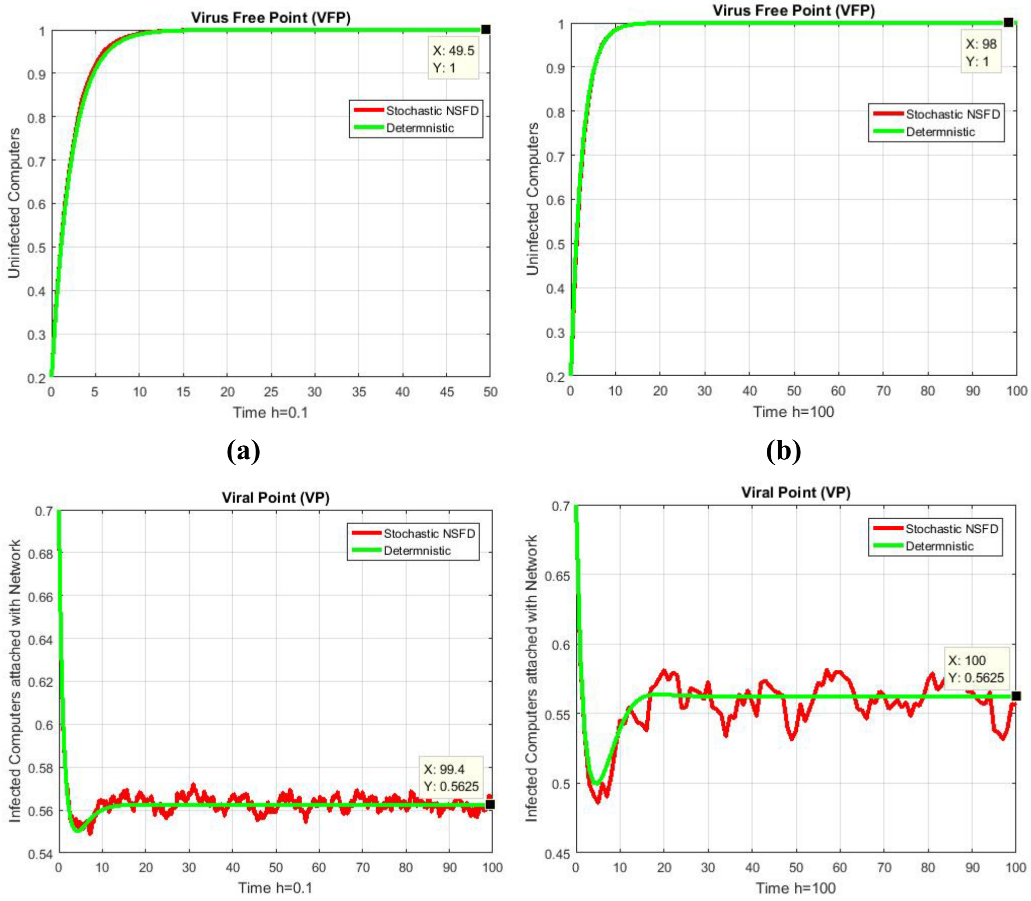
(a) **(b)**

(c) **(d)**

Figure 4: (a) Uninfected computers fraction for VFP at h=0.1 **(b)** Uninfected computers fraction for VFP at h=4 **(c)** Infected computers attached with network fraction for VP at h=0.1 **(d)** Infected computers attached with network fraction for VP at h=4

4.5.4 Stochastic NSFD technique

We pretend the solutions of the model (9) by utilizing Matlab database and parameters values assumed in Yang et al. [Yang, Zhang, Li et al. (2012)] (see Tab. 2)



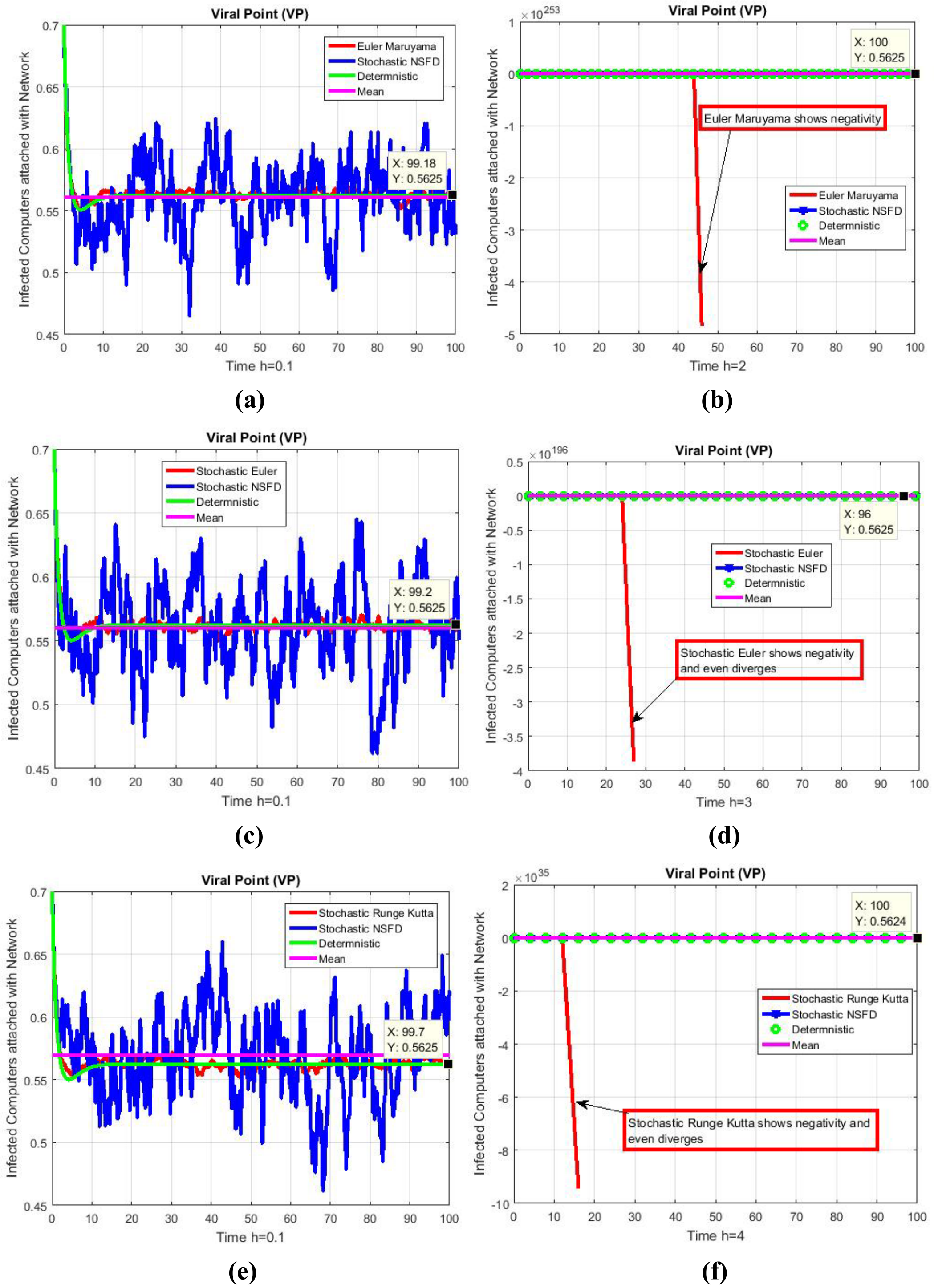
(a) (b)

(c) (d)

Figure 5: (a) Uninfected computers fraction for VFP at h=0.1 **(b)** Uninfected computers fraction for VFP at h=100 **(c)** Infected computers attached with network fraction for VP at h=0.1 **(d)** Infected computers attached with network fraction for VP at h=100

4.5.5 Comparison section

Comparison of explicit stochastic techniques with proposed SNSFD technique can be observed in this section as follows:



(a) (b)

(c) (d)

(e) (f)

Figure 6: Contrast in results of stochastic NSFD with stochastic explicit techniques **(a)** Spreader class with euler mayuyama and its average at h=0.1 **(b)** Spreader class with

euler mayuyama and its average at h=2 **(c)** Spreader class with stochastic euler and its average at h=0.1 **(d)** Spreader class with stochastic euler and its average at h=3 **(e)** Spreader class with stochastic runge kutta and its average at h=0.1 (f) Spreader class with stochastic runge kutta and its average at h=4

4.5.6 Covariance of sub-populations

The covariance of different sub-populations of computer virus model has been discussed in this section. The outcomes of covariance of sub populations are as follows in Tab. 3.

Table 3: Correlation coefficient

Sub-Populations	Correlation (ρ)	Coefficient	Relationship
(L, B)	0.8739		Direct
(S, L)	-0.9197		Inverse
(S, B)	-0.9944		Inverse

An inverse relationship can be seen between the uninfected class and the other two sub-populations. It shows that the increase in the uninfected class will occur with the decline in other sub-populations and ultimately the system attains virus-free equilibrium.

5 Outcomes and analysis

For discretisation parameter $\mathrm{h} = 0.1$, we see that euler maruyama technique meets to equilibria of the model, this can be seen by Fig. 2(a) and Fig. 2(c). On the other hand, the euler maruyama technique fails to sustain nonnegativity and even divergent, this can be seen by Fig. 2(b) and Fig. 2(d). For parameter $\mathrm{h} = 0.1$, we see that the stochastic euler technique meets to both equilibria, this can be seen by Fig. 3(a) and Fig. 3(c). On the other hand, for both equilibria the stochastic euler technique fails to maintain nonnegativity and consistency as shown in Fig. 3(b) and Fig. 3(d). For step size $\mathrm{h} = 0.1$, we see that the stochastic runge kutta technique converges to both equilibria, this can be seen graphically by Fig. 4(a) and Fig. 4(c).

The stochastic runge kutta technique fails to uphold stability and nonnegativity for both equilibrium points when we increase the step size this change happens in Fig. 4(b) and Fig. 4(d). Thus the aforementioned stochastic techniques do not sanctuary all the dynamical properties [Mickens (1994, 2005)]. On the other hand, for taking any discretisation parameter the stochastic NSFD technique converges for both equilibria, this can be seen by Fig. 5. In Fig. 6, we have presented the comparison of stochastic explicit and well-posed SNSFD techniques.

6 Conclusion and future framework

In comparison to deterministic computer virus model, the stochastic computer virus model is a more reliable strategy. The stochastic numerical techniques are detail-oriented and they work well for even minute time step size. They may lose the necessary properties of continuous dynamical system due to divergence on specific values of time step size. The SNSFD for computer virus model is capable of preserving important properties like positivity, dynamical consistency and boundedness. It is also appropriate for any time step size [Mickens (1994, 2005)]. For our future work, we are aiming to execute SNSFD to sophisticated stochastic delay and Spatio-temporal systems. Additionally, we could utilize the current numerical work in the extension of networking flows and fractional networking flows systems [Singh, Kumar and Baleanu (2019)]. In future, we are going to work for the reaction diffusion and fractional-order stochastic computer virus models.

Acknowledgement: We are the greatful to Vice-Chancellor, Air Vice Marshal Faaiz Amir (Retd.), Air University, Islamabad for providing an excellent research environment and facilities. The third author also thanks Prince Sultan University for funding this work through research-group number RG-DES2017-01-17.

Declaration: All author(s) have no competation regarding about publication of 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. 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.

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.

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.

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.

Karatzas, I., Shreve, S. E. (1988): *Brownian Motion and Stochastic Calculs*. Springer-Verlag.

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

Oksendal, B. (2003)*: Stochastic Differential Equations.* Springer Verlag, Berlin.

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.

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. 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.

Singh, J.; Kumar, D.; Baleanu, D. (2019): New aspects of fractional Biswas-Milovic model with mittag-leffer law. *Mathematical Modeling of Natural Phenomena*, vol. 14, no. 1, pp. 303-319.

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.

Yang, M.; Zhang, Z.; Li, Q.; Zhang, G. (2012): An SLBRS model with vertical transmission of computer virus over the Internet. *Discrete Dynamics in Nature and Society*, vol. 20, no. 12, pp. 1-17.

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.

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.