Tech Science Press

Spatio-Temporal Dynamics and Structure Preserving Algorithm for Computer Virus Model

**Nauman Ahmed[1,2], Umbreen Fatima[1], Shahzaib Iqbal[1], Ali Raza[3], Muhammad Rafiq[4,*]
Muhammad Aziz-ur-Rehman[2], Shehla Saeed[1], Ilyas Khan[5] and Kottakkaran Sooppy Nisar[6]**

[1]Department of Mathematics and Statistics, The University of Lahore, Lahore, Pakistan
[2]Department of Mathematics, University of Management and Technology, Lahore, Pakistan
[3]Department of Mathematics, National College of Business Administration and Economics, Lahore, Pakistan
[4]Department of Mathematics, Faculty of Sciences, University of Central Punjab, Lahore, Pakistan
[5]Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh, 72915, Vietnam
[6]Department of Mathematics, College of Arts and Sciences at Wadi Aldawaser, Prince Sattam Bin Abdulaziz University, Alkharj, Saudi Arabia
*Corresponding Author: Muhammad Rafiq. Email: m.rafiq@ucp.edu.pk

Abstract: The present work is related to the numerical investigation of the spatio-temporal susceptible-latent-breaking out-recovered (SLBR) epidemic model. It describes the computer virus dynamics with vertical transmission via the internet. In these types of dynamics models, the absolute values of the state variables are the fundamental requirement that must be fulfilled by the numerical design. By taking into account this key property, the positivity preserving algorithm is designed to solve the underlying SLBR system. Since, the state variables associated with the phenomenon, represent the computer nodes, so they must take in absolute. Moreover, the continuous system (SLBR) acquires two steady states i.e., the virus-free state and the virus existence state. The stability of the numerical design, at the equilibrium points, portrays an exceptional aspect about the propagation of the virus. The designed discretization algorithm sustains the stability of both the steady states. The computer simulations also endorse that the proposed discretization algorithm retains all the traits of the continuous SLBR model with spatial content. The stability and consistency of the proposed algorithm are verified, mathematically. All the facts are also ascertained by numerical simulations.

Keywords: Spatio-temporal; computer virus model; discretization; positive solution; computer simulations

1 Introduction

A computer virus is a program that can be spread out among the computers and networks by replicating itself. These viruses are deleterious for computer software as well as hardware. The message of removing all the files on your system is a clear indication of the virus attack. The virus can reproduce itself by operating on some other programs like an epidemic disease [1].

The motive behind developing the malware is to contaminate the systems, destruction of computer hardware, and stealing of significant data. In this way, the hackers get administrative control of the system [2]. They design such viruses with the malevolent intention to victimize online users by setting a trap for them. A virus infects the computer when malware runs on the system. They use many techniques to make the program run by the user. When someone opens the file, the virus attaches to it or hides in the form of codes that runs, automatically. When someone receives an infected file by email or from the internet while downloading the other files and the virus code becomes active, when the file is opened. In this way, the virus can make replicas of itself on a computer disk, on other files and can change the setting of the computers. Boot sector virus, direct action virus, resident virus, parasitic virus (file virus), multipartite virus, polymorphic virus, and macro viruses are some of the common computer viruses. The viruses not only corrupt or remove the data but can also harm the economy by interrupting trade activities. It is a common fact about the viruses that they can remove or corrupt everything on the hard drive. This is a serious issue, but a strong backup can resolve this problem. Some side-effects are more serious, for instance during working hours the virus prevents systems from functioning and gives a shutdown command to the device, resulting in economic loss. Some viruses interrupt the business activities, for instance, Melissa or Explore Zip, can block or destroy the server by generating a lot of unnecessary emails. Sometimes companies detect and respond to the risk by shutting down their mail servers to avoid the situation. When a system becomes infected, it shows unusual behavior such as low performance, automatic multiplication of the files, and the self-running of the program files, etc. Moreover, the files and folders become corrupted and the hard disk produces sounds. Now, people can get information more quickly than ever before, by the internet. The pitfall that has also arisen, is the harmful computer codes, which access the systems by different modes. The risk of virus spread has increased by the use of the internet and it is a major threat to internet users [3]. In the recent past, most of the viruses were propagated by floppy or compact disks. So, the role of the user in spreading the virus was obvious. Moreover, the side effects of the virus were so clear that everyone could adopt safety and precautionary measures. Now, the extensive use of the internet has changed the scenario by rapid sharing of the software. So, the propagation of any virus via the internet is very easy. Anyone can download a program easily from a website. So, the parasitic (file) viruses can rapidly grow by the widespread usage of the net. The micro viruses can seriously affect the documents. The internet users download the documents, spreadsheets, or files in routine and exchange them by email. A computer is infected either by downloading the file or by email. A computer virus works in two ways, the first one is instant replication when it runs on a susceptible computer and the second one remains inactive. In other words, the infected program needs to be run for its activation. Consequently, it is highly important to stay protected from viruses by installing a robust antivirus program. Only the end-users of the internet are safe. Some hackers make websites for targeting web servers. It is a common strategy to send a large number of requests on the webserver which slow down or crash it. When this happens, the candid user can no longer be able to get access to the website which is hosted by the server. It is worth mentioning that malicious computer viruses have become a great peril to the community. Since they acquire data and damage the parts of the computer like the hard drive and motherboard. To understand the dynamics of the computer virus, the mathematical epidemic models play an imperative role [4–9]. Numerous researchers suggested different mathematical models for explaining the virus communication through different

mediums [10–14]. Here, the spatially-structured computer virus model is studied analytically and numerically [15,16].

$$\frac{\partial S}{\partial t} = \mu - \mu S - \beta S (L + B) + \alpha (1 - S - L - B) + d_s \frac{\partial^2 S}{\partial x^2} \tag{1}$$

$$\frac{\partial L}{\partial t} = \beta S (L + B) - \mu L - \epsilon L + d_L \frac{\partial^2 L}{\partial x^2} \tag{2}$$

$$\frac{\partial B}{\partial t} = \epsilon L - \mu B - \gamma B + d_B \frac{\partial^2 B}{\partial x^2} \tag{3}$$

The initial conditions are of the form

$$S(x,0) = \Phi_1(x) \geq 0, \quad L(x,0) = \Phi_2(x) \geq 0, \quad B(x,0) = \Phi_3(x) \geq 0, \quad 0 \leq x \leq L$$

and the boundary conditions are

$$\frac{\partial S(0,t)}{\partial x} = \frac{\partial L(0,t)}{\partial x} = \frac{\partial B(0,t)}{\partial x} = 0; \quad t > 0,$$

$$\frac{\partial S(L,t)}{\partial x} = \frac{\partial L(L,t)}{\partial x} = \frac{\partial B(L,t)}{\partial x} = 0; \quad t > 0,$$

Also, $S + L + B \leq 1$.

Here, the quantity S describes the susceptible computers at time t and space x, that can be infected from virus, L and B represent the latent and the breaking out computers at time t and space x. The parameter μ is the rate at which the computers are connected and withdrawn from the internet. The parameters β, γ and ϵ are transmission rate, recovery rate and latent to breaking out rate respectively. The nonnegative constant value of α is the rate at which recovered computers become susceptible again. This study is about the numerical investigation of the computer virus epidemic model with diffusion in one space dimension. The motive behind this study is to design a reliable numerical algorithm that preserves all the core structure of the continuous computer virus epidemic model. In the literature, various researchers have designed many structure-preserving numerical techniques and applied them to solve the various dynamical systems belonging to different areas of science and engineering [17–21]. The appearance of chaotic behavior in graphical solutions by using a numerical technique whereas this chaos is not the part of the physical system under study is called the contrived chaos. The algorithm proposed in this manuscript not only eliminates this type of contrived chaos but also retains the positive behavior of the solution to the model (1)–(3).

2 Steady States of the System

This section is meant for the steady states of the model. The steady states of a dynamical system have a decisive role in describing the stability of the system as well as of the algorithm. There are two states of the computer virus epidemic model, virus-free state (VFS) and virus persistence state (VPS). VFS is $E_1 = (S_0, L_0, B_0) = (1, 0, 0)$.

VPS is

$$E_1 = (S^*, L^*, B^*) = \left(\frac{(\gamma+\mu)(\mu+\varepsilon)}{\beta(\mu+\gamma+\varepsilon)}, \frac{(\gamma+\mu)(\mu+\alpha)\beta(\mu+\gamma+\varepsilon)-(\gamma+\mu)(\gamma+\mu)(\mu+\varepsilon)(\mu+\alpha)}{\beta(\mu+\gamma+\varepsilon)(\alpha+\mu+\varepsilon)(\gamma+\mu)+\alpha\varepsilon}, \right.$$

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

$\mathfrak{R}^* = \dfrac{\beta(\mu+\gamma+\varepsilon)}{(\mu+\varepsilon)(\mu+\gamma)}$, where $d_S = d_L = d_B = 0$. $\mathfrak{R}^*$ is the basic reproductive value of underlying system (1)–(3).

3 Numerical Methods

In this portion, the proposed numerical design will be presented. To construct the algorithm, we divide $[0, \mathcal{L}] \times [0, \mathcal{T}]$ into $\mathcal{M} \times \mathcal{N}$, with step sizes $\Delta x = \dfrac{\mathcal{L}}{\mathcal{M}}$ and $\Delta t = \dfrac{\mathcal{T}}{\mathcal{N}}$. The nodal points for both the domains i.e., space and time, are considered as,

$$x_n = n\Delta x, \quad n \in \{0, 1, \ldots, \mathcal{M}\}, \quad t_j = j\Delta t, \quad j \in \{0, 1, \ldots, \mathcal{N}\}.$$

S_n^j, L_n^j and B_n^j denote the FD approximations of $S(n\Delta x, j\Delta t)$, $L(n\Delta x, j\Delta t)$ and $B(n\Delta x, j\Delta t)$ respectively.

Now, the proposed FD scheme for (3) is developed on the basis of the rules presented by Micken [22] as follows;

$$S_n^{j+1} = S_n^j + R_1\left(S_{n-1}^j + S_{n+1}^j\right) - 2R_1 S_n^{j+1} + \Delta t\mu - \Delta t\beta\left(L_n^j + B_n^j\right)S_n^{j+1} - \Delta t\mu S_n^{j+1} + \alpha\Delta t(1 - S_n^j - L_n^j - B_n^j)$$

$$(4)$$

After some computations, we have

$$S_n^{j+1} = \frac{S_n^j + R_1\left(S_{n-1}^j + S_{n+1}^j\right) + \mu\Delta t + \alpha\Delta t(1 - S_n^j - L_n^j - B_n^j)}{1 + 2R_1 + \Delta t\mu + \Delta t\beta\left(L_n^j + B_n^j\right)} \tag{5}$$

In a similar way, we have

$$L_n^{j+1} = \frac{L_n^j + R_2\left(L_{n-1}^j + L_{n+1}^j\right) + \Delta t\beta\left(L_n^j + B_n^j\right)S_n^j}{1 + 2R_2 + \Delta t(\mu + \epsilon)} \tag{6}$$

and

$$B_n^{j+1} = \frac{B_n^j + R_3\left(B_{n-1}^j + B_{n+1}^j\right) + \Delta t\epsilon L_n^j}{1 + 2R_3 + \Delta t(\mu + \gamma)} \tag{7}$$

Here, $R_1 = d_S \dfrac{\Delta t}{\Delta x^2}$, $R_2 = d_E \dfrac{\Delta t}{\Delta x^2}$ and $R_3 = d_I \dfrac{\Delta t}{\Delta x^2}$.

4 Stability of the Proposed Scheme

This section is devoted to validate the stability of the proposed algorithm (5)–(7) by using Von Neumann stability criteria.

Theorem: The proposed algorithm (5)–(7) is Von Neumann stable.

Proof. Substituting $S_n^j = \eta(t) e^{i\zeta x}$ in the proposed algorithm (4) and then linearizing, we have

$$\eta(t + \delta t) e^{i\zeta x} = \eta(t) e^{i\zeta x} + R_1 \left(e^{i\zeta(x - \delta x)} + e^{i\zeta(x + \delta x)} \right) \eta(t) - 2R_1 \eta(t + \delta t) e^{i\zeta x}$$

$$- \mu \Delta t \eta(t + \delta t) e^{i\zeta x} - \beta \Delta t \eta(t + \delta t)$$

After some computations, we have,

$$\left| \frac{\eta(t + \Delta t)}{\eta(t)} \right| = \left| \frac{1 + 2R_1 - 4R_1 sin^2(\zeta \delta x/2)}{1 + 2R_1 + \Delta t \mu + \beta \Delta t} \right| \leq \left| \frac{1 - 2R_1}{1 + 2R_1 + \Delta t \mu + \beta \Delta t} \right| < 1$$

From the above expression, it is clear that the approximation algorithm (5) is Von Neumann stable. In a similar fashion, it can be observed that the approximate algorithms (6) and (7) are also Von Neumann stable.

5 Consistency of the Proposed Scheme

In this section, we verify that the proposed algorithms (5)–(7) are consistent. For this, we apply the Taylor series expansion on S_n^{j+1}, S_{n+1}^j and S_{n-1}^j as follows:

$$S_n^{j+1} = S_n^j + \Delta t \frac{\partial S}{\partial t} + \frac{\Delta t^2}{2!} \frac{\partial^2 S}{\partial t^2} + \frac{\Delta t^3}{3!} \frac{\partial^3 S}{\partial t^3} + \cdots$$

$$S_{n+1}^j = S_n^j + \Delta x \frac{\partial S}{\partial x} + \frac{\Delta x^2}{2!} \frac{\partial^2 S}{\partial x^2} + \frac{\Delta x^3}{3!} \frac{\partial^3 S}{\partial x^3} + \cdots$$

$$S_{n-1}^j = S_n^j - \Delta x \frac{\partial S}{\partial x} + \frac{\Delta x^2}{2!} \frac{\partial^2 S}{\partial x^2} - \frac{\Delta x^3}{3!} \frac{\partial^3 S}{\partial x^3} + \cdots$$

First, we consider the finite difference approximation algorithm (4) for the consistency of the proposed numerical scheme,

$$S_n^{j+1} = S_n^j + R_1 \left(S_{n-1}^j + S_{n+1}^j \right) - 2R_1 S_n^{j+1} + \Delta t \mu - \Delta t \beta \left(L_n^j + B_n^j \right) S_n^{j+1}$$

$$- \Delta t \mu S_n^{j+1} + \alpha \Delta t (1 - S_n^j - L_n^j - B_n^j)$$

Inserting the values of S_n^{j+1}, S_{n+1}^j and S_{n-1}^j in the above equation and simplifying the expression we have,

$$\left(\frac{\partial S}{\partial t} + \frac{\Delta t}{2!} \frac{\partial^2 S}{\partial t^2} + \frac{\Delta t^2}{3!} \frac{\partial^3 S}{\partial t^3} + \cdots \right) \left(1 + \frac{d_S \Delta t}{\Delta x^2} + \Delta t \mu + \Delta t \beta \left(L_n^j + B_n^j \right) \right)$$

$$= 2 d_S \left(\frac{1}{2!} \frac{\partial^2 S}{\partial x^2} + \frac{\Delta x^2}{4!} \frac{\partial^4 S}{\partial x^4} + \cdots \right) + \mu - \beta \left(L_n^j + B_n^j \right) S_n^j - \mu S_n^j + \alpha (1 - S_n^j - L_n^j - B_n^j)$$

After inserting $\Delta t = \Delta x^3$ and $\Delta x \to 0$, the above equation coincides with (1). The similar procedure can be adopted to show that the finite difference approximation algorithms (6) and (7) are consistent.

6 Positivity of the Scheme

In this section, we present a result which shows that the proposed algorithm unconditionally retains the positivity of the computer virus model.

Theorem: The proposed algorithms (5)–(7) provide the positive solutions which are exhibited by the continuous system (1)–(3) under the non-negative initial functions ϕ_i, $i = 1, 2, 3$.

Proof: It is clear that the values $\phi_i \geq 0$, $\forall i \in \{1, 2, 3\}$ with $S + L + B \leq 1$. Also, no negative term is associated on the right hand side of algorithms (5)–(7). This proves the theorem.

7 Numerical Experiment

The following values of parameters [15,16] are used in numerical experiments.

7.1 Experiment 1

In the first experiment, the following initial conditions are supposed.

$$S(x, 0) = \begin{cases} 0.2x, & 0 \leq x < 0.5 \\ 0.2(1 - x), & 0.5 \leq x \leq 1 \end{cases}$$

$$L(x, 0) = \begin{cases} 0.4x, & 0 \leq x < 0.5 \\ 0.4(1 - x), & 0.5 \leq x \leq 1 \end{cases}$$

$$B(x, 0) = \begin{cases} 0.3x, & 0 \leq x < 0.5 \\ 0.3(1 - x), & 0.5 \leq x \leq 1 \end{cases}$$

From Fig. 1 it can be noticed that the maximum number of susceptible computers, latent computers, and infected computers are concentrated at the center of the domain value [0, 1] and decreases linearly to zero at the corners $x = 0$ and $x = 1$.
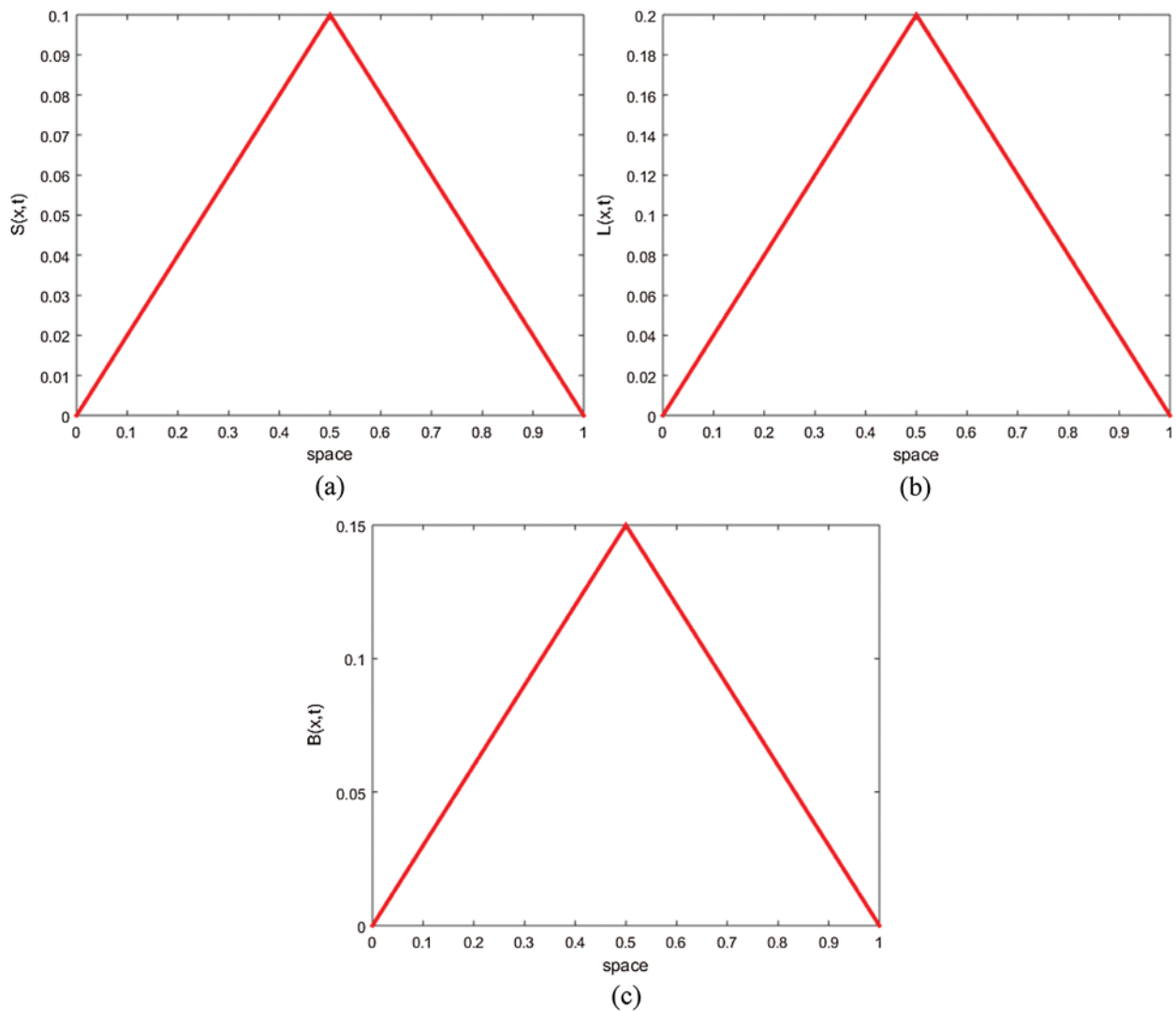
Figure 1: The initial dispersion of (a) susceptible computers, (b) latent computers and (c) breaking out computers

7.2 Disease Free Equilibrium

In this part, the graphical solutions of the proposed algorithm are examined against the parametric values taken in such a way that the value $\mathfrak{N}_{cv}$ is less than one i.e., virus free state.

In Fig. 2 we consider the values of the parameters describing VFS as mentioned in Tab. 1. The graphical representations reveal that the proposed algorithm demonstrates the positive behavior of the state variables S, L and B. Also, the algorithm under discussion attains the stability of VFS as these graphs converge to $(1, 0, 0)$.

Proposed FD Algorithm

(a)

Proposed FD Algorithm

(b)

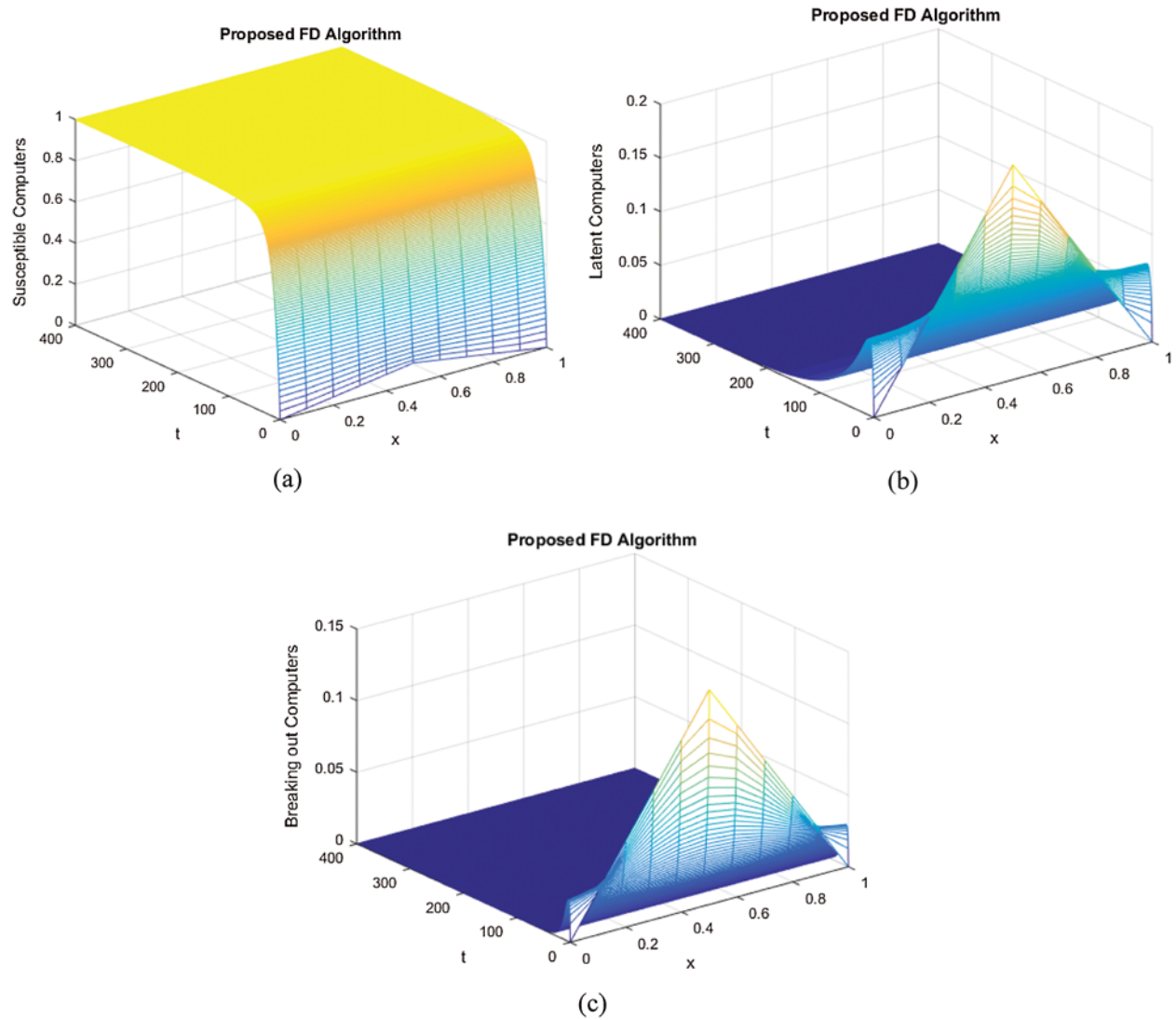**Proposed FD Algorithm**

(c)

Figure 2: The graphical representation of (a) susceptible class of computers, (b) latent class of computers, (c) breaking out class of computers

Table 1: Parameters values

Parameters	(Virus free state)	(Virus persisting state)
β	0.015	0.025
ϵ	0.002	0.03
γ	0.2	0.025
α	0.1	0.02
μ	0.05	0.01

7.3 Endemic Equilibrium

This section is devoted to perform the graphical solutions of the proposed algorithm against the values that make $\mathfrak{N}_{cv}$ is greater than one i.e., virus persistence state.

Fig. 3 elaborates the solution behavior of $S(x,t)$, $L(x,t)$ and $B(x,t)$ using designed algorithm for the state when virus exists in the computer population. Again, the computer simulations illustrate that the designed algorithm holds all the important properties of the SLBR model under discussion.
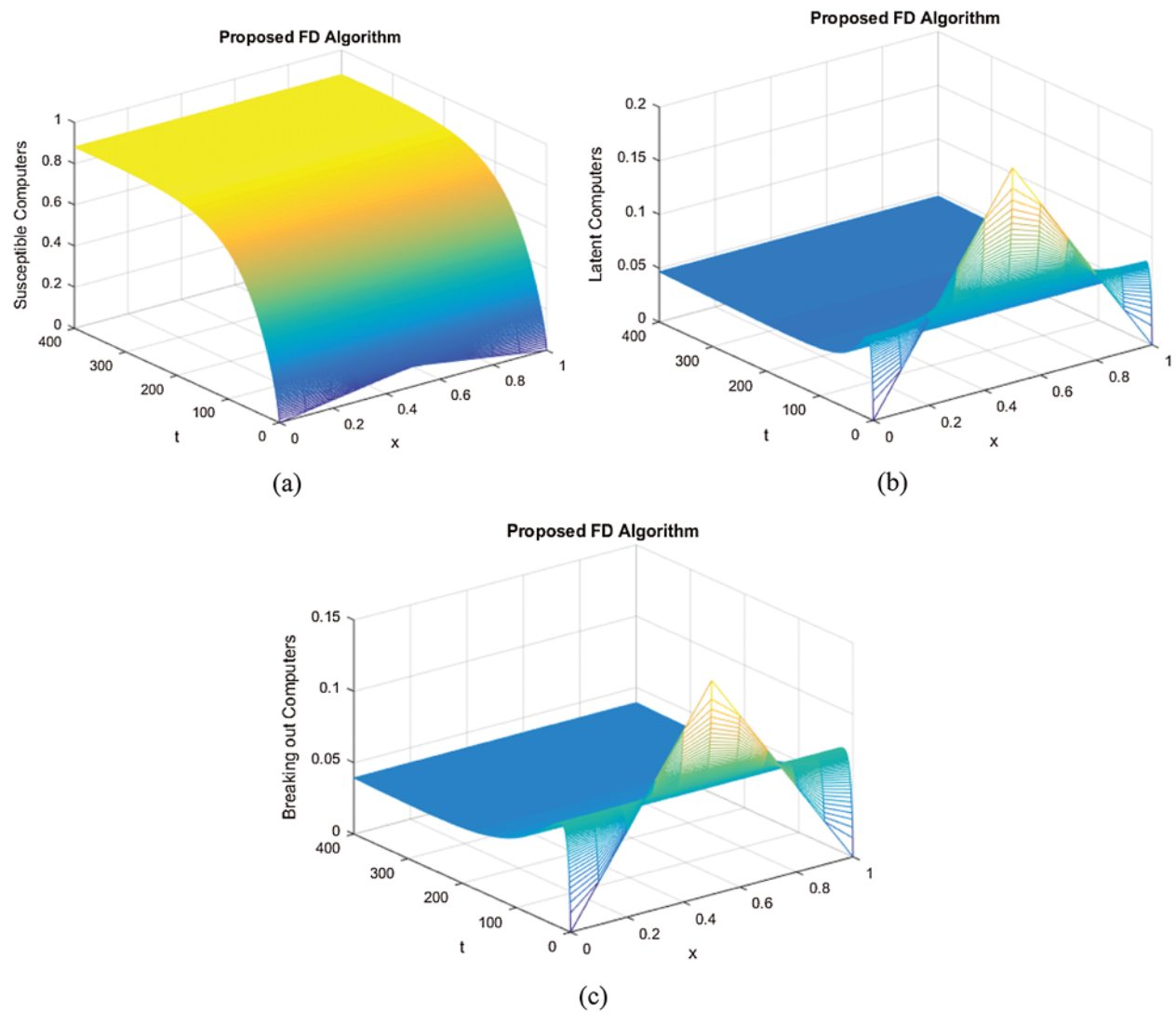

(a)

(b)

(c)

Figure 3: The graphical representation of (a) susceptible class of computers, (b) latent class of computers, (c) breaking out class of computers

8 Conclusion

The spatio-temporal computer virus epidemic model is proposed and studied, numerically. The algorithm proposed for the SLBR model is developed with the aid of the rules developed by Mickens. The consistency and the stability of the designed algorithm are confirmed with the Taylor series expansion and the Von Neumann criteria. The unknown variables of the SLBR model exhibit the computer population, so it is the basic property of the solutions to be positive. A theorem is presented which verifies that the underlying algorithm preserves positivity. The computer simulations demonstrate that the proposed numerical algorithm describes the consistent behavior with the continuous SLBR system. In the future, the current algorithm may be applied to solve the multidimensional reaction-diffusion systems. Furthermore, this numerical scheme may be applied to epidemic reaction-diffusion systems with time delay and predator-prey models with spatial content.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] U. Fatima, M. Ali, N. Ahmed and M. Rafiq, "Numerical modeling of susceptible latent breaking-out quarantine computer virus epidemic dynamics," *Heliyon*, vol. 4, no. 5, pp. 1–20, 2018.

[2] Z. Sun, L. Chen and Q. Chen, "A VEIS computer virus propagation model based on partly immunization," *Association of Computing Machinery*, vol. 34, no. 1, pp. 1–6, 2016.

[3] L. Yang, X. Yang, L. Wen and J. Liu, "A novel computer virus propagation model and its dynamics," *International Journal of Computer Mathematics*, vol. 89, no. 17, pp. 2307–2314, 2012.

[4] J. R. C. Piqueira and V. O. Araujo, "A modified epidemiological model for computer viruses," *Applied Mathematics and Computation*, vol. 213, no. 2, pp. 355–360, 2009.

[5] B. K. Mishra and N. Jha, "SEIQRS model for the transmission of malicious objects in computer network," *Applied Mathematical Modelling*, vol. 34, no. 3, pp. 710–715, 2010.

[6] J. Ren, X. Yang, L. X. Yang, Y. Xu and F. Yang, "A delayed computer virus propagation model and its dynamics," *Chaos Solitons & Fractals*, vol. 45, no. 1, pp. 74–79, 2012.

[7] Q. Zhu, X. Yang and J. Ren, "Modeling and analysis of the spread of computer virus," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 12, pp. 5117–5124, 2012.

[8] M. S. Arif, A. Raza, M. Rafiq, M. Bibi, J. N. Abbasi *et al.,* "Numerical simulations for stochastic computer virus propagation model," *Computers Materials and Continua*, vol. 62, no. 1, pp. 61–77, 2020.

[9] Z. Zhang and H. Yang, "Hopf bifurcation of an SIQR computer virus model with time delay," *Discrete Dynamics in Nature and Society*, vol. 12, no. 1, pp. 1–8, 2015.

[10] X. Han and Q. Tan, "Dynamical behavior of computer virus on internet," *Applied Mathematics and Computation*, vol. 217, no. 6, pp. 2520–2526, 2010.

[11] L. Billings, W. M. Spears and I. B. Schwartz, "A unified prediction of computer virus spread in connected networks," *Physics Letters A*, vol. 297, no. 4, pp. 261–266, 2002.

[12] J. C. Wierman and D. J. Marchette, "Modeling computer virus prevalence with a susceptible-infected-susceptible model with reintroduction," *Computational Statistics & Data Analysis*, vol. 45, no. 1, pp. 1–23, 2004.

[13] H. Yuan and G. Chen, "Network virus epidemic model with the point-to-group information propagation," *Applied Mathematics and Computation*, vol. 206, no. 1, pp. 357–367, 2008.

[14] C. Zhang, Y. Zhao and Y. Wu, "An impulse dynamic model for computer worms," *Abstract and Applied Analysis*, vol. 12, no. 2, pp. 1–8, 2015.

[15] M. Yang, Z. Zhang, Q. Li and G. Zhang, "An SLBRS model with vertical transmission of computer virus over the internet," *Discrete Dynamics in Nature and Society*, vol. 10, no. 1, pp. 1–17, 2012.

[16] M. S. Arif, A. Raza, W. Shatanawi, M. Rafiq and M. Bibi, "A stochastic numerical analysis for computer virus model with vertical transmission over the internet," *Computers Materials & Continua*, vol. 61, no. 3, pp. 1025–1043, 2019.

[17] S. Azam, J. E. M. Diaz, N. Ahmad, I. Khan, M. S. Iqbal *et al.,* "Numerical modeling and theoretical analysis of a nonlinear advection-reaction epidemic system," *Computer Methods and Programs in Biomedicine*, vol. 193, no. 3, pp. 1–19, 2020.

[18] J. E. M. Diaz, N. Ahmad and M. Rafiq, "Analysis and nonstandard numerical design of a discrete three-dimensional hepatitis B epidemic model," *Mathematics of Computation*, vol. 7, no. 12, pp. 1157–1167, 2019.

[19] N. Ahmad, M. Rafiq, D. Baleanu and M. A. Rehman, "Spatio-temporal numerical modeling of auto-catalytic brusselator model," *Romanian Journal of Physics*, vol. 64, no. 110, pp. 1–19, 2018.

[20] Z. Iqbal, N. Ahmad, D. Baleanu, M. Rafiq, M. S. Iqbal *et al.,* "Structure preserving computational technique for fractional order schnakenberg model," *Computational and Applied Mathematics*, vol. 39, no. 61, pp. 1–19, 2020.

[21] N. Shahid, N. Ahmad, D. Baleanu, A. S. Alshomrani, M. S. Iqbal *et al.,* "Novel numerical analysis for nonlinear advection reaction diffusion systems," *Open Physics*, vol. 18, no. 1, pp. 112–125, 2020.

[22] R. E. Mickens, "A fundamental principle for constructing non-standard finite difference schemes for differential equations," *Journal of Difference Equations and Applications*, vol. 11, no. 2, pp. 645–653, 2005.