Numerical Simulations for Stochastic Computer Virus Propagation Model

Muhammad Shoaib Arif[1, *], Ali Raza[1], Muhammad Rafiq[2] , Mairaj Bibi[3], Javeria Nawaz Abbasi[3], Amna Nazeer[3] and Umer Javed[4]

Abstract: We are presenting the numerical simulations for the stochastic computer virus propagation model in this manuscript. We are comparing the solutions of stochastic and deterministic computer virus models. Outcomes of a threshold number R_0 hold in stochastic computer virus model. If $R_0 < 1$ then in such a condition virus controlled in the computer population while $R_0 > 1$ shows virus rapidly 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 technique can never violate the dynamical properties. On this basis, we can suggest a collection of strategies for removing virus's propagation in the computer population.

Keywords: Computer virus propagation model, Stochastic modelling, Stochastic processes, Stochastic techniques, Convergence analysis.

1 Introduction

A "computer virus" is a kind of malicious program which if performed, copies itself by changing various soft wares and putting in its particular code. When this process is successful, damaged areas are known as "diseased" by a computer virus. There are certain types of computer virus which include boot sector virus, multipartite viruses, macro viruses, stealth viruses, program virus, polymorphic virus and FAT virus. Motives for creating viruses are to get financial gains, to deliver public messages, someone's pleasure, to show that the system has some weaknesses. A typical virus makes two functions thus first it copies itself into uninfected programs or files. Second, it executes other malicious instructions the virus developer included in it. The techniques such as space-filling, packing and encryption are employed by computer virus experts in order to escape from detection. At the same time alternative static and dynamic methods are adopted by antivirus programs to detect the viruses. Some common sources of computer

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

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

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

[4] Department of Electrical and Computer Engineering, Comsats University, Wah Campus, Islamabad, Pakistan.

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

virus are downloading programs, pirated or cracked software, email attachments, internet, booting data from unknown CDs, Bluetooth and unpatched software. The symptoms such as partition completely disappears, no response from programs that use to run, due to the absence of certain critical system files windows does not start, receive the error messages containing the missing files, without uninstalling process a program vanishes from the computer, new icons appear on the desktop by self, the anti-virus software is not allowed to re-install by the computer, an unknown reason causes the anti-virus software to incapacitate and it cannot be restarted, a weird attachment is received from e-mail message, computer is not able to update the anti-virus software, email account consequently send messages with the virus to our contacts, we can't open files and documents with certain error or unknown file format, difficulty in re-opening the squashed information whose configuration has been changed, maximum functionality of an application is difficult to achieve, there is an un-usual sound or music plays from speakers and operations which are crashed and the computer shows the alarming messages along with the un-identified errors, it gets restarted again and again on itself, computer requires a long time to start and its execution is backed off etc. are observed in a virus tainted computer. Viruses regularly carry out different sort of damaging activities on diseased host computers, for instance acquirement of computer space and central processing unit (CPU) time, gaining access to secretive material (for example, credit card numbers), modifying data, showing a party-political or hilarious message on the desktop, spamming the e-mail contacts, taking down keystrokes and even sometimes making the computer unworkable.

2 Literature survey

In 1971, the first computer virus known as "Creeper system" was discovered and it could replicate itself. The computers which were affected by this virus could not work properly because the virus continues to fill up the hard drive. BBN technologies manufactured the virus in the US. In 1982, another worm is known as "Elk Cloner" came up as the initial virus to show outside a single computer lab where it was made. It was developed in 1981 by Richard Skrenta. The year 1986 was the discovery of first computer virus for MS-DOS named as "Brain". It had the functionality to obstruct the computer from booting, and it overwrites the boot sector on the floppy disk. In 1988 the first computer virus named "The Morris" emerged and it affected a large number of computer population. The purpose of writing this virus was to measure the magnitude of internet, and it was written by Robert Morris, a graduate student from Cornell University. The virus which was discovered in 1991 for the first time in Australia was named as "Michelangelo". Every year until 6^{th} march the virus stays inactive and then it restrains the computers from booting by overwriting the first one hundred blocks on the storage devices with zeros. The first virus to precisely attack MS windows was revealed in April 1992, two years after the launch of Windows 3.0. The first widespread word macro virus was released in the year 1999 known as "Melissa". In the year 2000, the virus named "I love you" reappears and sent itself to all contacts via email. The virus could overwrite music files, pictures and office files. In a short period of ten days the virus contaminated over fifty million computers. During the latent period of the computer virus, the individuals are exposed to a computer virus, but still they are not infected. An exposed computer is that which is infected in latency, but will not be able to infect other computers at once. However, there might be chance to get infected. In order to demonstrate the fact that although the exposed computer does not infect other computers, it still has infectivity, we use delay in modelling the computer virus [Han and Tan (2010); Zhu, Yang and Ren (2012)]. SLB and SLBS models were propounded by Yang et al. in these models, the authors assumed that during the period of latency the computer also has infectivity [Yang, Yang, Zhu et al. (2013); Yang, Yang, Wen at el. (2012)]. The task for modelling the spread nature of computer virus was done first time by Kephart et al. [Kephart and White (1991); Kephart and White (1993)]. A lot of research work has been done in the past in order to investigate the computer virus propagation by constructing the mathematical models presented in Han et al. [Han and Tan (2010); Ren, Yang, Zhu et al. (2012); Wierman and Marchette (2004); Yuan and Chen (2008)]. SIRS computer virus models were propounded by Mishra et al. in different forms in Mishra et al. [Mishra and Jha (2007); Mishra and Pandey (2010); Ren, Yang, Yang et al. (2012); Zhang and Yang (2015); Feng, Liao, Li et al. (2012)]. SEIR computer virus propagation model was illustrated by Yuan and Chen and they studied the stability of the model in Yuan et al. [Yuan and Chen (2008)]. The Hopf bifurcation of the SEIR model with time delay was explored by Dong et al. [Dong, Liao and Li (2012)]. In recent years many different computer virus models have been developed by other scholars presented in Wang et al. [Wang, Zhang, Wang et al. (2010); Mishra and Jha (2010); Yao, Xie, Guo et al. (2013); Muroya and Kuniya (2014); Gan, Yang and Zhu (2014)]. The discrete Markov model and a differential equation model of the computer virus propagation was credited to Billings et al. in Billings et al. [Billings, Spears and Schwartz (2002)]. The SIRA computer virus propagation model was proposed by Piqueira in Piqueira et al. [Piqueira, Vasconcelos, Gabriel et al. (2008)] and later he studied the mathematical properties such as stability and bifurcation conditions in Piqueira et al. [Piqueira and Araujo (2009)]. The research work made by these scholars leads us to utilize the subjective approach to figure out the conditions due to which virus spread in a computer population. The usual quantitative schemes like Euler and Runge-Kutta never maintain dynamical possessions as we have seen in the deterministic modelling. We have also seen that in Euler Maruyama, stochastic Euler and stochastic Runge-Kutta does not maintain the dynamical possessions in the stochastic case. So, from this a question arises and need to research more: Can we develop technique which does not violate the dynamical properties [Mickens (1994, 2005, 2005)].

We have a claim to call stochastic nonstandard finite difference (SNSFD) technique which always fulfils a need for a numerical method and preserves the dynamical properties. These properties defined by Mickens in the stochastic context presented in Mickens et al. [Mickens (1994, 2005, 2005)]. So, this is the major point of our paper.

The strategy of this paper is as follows:

The necessary details of SDEs have been given in Section 3. In Section 4, described the deterministic computer virus propagation model and their equilibria. In Section 5, explains the construction way of stochastic computer virus propagation model. In Section 6, explains the stochastic numerical techniques for stochastic computer virus propagation model and their convergence analysis. In the end, conclusion and our future work will be discussed in Section 7.

3 Deterministic computer virus propagation model

The deterministic computer virus propagation model has been presented in Yang et al. [Yang, Yang, Wen et al. (2012)]. The description of variables at any arbitrary time t is as follows, $S(t)$: (Represents susceptible PC's at any time t), $L(t)$: (Represents latent PC'S at any time t), $B(t)$:(Represents breaking-out computers at any time t). The flow of deterministic computer virus propagation model as shown in Fig. No. 1.

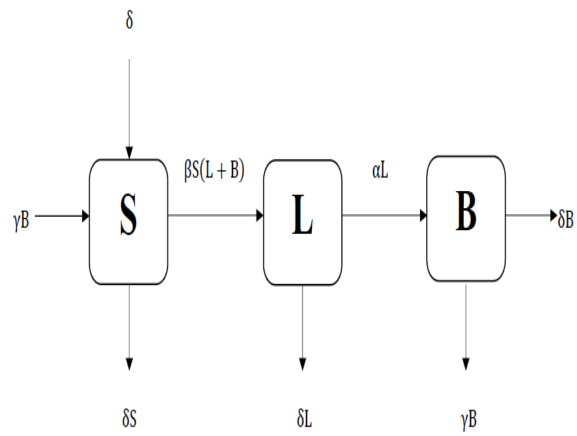


Figure 1: Flow map of computer virus propagation model

The parameters of computer virus propagation model are described as α: (This constant rate shows the number of latent computers that break out), β: (Represents the constant rate at which every virus-free PC is damaged by an infectious system), γ: (Represents the constant ratio with which the breaking-out systems are recovered.), δ: (Represents the constant ratio with which the outside systems are linked to the internet and the inside systems are detached from the world wide web).

The governing equations of the deterministic computer virus propagation model are given below as

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

where the region for system (1) is $\Omega = \{(S, L, B): S + L + B \leq 1, S \geq 0, L \geq 0, B \geq 0\}$. All solutions of system (1) will be nonnegative invariant and closed. This region will be called a feasible region.

3.1 Equilibria of the computer virus propagation model

The computer virus propagation model (1) has two following steady states which are as follows:

Virus-free equilibrium is $K_1 = (S, L, B) = (1,0,0)$

Virulent equilibrium is $K_2 = (S, L, B)$

where,

$S = \frac{\delta(\alpha+\delta)^2+\delta\gamma(2\delta+\alpha+\gamma)+\alpha\beta(\delta-\alpha)+\alpha\gamma}{\beta(\delta+\gamma)(\delta+\gamma+2\alpha)}$, $L = \frac{(\alpha+\delta+\gamma)(\beta-\delta)-\alpha\gamma}{\beta(\delta+\gamma+2\alpha)}$, $B = \frac{\alpha[\alpha\beta-\delta(\alpha+\delta)+\gamma(\beta-1)]}{\beta(\delta+\gamma)(\delta+\gamma+2\alpha)}$

$R_0 = \frac{\beta}{\alpha+\gamma} > 1$

Note that R_0 is the reproduction number.

4 Stochastic computer virus propagation model

Let we consider the vector $W = [S, L, B]^T$, the possible changes in the stochastic computer virus propagation model as follows (see Tab. 1).

Table 1: Transitions for the computer virus propagation model

Transition	Probabilities
$(\Delta W)_1 = [1, 0, 0]^T$	$P_1 = \delta\Delta t$
$(\Delta W)_2 = [-1, 1, 0]^T$	$P_2 = \beta S(L + B)\Delta t$
$(\Delta W)_3 = [1, 0, -1]^T$	$P_3 = \gamma B\Delta t$
$(\Delta W)_4 = [-1, 0, 0]^T$	$P_4 = \delta S\Delta t$
$(\Delta W)_5 = [0, -1, 1]^T$	$P_5 = \alpha L\Delta t$
$(\Delta W)_6 = [0, -1, 0]^T$	$P_6 = \delta L\Delta t$
$(\Delta W)_7 = [0, 0, -1]^T$	$P_7 = \delta B\Delta t$

The expectation and variance of the stochastic computer virus propagation model is defined as

$E^*[\Delta W] = \sum_{i=1}^{7} P_i T_i$.

Expectation $=E^*[\Delta W] = \begin{bmatrix} P_1 - P_2 + P_3 - P_4 \\ P_2 - P_5 - P_6 \\ -P_3 + P_5 - P_7 \end{bmatrix} \Delta t$.

Var= $E^*[\Delta W \Delta W^T] = \sum_{i=1}^{7} P_i [T_i][T_i]^T$.

$E^*[\Delta W \Delta W^T] == \begin{bmatrix} P_1 + P_2 + P_3 + P_4 & -P_2 & -P_3 \\ -P_2 & P_2 + P_5 + P_6 & -P_5 \\ -P_3 & -P_5 & P_3 + P_5 + P_7 \end{bmatrix} \Delta t.$

The general form of SDEs as follows:

$\frac{dW(t)}{dt} = f(W(t), t) + L(W(t), t) \frac{dB(t)}{dt}$.

Stochastic drift $= f(W(t), t) = \frac{E^*[\Delta W]}{\Delta t}$

Stochastic diffusion $= L(W(t), t) = \sqrt{\frac{E^*[\Delta W \Delta W^T]}{\Delta t}}$.

The SDE of system (1) as follows:

$$dW(t) = f(W(t), t)dt + L(W(t), t)dB(t). \quad (2)$$

with initial conditions $W(0) = W_o = [0.4, 0.4, 0.2]^T$, $0 \leq t \leq T$ and the Brownian motion is denoted by $B(t)$.

4.1 Euler Maruyama technique

The construction of this technique is presented in Maruyama [Maruyama (1955)]. For finding the solution of given SDEs presented as (2) and for parameters values see Tab. 2.

$$W_{n+1} = W_n + G_1(W_n, t)\Delta t + G_2(W_n, t)\Delta B_n. \quad (3)$$

The time step size is presented by 'Δt' and ΔB_n is standard normal distribution. i.e., $\Delta B_n \sim N(0,1)$. The solution of system (1) i.e., VFE is $K_1 = (1,0,0)$ and VE is $K_2 = (0.4537, 0.4249, 0.1214)$.

Table 2: Values of Parameter [Yang, Yang, Wen et al. (2012)]

Parameters	**Values (Years)**
δ	0.5
β	VFP=0.2
	VP=1.2
γ	0.2
α	0.2
σ	0.001

5 Parametric perturbation of computer virus propagation model

In this technique, we shall choose parameters from the system (1) and change into the random parameters with small noise as $\beta dt = \beta dt + \sigma dB$. So, the stochastic system (1) is as follows [Allen and Burgin (2000); Allen (2007); Allen, Allen, Arciniega et al. (2008)]

$$\left.\begin{aligned} dS &= [\delta - \beta S(L+B) + \gamma B - \delta S]dt - \sigma S(L+B)dB \\ dL &= [\beta S(L+B) - L(\alpha+\delta)]dt + \sigma S(L+B)dB \\ dB &= [\alpha L - B(\gamma+\delta)]dt \end{aligned}\right\} \quad (4)$$

The Brownian motion is denoted by $B_k(t), (k = 1,2,3)$, σ is the randomness of the system (4). The system (4) is non-integrable because of Brownian motion. So, we shall find its solution by using different stochastic techniques.

5.1 Stochastic Euler technique

The system (4) can be written in this technique as follows [Raza, Arif and Rafiq (2019); Raza, Arif, Rafiq et al. (2019); Arif, Raza, Rafiq et al. (2019); Arif, Raza, Rafiq et al. (2019)]:

$$\left.\begin{aligned} S^{n+1} &= S^n + h[\delta - \beta S^n(L^n + B^n) + \gamma B^n - \delta S^n - \sigma S^n(L^n + B^n)\Delta B_n] \\ L^{n+1} &= L^n + h[\beta S^n(L^n + B^n) - L^n(\alpha+\delta) + \sigma S^n(L^n + B^n)\Delta B_n] \\ B^{n+1} &= B^n + h[\alpha L^n - B^n(\gamma+\delta)] \end{aligned}\right\} \quad (5)$$

where $\Delta B_n \sim N(0,1)$ and 'h' called the time step size.

5.2 Stochastic Runge Kutta technique

The system (4) can be written in this technique as follows [Raza, Arif and Rafiq (2019); Arif, Raza, Rafiq et al. (2019)]:

Stage 1

$$A_1 = h[\delta - \beta S^n(L^n + B^n) + \gamma B^n - \delta S^n - \sigma S^n(L^n + B^n)\Delta B_n]$$
$$B_1 = h[\beta S^n(L^n + B^n) - L^n(\alpha + \delta) + \sigma S^n(L^n + B^n)\Delta B_n]$$
$$C_1 = h[\alpha L^n - B^n(\gamma + \delta)]$$

Stage 2

$$A_2 = h[\delta - \beta(S^n + \frac{A_1}{2})(L^n + \frac{B_1}{2}) + (B^n + \frac{C_1}{2}) + \gamma(B^n + \frac{C_1}{2}) - \delta(S^n + \frac{A_1}{2}) - \sigma(S^n + \frac{A_1}{2})\left((L^n + \frac{B_1}{2}) + (B^n + \frac{C_1}{2})\right)\Delta B_n]$$
$$B_2 = h\left[\beta(S^n + \frac{A_1}{2})\left((L^n + \frac{B_1}{2})(B^n + \frac{C_1}{2})\right) - (L^n + \frac{B_1}{2})(\alpha + \delta) + \sigma(S^n + \frac{A_1}{2})\left((L^n + \frac{A_1}{2}) + (B^n + \frac{C_1}{2})\right)\Delta B_n\right]$$
$$C_2 = h[\alpha(L^n + \frac{B_1}{2}) - (B^n + \frac{C_1}{2})(\gamma + \delta)]$$

Stage 3

$$A_3 = h[\delta - \beta(S^n + \frac{A_2}{2})(L^n + \frac{B_2}{2}) + (B^n + \frac{C_2}{2}) + \gamma(B^n + \frac{C_2}{2}) - \delta(S^n + \frac{A_2}{2}) - \sigma(S^n + \frac{A_2}{2})\left((L^n + \frac{B_2}{2}) + (B^n + \frac{C_2}{2})\right)\Delta B_n]$$
$$B_3 = h\left[\beta(S^n + \frac{A_2}{2})\left((L^n + \frac{B_2}{2})(B^n + \frac{C_2}{2})\right) - (L^n + \frac{B_2}{2})(\alpha + \delta) + \sigma(S^n + \frac{A_2}{2})\left((L^n + \frac{B_2}{2}) + (B^n + \frac{C_2}{2})\right)\Delta B_n\right]$$
$$C_3 = h[\alpha(L^n + \frac{B_2}{2}) - (B^n + \frac{C_2}{2})(\gamma + \delta)]$$

Stage 4

$$A_4 = h[\delta - \beta(S^n + \frac{A_3}{2})(L^n + \frac{B_3}{2}) + (B^n + \frac{C_3}{2}) + \gamma(B^n + \frac{C_3}{2}) - \delta(S^n + \frac{A_3}{2}) - \sigma(S^n + \frac{A_3}{2})\left((L^n + \frac{B_3}{2}) + (B^n + \frac{C_3}{2})\right)\Delta B_n]$$
$$B_4 = h\left[\beta(S^n + \frac{A_3}{2})\left((L^n + \frac{B_3}{2})(B^n + \frac{C_3}{2})\right) - (L^n + \frac{B_3}{2})(\alpha + \delta) + \sigma(S^n + \frac{A_3}{2})\left((L^n + \frac{B_3}{2}) + (B^n + \frac{C_3}{2})\right)\Delta B_n\right]$$
$$C_4 = h[\alpha(L^n + \frac{B_3}{2}) - (B^n + \frac{C_3}{2})(\gamma + \delta)]$$

Final stage

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

where $\Delta B_n \sim N(0,1)$ and 'h' called the time step size.

5.3 Stochastic NSFD technique

The system (4) can be written in this technique as follows [Raza, Arif and Rafiq (2019); Arif, Raza, Rafiq et al. (2019)]

$$\left.\begin{aligned} S^{n+1} &= \frac{S^n + h\delta + h\gamma B^n}{1 + h\beta(L^n + B^n) + h\delta + h\sigma(L^n + B^n)\Delta B_n} \\ L^{n+1} &= \frac{L^n + h\beta S^n(L^n + B^n) + h\sigma S^n(L^n + B^n)\Delta B_n}{1 + h(\alpha + \delta)} \\ B^{n+1} &= \frac{B^n + h\alpha L^n}{1 + h(\gamma + \delta)} \end{aligned}\right\} \quad (7)$$

where $\Delta B_n \sim N(0,1)$ and 'h' called the time step size.

5.3.1 Convergence analysis

Theorem

For any given initial value $[S(0), L(0), B(0) \in R_+^3]$ system (7) has a unique positive solution $(S^n, L^n, B^n) \in R_+^3$ on $n \geq 0$, almost surely

Theorem

The region $\Omega = \{(S^n, L^n, B^n) \in R_+^3 : S^n \geq 0, L^n \geq 0, B^n \geq 0, S^n + L^n + B^n \leq 1\}$ for all $n \geq 0$ is a nonnegative invariant set for the system (7).

Proof: The system (7) can be written as follows:

$$\frac{S^{n+1} - S^n}{h} = \delta - \beta S^n L^n - \beta S^n B^n + \gamma B^n - \delta S^n - \sigma S^n L^n \Delta B_n - \sigma S^n B^n \Delta B_n$$

$$\frac{L^{n+1} - L^n}{h} = \beta S^n L^n + \beta S^n B^n - \alpha L^n - \delta L^n + \sigma S^n L^n \Delta B_n + \sigma S^n B^n \Delta B_n$$

$$\frac{B^{n+1} - B^n}{h} = \alpha L^n - \beta B^n - \delta B^n$$

Adding all the equations, we have

$$\frac{S^{n+1} - S^n}{h} + \frac{L^{n+1} - L^n}{h} + \frac{B^{n+1} - B^n}{h} = \delta - \delta S^n - \delta L^n - \delta B^n$$

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

$$(S^{n+1} + L^{n+1} + B^{n+1}) = (S^n + L^n + B^n) + h\delta[1 - (S^n + L^n + B^n)].$$

$$(S^{n+1} + L^{n+1} + B^{n+1}) \leq 1 + h\delta(1 - 1).$$

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

almost surely.

Theorem

The discrete dynamical system (7) has the same steady states as that of the continuous dynamical system (4) for all $n \geq 0$.

Proof: For solving the system (7), we get two states as follows:

VFE i.e., $K_3 = (S^n, L^n, B^n) = (1,0,0)$.

VE i.e., $K_4 = (S^n, L^n, B^n)$.

where,

$S^n = \frac{\delta(\alpha+\delta)^2+\delta\gamma(2\delta+\alpha+\gamma)+\alpha\beta(\delta-\alpha)+\alpha\gamma}{\beta(\delta+\gamma)(\delta+\gamma+2\alpha)}$, $L^n = \frac{(\alpha+\delta+\gamma)(\beta-\delta)-\alpha\gamma}{\beta(\delta+\gamma+2\alpha)}$, $B^n = \frac{\alpha[\alpha\beta-\delta(\alpha+\delta)+\gamma(\beta-1)]}{\beta(\delta+\gamma)(\delta+\gamma+2\alpha)}$

almost surely.

Theorem

The eigenvalues of the discrete dynamical system (7) lie in the unit circle for all $n \geq 0$.

Proof:

We suppose F, G, and H from the system (7) as follows:

$$F = \frac{S + h\delta + h\gamma B}{1 + h\beta(L + B) + h\delta + h\sigma(L + B)\Delta B_n},$$

$$G = \frac{L + h\beta S(L + B) + h\sigma S(L + B)\Delta B_n}{1 + h(\alpha + \delta)},$$

$$H = \frac{B + h\alpha L}{1 + h(\gamma + \delta)},$$

The Jacobean matrix defined as

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

where, $\frac{\partial F}{\partial S} = \frac{1}{1+h\beta(L+B)+h\delta+h\sigma(L+B)\Delta B_n}$, $\frac{\partial F}{\partial L} = \frac{-(S+h\delta+h\gamma B)(h\beta+h\sigma\Delta B_n)}{[1+h\beta(L+B)+h\delta+h\sigma(L+B)\Delta B_n]^2}$,

$\frac{\partial F}{\partial B} = \frac{h[\gamma(1+h\beta L+h\delta+h\sigma L\Delta B_n)-S(\beta+\sigma)-h\delta(\beta+\sigma\Delta B_n)]}{[1+h\beta(L+B)+h\delta+h\sigma(L+B)\Delta B_n]^2}$, $\frac{\partial G}{\partial S} = \frac{(L+B)(h\beta+h\sigma\Delta B_n)}{1+h(\alpha+\delta)}$, $\frac{\partial G}{\partial L} = \frac{1+hS(\beta+\sigma\Delta B_n)}{1+h(\alpha+\delta)}$,

$\frac{\partial G}{\partial B} = \frac{hS(\beta+\sigma\Delta B_n)}{1+h(\alpha+\delta)}$, $\frac{\partial H}{\partial S} = 0$, $\frac{\partial H}{\partial L} = \frac{h\alpha}{1+h(\gamma+\delta)}$, $\frac{\partial H}{\partial B} = \frac{1}{1+h(\gamma+\delta)}$,

Now we want to linearize the model about the equilibria of the model for virus-free equilibrium $K_1 = (S, L, B) = (1,0,0)$ and $R_0 < 1$.

The given Jacobean is

$$
\mathrm{J} = \begin{bmatrix} \frac{1}{1+h\delta} & \frac{-(1+h\delta+h\gamma B)(h\beta+h\sigma\Delta B_n)}{[1+h\delta]^2} & \frac{h[\gamma(1+h\delta)-(\beta+\sigma)-h\delta(\beta+\sigma\Delta B_n)]}{[1+h\delta]^2} \\ 0 & \frac{1+h(\beta+\sigma\Delta B_n)}{1+h(\alpha+\delta)} & \frac{h(\beta+\sigma\Delta B_n)}{1+h(\alpha+\delta)} \\ 0 & \frac{h\alpha}{1+h(\gamma+\delta)} & \frac{1}{1+h(\gamma+\delta)} \end{bmatrix}.
$$

The eigenvalues of the Jacobian matrix is

$\lambda_1 = \frac{1}{1+h\delta} < 1, \lambda_2 = \frac{1+h(\beta+\sigma\Delta B_n)}{1+h(\alpha+\delta)} < 1,\ R_0 < 1$

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

This is guaranteed to fact that the all eigenvalues of Jacobean lies in a unit circle. So, the system (7) is LAS around K_1.

5.4 Numerical experiments

5.4.1 Euler Maruyama technique

The simulation for the system (3) as follows:

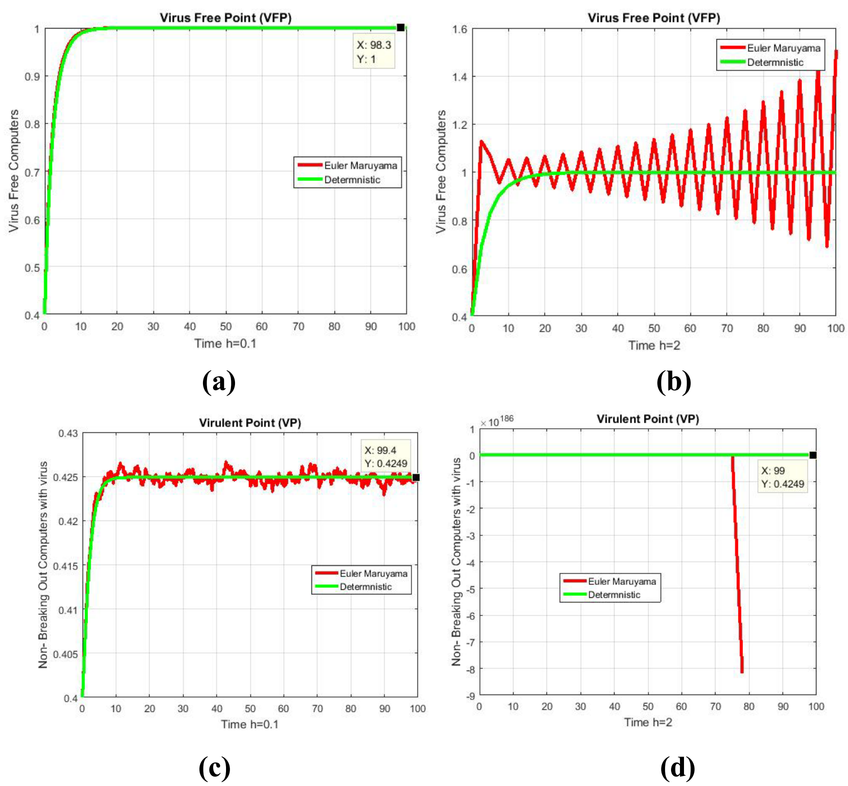
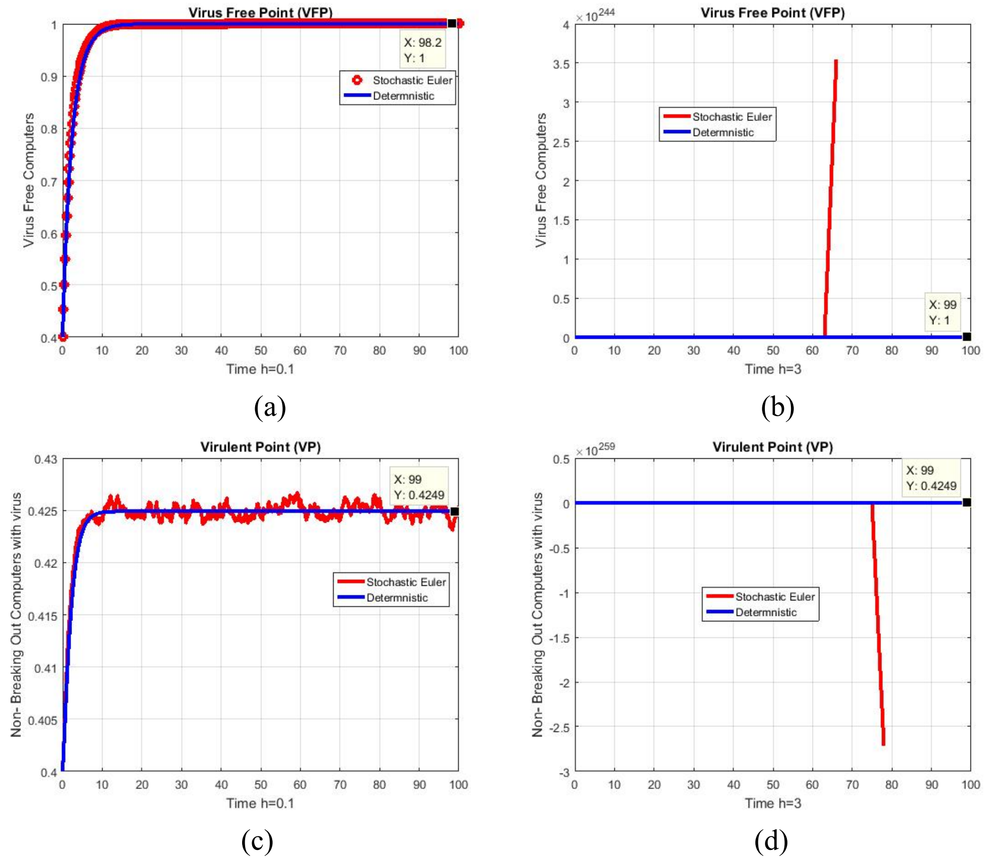


Figure 2: (a) Virus-free computers at VFP for h=0.1 (**b)** Virus-free computers at VFP for h=2 **(c)** Non-Breaking out computers with the virus at VP for h=0.1 **(d)** Non-Breaking out computers with virus at VP for h=2

5.4.2 Stochastic euler technique

The simulation for the model (5) as follows:

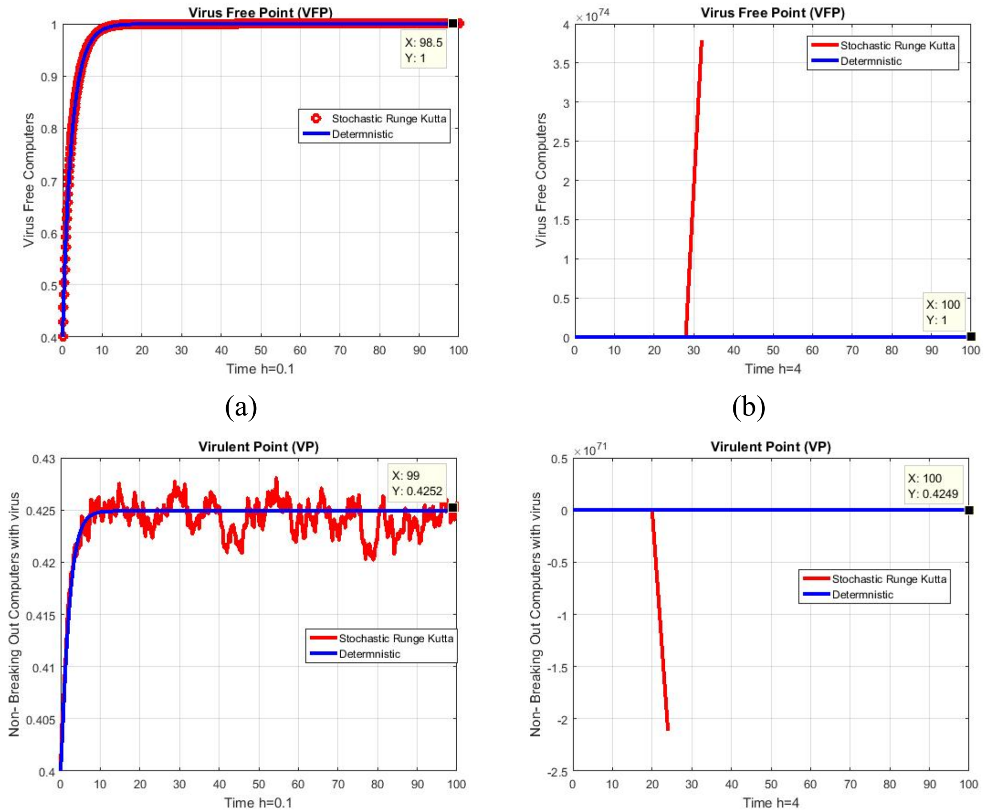


(a) (b) (c) (d)

Figure 3: (a) Virus-free computers at VFP for h=0.1 (**b)** Virus-free computers at VFE Point for h=3 **(c)** Non-Breaking out computers with the virus at VP for h=0.1 **(d)** Non-Breaking out computers with virus at VP for h=3

5.4.3 Stochastic Runge Kutta technique

The simulation for the model (6) as follows



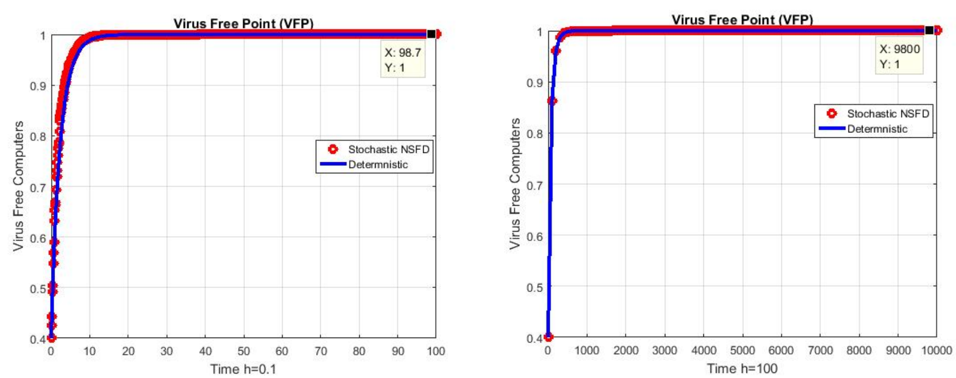
(a) (b)

(c) (d)

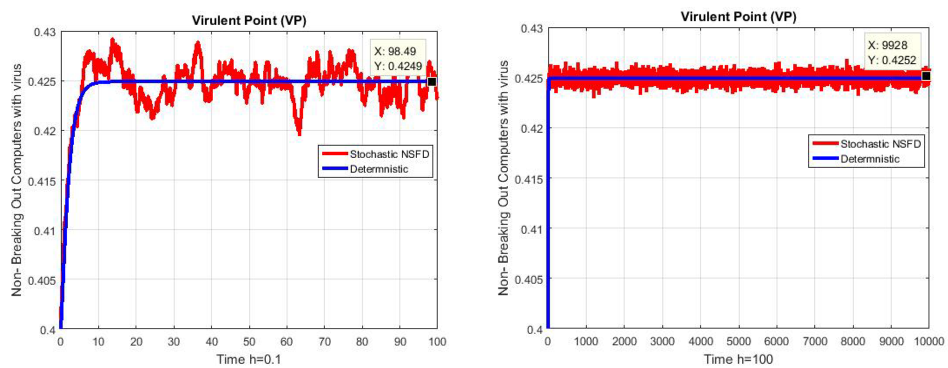
Figure 4: (a) Virus free computers at VFP for h=0.1 (**b)** Virus free computers at VFP for h=4 **(c)** Non-Breaking out computers with virus at VP for h=0.1 **(d)** Non-Breaking out computers with virus at VP for h=4

5.4.4 Stochastic NSFD technique

The simulation for the model (7) as follows:



(a) **(b)**

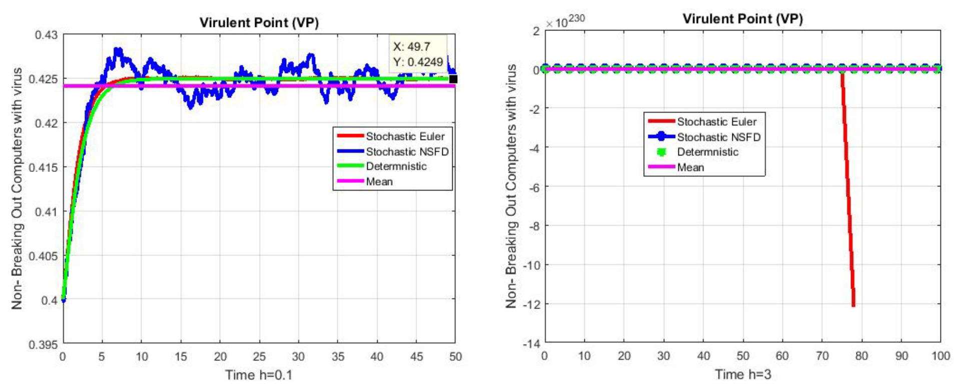


(c) **(d)**

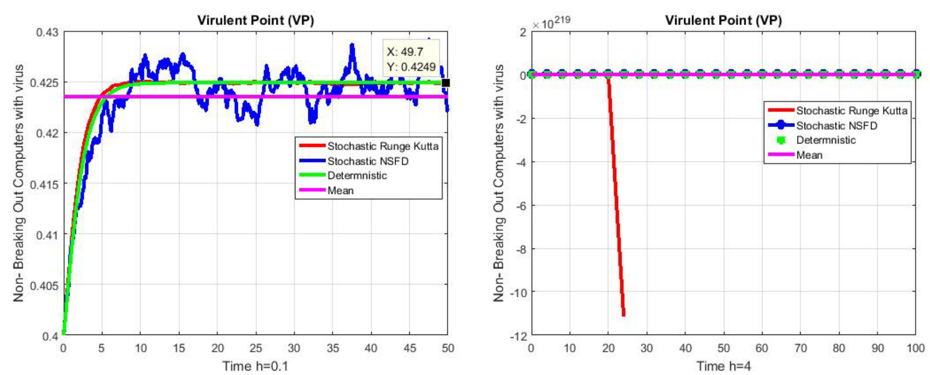
Figure 5: (a) Virus-free computers at VFP for h=0.1 (**b)** Virus-free computers at VFP for h=100 **(c)** Non-Breaking out computers with the virus at VP for h=0.1 **(d)** Non-Breaking out computers with virus at VP for h=100

5.5.5 Contrast section

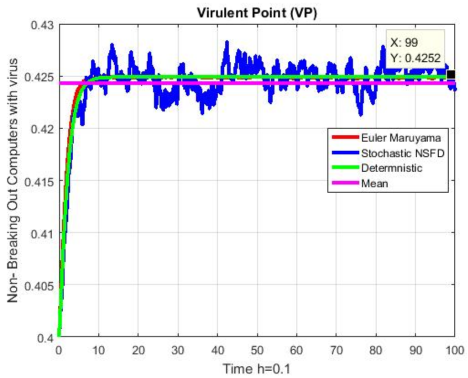
In this segment, we shall draw the contrast of stochastic techniques for both equilibria as follows:



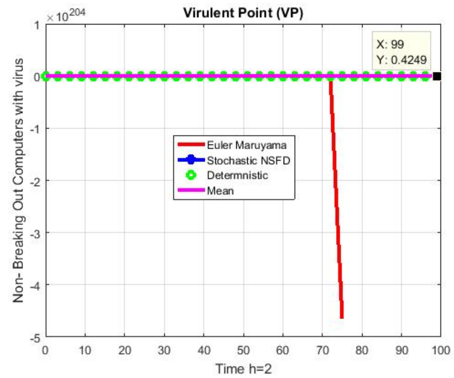
(a) **(b)**



(c) **(d)**



(e)



(f)

Figure 6: (a) Non-Breaking out computers with virus, stochastic Euler and its average at h=0.1 (**b)** Non-Breaking out computers with virus, stochastic Euler and its average at h=3 **(c)** Non-Breaking out computers with virus, stochastic Runge Kutta and its average at h=0.1 **(d)** Non-Breaking out computers with virus, stochastic Runge Kutta and its average at h=4 **(e)** Non-Breaking out computers with virus, Euler Maruyama and its average at h=0.1 **(f)** Non-Breaking out computers with virus, Euler Maruyama and its average at h=2

5.5.6 Covariance of subpopulations

The covariance of the stochastic computer virus propagation model has been discussed in this section. By calculating the correlation coefficients, we shall be able to inspect covariance between distinct sub-populations and the results are dispatched in Tab. 3.

Table 3: Correlation number

Sub-Populations	Correlation Number (ρ)	Relationship
(L, B)	−0.9715	Inverse
(S, L)	0.9374	Direct
(S, B)	−0.9933	Inverse

We can observe in Tab. 3 that there is an inverse relationship between virus-free computers and remaining two sub-populations of the computer model. The inverse relationship among these sub-compartments shows that virus-free equilibrium can be attained if there is an increase in virus-free computers along with decrease in remaining sub-populations. Then, the system completely virus free.

6 Discussion of results

The Euler Maruyama shows convergence in Fig. 2(a) and Fig. 2(c) at h=0.01 and shows non-positivity in Fig. 2(b) and Fig. 2(d). On the other hand, The stochastic Euler shows convergence in Fig. 3(a) and Fig. 3(c) at h=0.01 and shows non-positivity in Fig. 3(b) and Fig. 3(d). In same manner, The stochastic Runge Kutta shows convergence in Fig. 4(a) and Fig. 4(c) at h=0.01 and shows non-positivity and unboundedness in Fig. 4(b) and Fig.

4(d). So, we concluded that those mentioned above explicit stochastic techniques are time-dependent and conditionally convergent. In Fig. 5, the SNSFD approaches to both equilibria of model for any discretization. In Fig. 6, we have shown the efficiency of SNSFD technique with existing stochastic explicit techniques for different time-step sizes. Also, the solution of ode (deterministic) system is obtained from the arithmetic mean of stochastic simulations. This is the beauty of SNSFD as compared to other stochastic explicit techniques.

7 Conclusion and directions

After this analysis, we can give idea that SDEs analysis of computer virus propagation model is suitable as compared to ODEs analysis. All stochastic techniques violate dynamical properties. These techniques give a non-positive solution and unbounded solutions. This type of dynamics has no significance in physical systems. We have introduced SNSFD technique for this modelling under the assumption the discussed by Mickens in stochastic context [Mickens (1994, 2005]. This technique always satisfies the dynamical properties such as dynamical consistency, nonnegativity and boundedness of model. In future, we shall extend this idea in the field of all type of networking systems. Also, we shall construct fraction order networking models [Jajarmi and Baleanu (2018); Jajarmi, Baleanu, Bonyah et al. (2018); Singh, Kumar and Baleanu (2019)].

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: All author(s) have no competition regarding about publication of this article.

References

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.

Arif, M. S.; Raza, A.; Rafiq, M.; Bibi M. (2019): A reliable numerical analysis for stochastic hepatitis B virus epidemic model with the migration effect. *Iranian Journal of Science and Technology*, *Transaction A*, vol. 9, no. 4, pp. 1-16.

Arif, M. S.; Raza, A.; Rafiq, M.; Bibi M.; Fayyaz, R. et al. (2019): A reliable stochastic numerical analysis for typhoid fever incorporating with protection against fever. *Computers, Materials and Continua*, vol. 59, no. 3, pp. 787-804.

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.

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.

Dong, T.; Liao. X.; Li, H. (2012): Stability and Hopf bifurcation in a computer virus model with multistate antivirus. *Abstract and Applied Analysis*, vol. 1, no. 4, pp. 1-16.

Feng, L.; Liao, X.; Li, H.; Han, Q. (2012): Hopf bifurcation analysis of a delayed viral infection model in computer networks. *Mathematical and Computer Modelling*, vol. 56, no. 8, pp. 167-179.

Gan, C.; Yang, X.; Zhu, Q. (2104): Propagation of computer virus under the influences of infected external computers and removable storage media: modeling and analysis. *Nonlinear Dynamics*, vol. 78, no. 2, pp. 1349-1356.

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

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.

Kephart J. O.; White, S. R. (1991): Directed-graph epidemiological models of computer viruses. *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 343-359.

Kephart J. O.; White S. R. (1993): Measuring and modeling computer virus prevalence. *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 2-15.

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.

Mishra, B. K.; Pandey, S. K. (2010): Fuzzy epidemic model for the transmission of worms in computer network. *Nonlinear Analysis: Real World Applications*, vol. 11, no. 5, pp. 4335-4341.

Muroya, Y.; Huaixing, L.; Kuniya, T. (2014): On global stability of a nonresident computer virus model. *Acta Mathematica Scientia*, vol. 34, no. 5, pp. 1427-1445.

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, pp. 355-359.

Raza, A.; Arif, M. S.; Rafiq, M.; Bibi, M.; Naveed, M. et al. (2019): Numerical treatment for stochastic computer virus. *Computer Modeling in Engineering & Sciences*, vol. 120, no. 2, pp. 445-465.

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. 3, pp. 303.

Wang, F.; Zhang, Y.; Wang, C.; Ma, J.; Moon, S. (2010): Stability analysis of a SEIQV epidemic model for rapid spreading worms. *Computers & Security*, vol. 29, no. 4, pp. 410-418.

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.

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.