Journal of Innovative Technology, Vol. 7, No. 1, pp. 33-49, March 2025
http://doi.org/10.29424/JIT.202503_7(1).0004

Expedition of deterministic numerical solvers for computer virus spread: Explicit Runge-Kutta and backward differential methods

Kiran Asma [1], Muhammad Asif Zahoor Raja [2*], Chuan-Yu Chang [3]

ABSTRACT

In this paper, advanced computing techniques are exploited for the numerical implementation of a system of ordinary differential equations (ODEs) representing the computer virus spread (CVS) model with Explicit Runge-Kutta (ERK) and Backward Differential Formula (BDF). The findings achieved by both numerical experimentations, are compared to solve the dynamics of nonlinear epidemiological model of CVS. Specifically, this scheme of study uses the NDSolve function to numerically solve the system over a specified time interval, reflecting three differential compartments observed as the state transformation of susceptible, infected and recovered computer systems in a network. The dynamics of the CVS model are studied with different scenarios for several cases by utilizing both ERK and BDF numerical solution and the accuracy of numerical results is established by absolute error (AE) plots to demonstrate the significance of the algorithms for solving mathematical models of epidemiological CVS. By exploiting the robustness of ERK and BDF methods, the proposed approximate technique generates accurate and efficient numerical solutions, enabling comprehensive analysis of virus propagation patterns. Through extensive simulations, the proposed technique exhibits the accuracy of the methodology that represent the complicated dynamics of computer virus spread and produce applaud understanding of efficacious mitigation approaches. This scheme of study strengthens the field of computational epidemiology and contributes to the development of vigorous cybersecurity techniques that are effective of addressing the evolving challenges constitute by digital pathogens.

Keywords: Computer virus propagation NDSolve function Explicit Runge-Kutta method Backward Differentiation Formula method computational epidemiology

1. INTRODUCTION

The computerization revolution has substantially enhanced the everyday life services like online banking, e-commerce, entertainment, travelling arrangement, online business and other enterprise resources planning related events but this information technology development has also caused the uneconomic manoeuvres and unproductive operations through spread of computer viruses. In the modern digital era, computer viruses cause a consequential threat to cybersecurity, conceivable disrupting systems, compromising sensitive data, and lead to substantial financial losses. To attenuate these risks, it is critical to flourish exact models that represent the behaviour of computer viruses and prognosticate their propagation dynamics. Computer virus is a malicious mobile code or software that is replicate itself and it also cause crushes the data and corrupts the system and files certainly. Some computer viruses include Sasser, DarkMe Malware, Water Hydra, CVE-2024-1709, Trojan horses, CVE-2024-1708, and CVE-2023-22527 etc [1].

The virus does not only damage the compromised system but also spread into the whole network and disturbs all the systems connected to the network. The consequences in damage of data, displacement of files and abnormal activities of system like hanged and restart again and again without user command. The conception of computational frameworks to study the computer virus dynamics became initiated in early eighties. The conception of epidemic models for computer virus has been commenced since 1988[2]. An epidemic is a strangely large or short-term eruption of a transmissible disease in epidemiology. If a virus continues to spread in a population, then it is called endemic. The growth of an infectious disease is affected not only by disease-specific dynamics like infection rates, susceptibility, resistance, transmission modes, and latency periods but also by economic, social, cultural, and geographic factors. A computer virus activates in a network has a significant number of resemblances with the propagation of an infectious disease in a populated area [3]. In the context of computer virus, a huge collection of computer virus propagation model has been resented in last decade, such as SIR model, SEIR model, SIRS model and SEIRS model, these models have also been represented in the mathematical structures to investigates the dynamics of computer virus spread in network topologies [4-6]. A UPD model was investigated to portray the patch propagation network layer and patch distribution in multiplex networks [7,8]. Another SIV model was used to define the computer virus propagation network layer, which structure a network model of a multiplexed

Manuscript received September 14, 2024; revised November 7, 2024; accepted November 21, 2024.

1 Ph.D. Student, Department of Data Science and AI Applications, Graduate School of Engineering Science and Technology, National Yunlin University of Science and Technology, Taiwan.

2* Professor (corresponding author), Department of Data Science and AI Applications, Graduate School of Engineering Science and Technology, National Yunlin University of Science and Technology, Taiwan. (email: rajamaz@yuntech.edu.tw)

3 Professor, Department of Computer Science and Information Engineering, National Yunlin University of Science and Technology, Taiwan.

network [9].

An automated hubs-patching model with the dynamics of patching exceedingly connected nodes (hubs) as a precautionary measure against malware spreading through the Internet and removable storage devices was presented and the related optimal control was achieved [10]. BK. Mishra have researched several mathematical models on computer viruses, recently SIR model is studied for transmission dynamics of malware in networks using caputo fractional order derivative [11]. Haar wavelet collocation methods of fractional-order antidotal modelling of the computer virus propagation have also been modelled by researchers This modelling demonstrates the interactivity among computers and removable devices [12]. Researchers have also been investigated the dynamics of fractional order computer virus propagation mathematical model with kill signals. In this study the KS received alerts about viruses which can be infecting the computer system, to minimum the virus propagation vulnerability [13]. A computer virus propagation model introduce that is based on the limitation of resources. This research considers the constrained accessibility of resources in the perspective of computer virus prevention and control [14]. A SLBRS virus propagation model is widely investigated in the domain of computer virus propagation like complex networks, optimal control with recovery rate and safety entropy [15-18]. Some scholars have performed the control of Turing instability and bifurcation for spatial-temporal propagation of computer virus [19].

An epidemiological SIRA model is also utilized by several scholars in the field of computer virus propagation, it has been investigated through operational matrix methodology. The model has also studied with stealth viruses and antivirus renewal in a network with fast infectors. SIRA model has developed for mortality and robustness in the context of computer virus propagation and investigated in Bluetooth virus propagation in real map by using infectious attenuation algorithm [20-23]. Recently some researchers studied the computer virus propagation and control of computer virus by multimedia technology [24]. The fractional order modelling of epidemiological computer virus propagation model by using fibonacci wavelets is a unique technique of exploring the computer virus [25]. In the modern era artificial intelligence (AI) play its vital roll in every field of our life. Artificial intelligence technology has important application benefits in cyberspace security, in the domain of the Internet and system security. By implementing self-directed learning and pattern recognition it improves threat detection, risk assessment and defense strategies. Artificial intelligence technology has played an important technical support role in firewalls and computer security monitoring [26-29]. So, research community has shown their deep interest in the study of dynamics of computer virus by using AI techniques. Recently scholars research on virus propagation network intrusion detection based on graph neural network [30]. The cybersecurity is also enhanced by utilizing the AI predictive techniques [31]. The SEIRQ model is also investigated by using artificial neural networks-based technique for complex networks [31,32].

All the above-mentioned models have been investigated for computer virus spread (CVS) with different techniques and methodologies. In this paper, we implement the SIR model [33] by utilizing the explicit Runge-Kutta (ERK) and BDF methods. The ERK method, acknowledged for their accuracy and robustness, are employed to tackle computer virus spread. These methodologies contain discretising the ODEs and iteratively computing the system state at successive time periods. The ERK method have impressive capability to handle the high nonlinearity and dimensionality built-in in virus propagation models and deliver consistent and precise solutions [34-36]. The proposed methodology developed a better understanding of how the number of SIR computers evolve over time. All these aspects are the motivation to designate this methodology for implementation. Based on a system of three ODEs , this research demonstrates advanced application of ERK and BDF methods to solve the nonlinear compartment model of computer virus spread (CVS). Both methods are compared in terms of absolute error (AE) to evaluate their effectiveness, accuracy and robustness. The effectiveness of ERK and BDF methods in solving the complicated dynamics of computer virus spread is proved through extensive numerical experiments and simulations. The analysis incorporates comprehensive evaluations of the dynamics of susceptible, infected, and recovered nodes, underscoring their variations.

The rest of the paper is constituted in the following manner: the Section 2 discusses the mathematical representation of computer virus propagation model. Section 3 describes the designed methodology (ERK and BDF methods computing procedure for numerical solutions). Section 4 discuss the results and discussion; Section 5 includes concluding remarks and Section 6 discuss the future directions.

2. SYSTEM MODEL: COMPUTER VIRUS SPREAD MODEL

In this section, the epidemiological inspired design of nonlinear computer virus spread model is exhibited. The state transformation of nonlinear epidemiological model of computer virus

$$\frac{dS}{dt} = b - \beta SI - \mu S, \qquad S(0) = S_0 \tag{1}$$

$$\frac{dI}{dt} = \beta sI - (Y + k)l \qquad I(0) = I_0 \tag{2}$$

$$\frac{dR}{dt} = \gamma I - \mu R \qquad R(0) = R_0 \tag{3}$$

spread (CVS) is shown in Fig.1, represented with three differential compartments via susceptible S, infected I and recover R, i.e., (SIR) computers as follows [33]. The SIR model is an extensively used mathematical model in epidemiology to demonstrate the spread of computer virus. The dynamics of these three differential compartments are observed by the variations in β (contact rate of susceptible computers to infected computers), γ (rate of recovery due to antivirus treatment), b (rate of external computers connected to the network) and μ (rate of removal of computer from the network)., while the constants S0, I0, and R0 represents the initial conditions of CVS.

Transformation of states in Figure.1 is showing the flow of computer systems between three compartments, susceptible computers become infected and infected computers become recovered computers in the network.

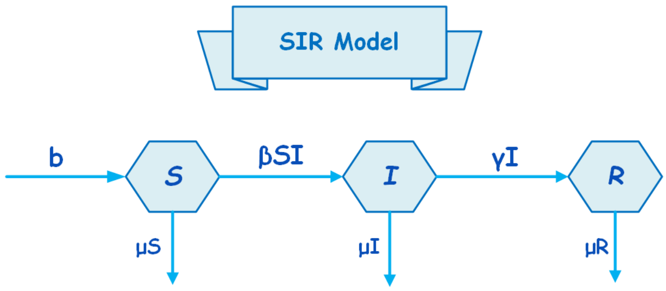


Fig. 1 State transition dynamics of computer virus spread (CVS) model.

The CVS model described in equations (1-3) is solved for four scenarios and cases as presented in Table.1 with variables and fixed parameters.

3. DESIGN METHODOLOGY

The methodology employed in this scheme of study for solving nonlinear SIR (Susceptible, Infected, Recovered) computer virus spread model is explane in Figure. 2, that shows the step by step flow structures of the process. The proposed schemeof study consists of two steps. In the first step, the numerical solution for nonlinear CVS using ERK and BDF methods is demostrated. In the second step, the numerical solutions attain from ERK and BDF methods are compared with reference values by computing the absolute errors to approximate the solution.

This workflow scheme can significantly summarise the proposed research by illustrating the transition from an initial secure state to a compromised state, modelling the computer virus spread, solving the model numerically with proposed methodology, and evaluating the accuracy of these solutions by computing absolute error. This underscores the importance of modelling computer virus spread to improve cybersecurity measures.

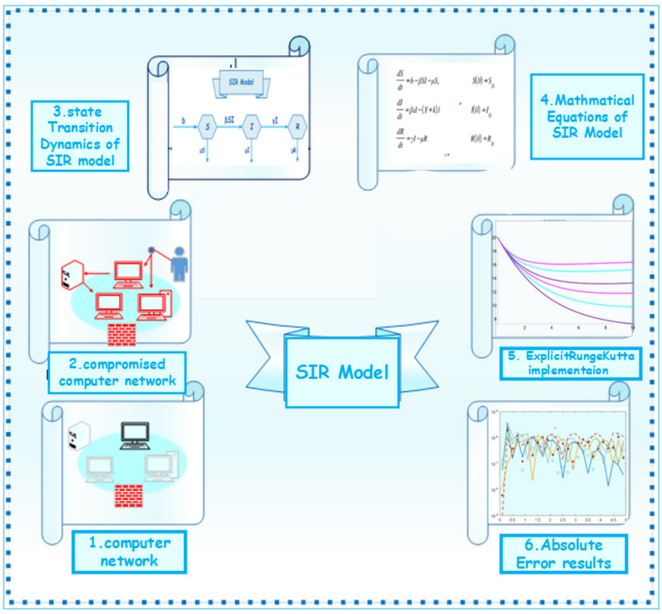


Fig. 2 Workflow scheme of nonlinear SIR computer virus spread model

4. Simulation and Results

The proposed scheme of study exploits the NDSolve function in Mathematica to numerically execute the system over a specified time interval, signifying three differential compartments S(t), I(t) and R(t) (susceptible, infected and recovered computers). The results of numerical experiments are demonstrated here by implementing the proposed design methodology for solving nonlinear CVS model given in equations (1) to (3) for four scenarios based on variations in β (contact rate of susceptible computers to infected computers), γ (rate of recovery due to antivirus treatment), b (rate of external computers connected to the network) and μ (rate of removal of computer from the network). The dynamics of CVS model are computed for four scenarios and six cases of each scenario, and these are stated in Table.1 for the fluctuating parameters and the constant values of S0=20, I0 =18, and R0 =16 represent the initial conditions for solving CVS model.

Table 1 Scenarios and Cases for SIR computer virus spread (CVS) model

Scenarios	Cases	Parameter of interest				Remarks
		b	β	μ	γ	
1	1	0.1	0.01	0.02	0.2	Constant initial values: S_0, I_0, R_0 = {20, 18, 16}
	2	0.3	0.01	0.02	0.2	
	3	0.4	0.01	0.02	0.2	
	4	0.5	0.01	0.02	0.2	
	5	0.7	0.01	0.02	0.2	
	6	0.9	0.01	0.02	0.2	
2	1	0.4	0.01	0.02	0.2	
	2	0.4	0.02	0.02	0.2	
	3	0.4	0.03	0.02	0.2	
	4	0.4	0.04	0.02	0.2	
	5	0.4	0.05	0.02	0.2	
	6	0.4	0.06	0.02	0.2	
3	1	0.4	0.01	0.02	0.2	
	2	0.4	0.01	0.03	0.2	
	3	0.4	0.01	0.04	0.2	
	4	0.4	0.01	0.05	0.2	
	5	0.4	0.01	0.07	0.2	
	6	0.4	0.01	0.09	0.2	
4	1	0.4	0.01	0.02	0.2	
	2	0.4	0.01	0.02	0.3	
	3	0.4	0.01	0.02	0.4	
	4	0.4	0.01	0.02	0.5	
	5	0.4	0.01	0.02	0.7	
	6	0.4	0.01	0.02	0.9	

Scenario 1: Scrutinize the dynamics of nonlinear computer virus spread model (1-3) for different values of b (variations in rate of external computers connected to the network).

Scenario 2: Scrutinize the dynamics of nonlinear computer virus spread model (1-3) for different values of β (variations in contact rate of susceptible computers to infected computers).

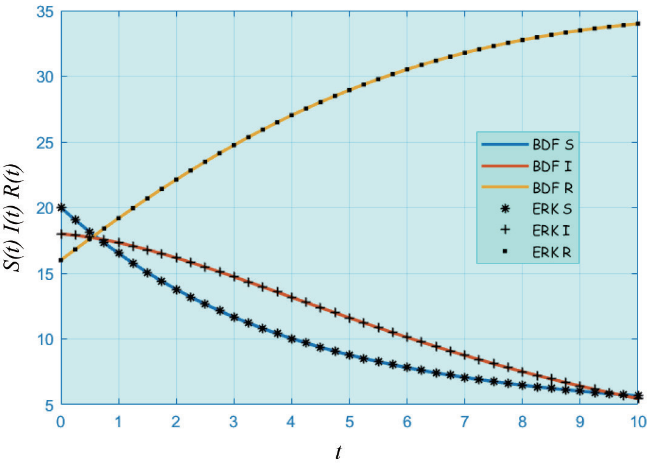
Scenario 3: Scrutinize the dynamics of nonlinear computer virus spread model (1-3) for different values of μ (variations in rate of removal of computer from the network).

Scenario 4: Scrutinize the dynamics of nonlinear computer virus spread model (1-3) for different values of γ (variations in rate of recovery due to antivirus treatment).

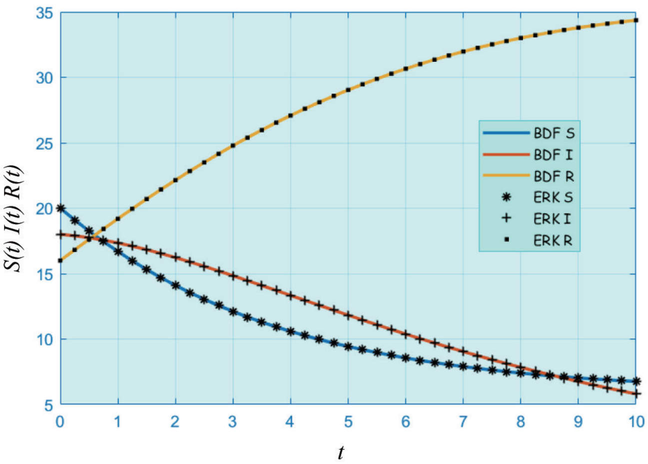
The results of numerical experiments along with a detailed explanation of the proposed methodology exhibited for the dynamics of epidemiological nonlinear CVS model. This investigation consists of four scenarios by varying b, β, μ and γ respectively, for all scenarios, reference datasets for $S(t)$, $I(t)$, and $R(t)$ are established by using the ERK and BDF methods with a step size of 0.25 with final point on 10.

Fig. 3 portrayed the numerical results of ERK and BDF methods for the solution *S(t)* of nonlinear epidemiological system for CVS for all six cases *b*=0.1 subfigure-3a, *b*=0.3 subfigure-3b, *b*=0.4 subfigure-3c, *b*=0.5 subfigure-3d, *b*=0.7 subfigure-3e and *b*=0.9 subfigure-3f of scenario 1. To achieve the accuracy of the ERK and BDF methods the scrutiny on AE is directed and results are plotted in Fig. 4 for all the cases of nonlinear CVS model for six variations of *b*. The range of AE found 10^{-07} to 10^{-05} for b = 0.1 subfigure-4a, 10^{-08} to 10^{-05} for b = 0.3 subfigure-4b, 10^{-07} to 10^{-05} for b = 0.4 subfigure-4c, 10^{-07} to 10^{-05} for b= 0.5 subfigure- 4d, 10^{-07} to 10^{-05} for b = 0.7 subfigure-4e and 10^{-08} to 10^{-05} for b = 0.9 subfigure-4f. It may observe a close matched is consistently achieved by ERK and BDF scheme for scenario 1 of CVS model. Fig. 5 displays the computational dynamics of the BDF method for the *S(t)*, *I(t)*, and *R(t)* compartments in a nonlinear CVS model through six different cases in Scenario 1. The plotted results presents that the susceptible computers decrease over time subfigure-5a, the number of infected computers is increases initially and then decreases with time subfigure- 5b, and the number of recovered computers increases gradually over time subfigure-5c. This information is important for understanding the dynamics of computer viruses spread in a network. Fig.6 demonstrates the computing dynamics of the ERK method for the three compartments *S(t)*, *I(t)*, and *R(t)* of nonlinear CVS model across six different cases in Scenario 1. The fig. 06 illustrates that, the number of susceptible computers decreases gradually for all cases as time progresses, it directs the spread of the virus in a network subfigure-6a. The number of infected computers increases first and reaches a peak, then decreases with passage of time, indicating the infection progression and eventual control subfigure-6b. The number of recovered computers increases over time, indicating the removal and recovery of the infection from the network subfigure-6c. It efficiently shows how the ERK method is exploited to simulate the spread of a computer virus over time within a network. For each susceptible, infected, and recovered compartment, the behaviour over time is plotted for six cases.

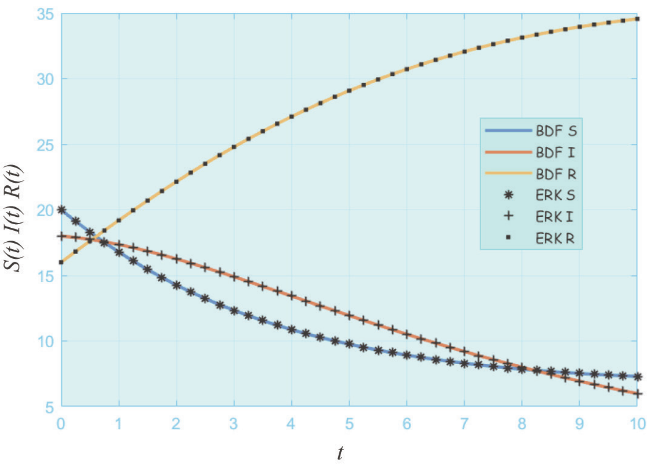
Fig.7 portrayed the outcomes of ERK and BDF methods for the solution *S(t)* of nonlinear epidemiological system for CVS for all six cases *β*=0.01 subfigure-7a, *β*=0.02 subfigure-7b, *β*=0.03 subfigure-7c, *β*=0.04 subfigure-7d, *β*=0.05 subfigure-7e and *β*=0.06 subfigure-7f of scenario 2. To attain the accuracy of the ERK and BDF methods, the scrutiny on AE is directed and results are plotted in Fig.8 for all the cases of nonlinear CVS model for six variations of β. The range of AE found 10^{-07} to 10^{-05} for *β*=0.01 subfigure-8a, 10^{-07} to 10^{-04} for *β*=0.02 subfigure-8b, 10^{-07} to 10^{-03} for *β*=0.03 subfigure-8c, 10^{-07} to 10^{-03} for *β*=0.04 subfigure-8d, 10^{-07} to 10^{-03} for *β*=0.05 subfigure- 8e and 10^{-07} to 10^{-02} for *β*=0.06 subfigure- 8f. It may observe a close matched is consistently achieved by ERK and BDF scheme for scenario 2 of CVS model. Fig. 9 displays the computational dynamics of the BDF method for the *S(t)*, *I(t)*, and *R(t)* compartments in a nonlinear CVS model through six different cases in scenario 2. The plotted results presents that susceptible computers decreases over time subfigure-9a, the number of infected computers is increases initially and then decreases with time subfigure-9b, and the number of recovered computers increases gradually over time subfigure- 9c. This information is important for understanding the dynamics of computer virus spread in a network. Fig.10 demonstrates the computing dynamics of the ERK method for the three compartments *S(t)*, *I(t)*, and *R(t)* of nonlinear computer virus spread (CVS) model across six different cases in scenario 2. The fig.10 illustrates that, the number of susceptible computers decreases gradually for all cases as time progresses, it directs the spread of the virus in a network subfigure-10a. The number of infected computers increases first and reaches a peak, then decreases with passage of time, indicating the infection progression and eventual control subfigure- 10b. The number of recovered computers increases over time, indicating the removal and recovery of the infection from the network subfigure- 10c. It efficiently shows how the ERK method is exploited to simulate the spread of a computer virus over time within a network. For each susceptible, infected, and recovered compartment, the behaviour over time is plotted for six cases.



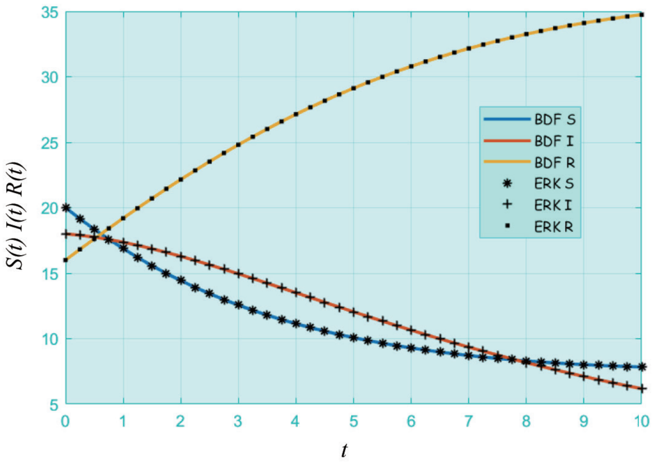
(a) Solution dynamics for *b*=0.1



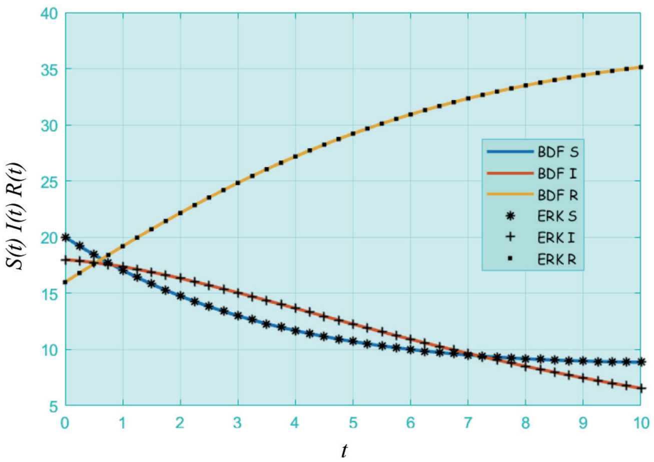
(b) Solution dynamics for *b*=0.3



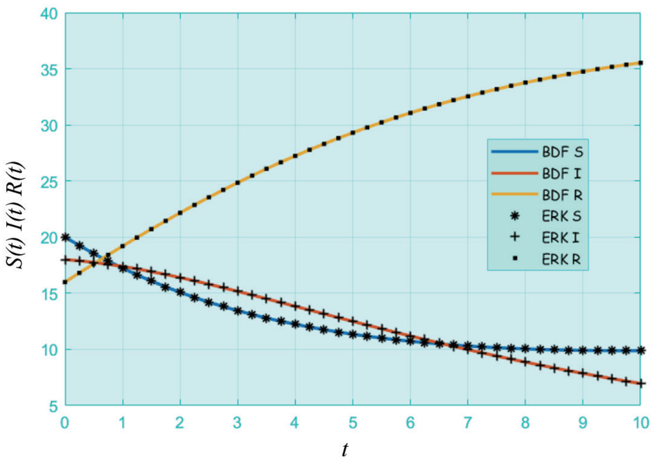
(c) Solution dynamics for *b*=0.4



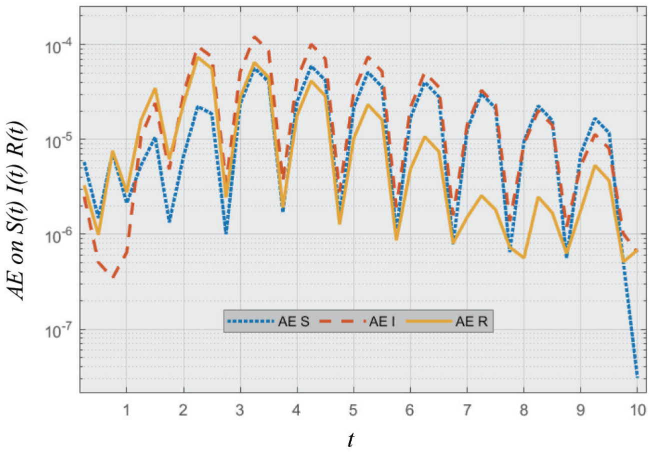
(d) Solution dynamics for b=0.5



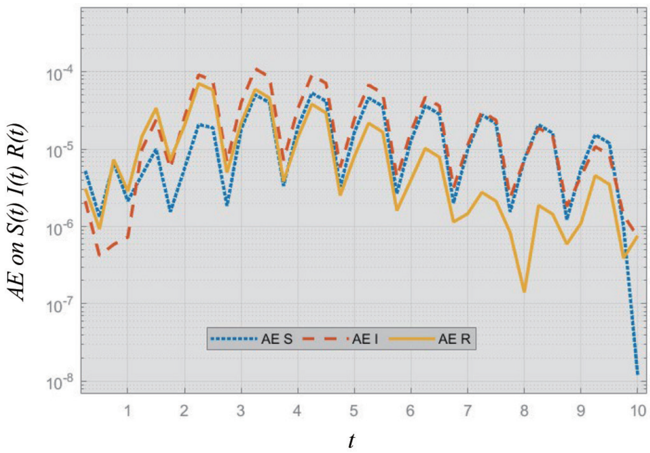
(e) Solution dynamics for b=0.7



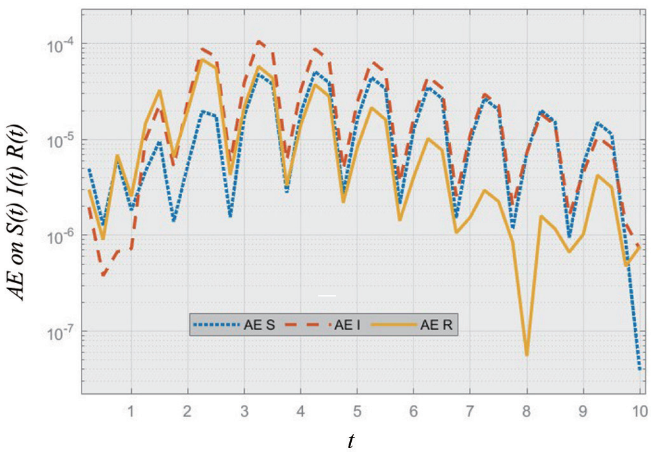
(f) Solution dynamics for b=0.9



(a) AE for b=0.1

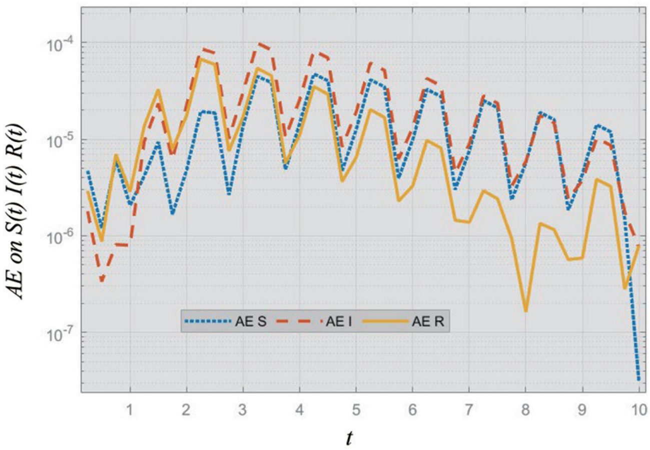


(b) AE for b=0.3

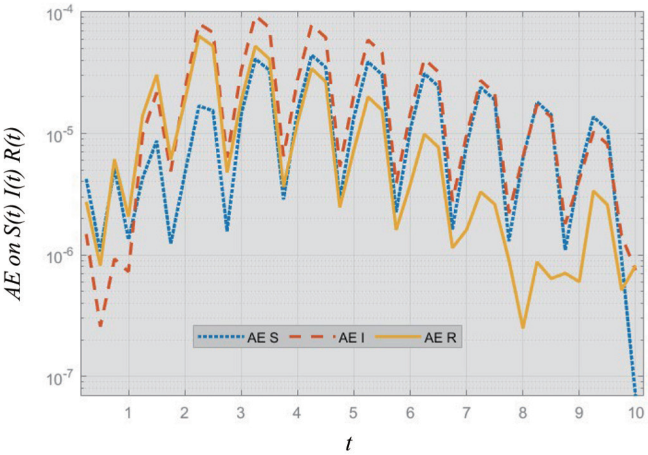


(c) AE for b=0.4

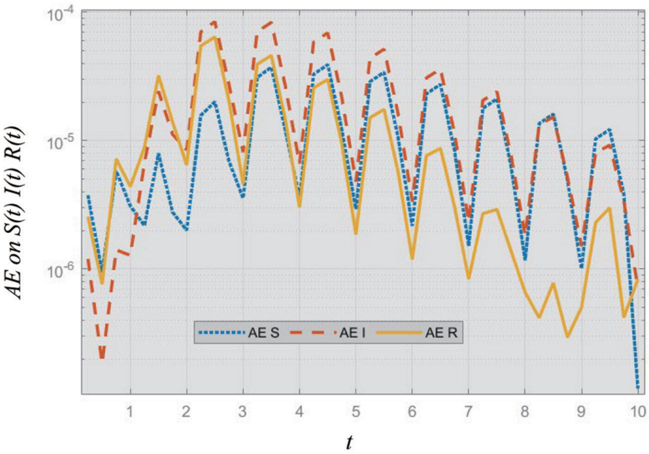
Fig. 3 The solution dynamics of ERK and BDF methods for the nonlinear SIR model for all six cases of scenario 1



(d) AE for b=0.5

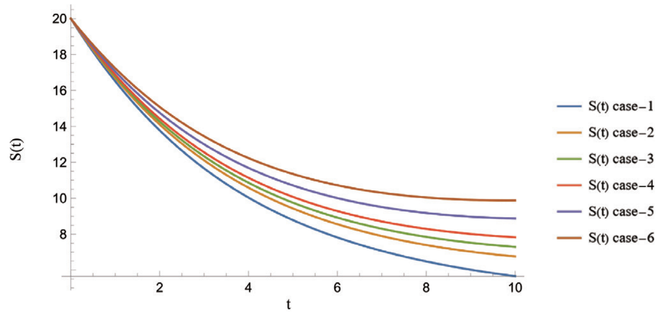


(e) AE for b=0.7

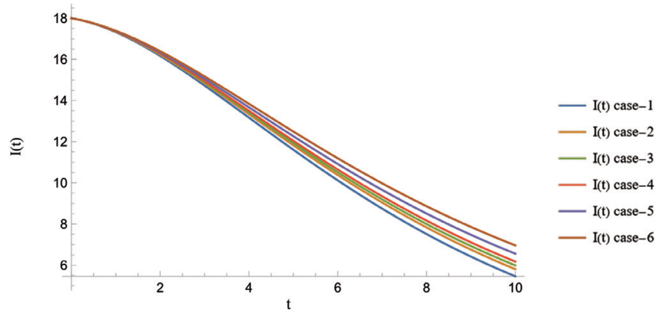


(f) AE for b=0.9

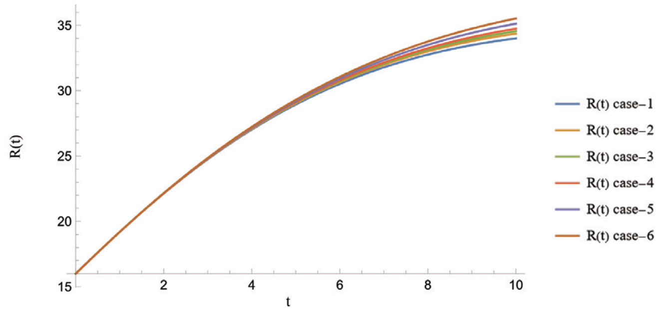
Fig. 4 Comparison on AE for ERK and BDF for nonlinear CVS model across all six cases of the scenario 1



(a) S(t) for Scenario 1 (cases 1-6)

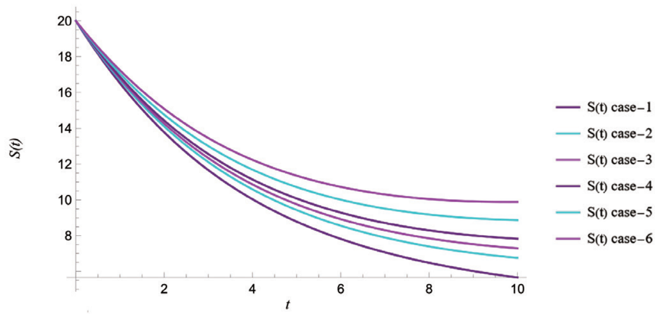


(b) I(t) for** Scenario **1 (cases 1-6)

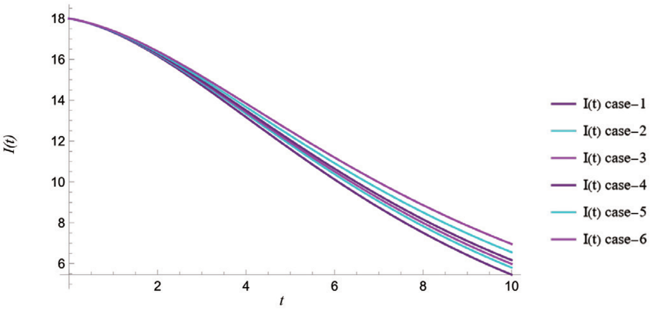


(c) R(t) for** Scenario **1 (cases 1-6)

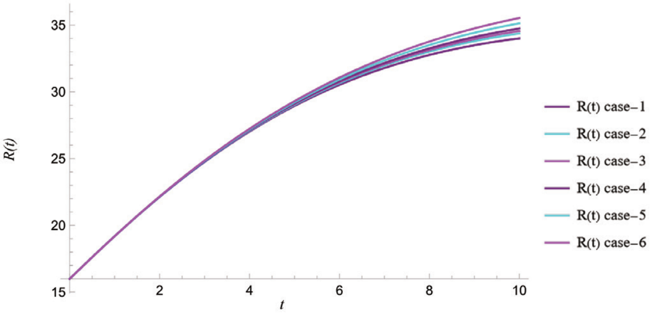
Fig. 5 The computing dynamics of the BDF method for the *S(t)*, *I(t)* and *R(t)* compartments in the nonlinear CVS model across all six cases of Scenario 1.



(a) S(t) for Scenario 1 (case 1-6)

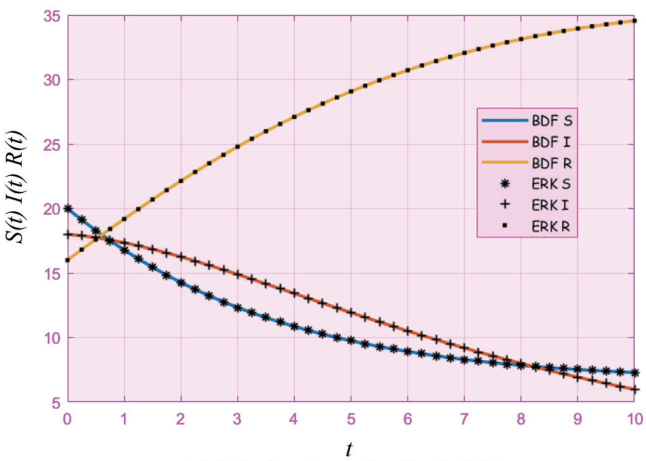


(b) I(t) for** Scenario **1(cases 1-6)

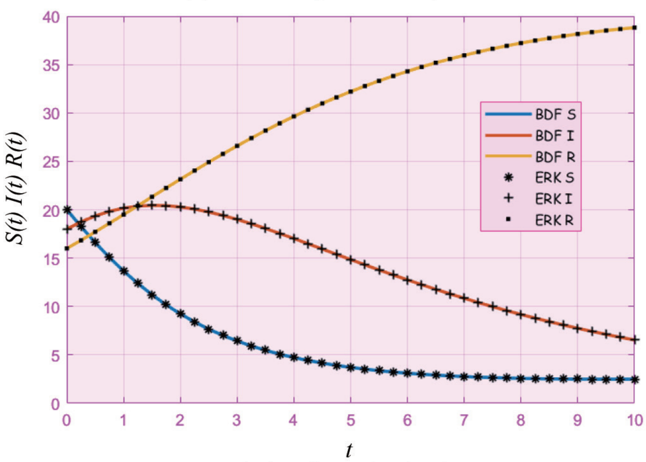


(c) *R(t) for* *Scenario* ***1 case 1-6***

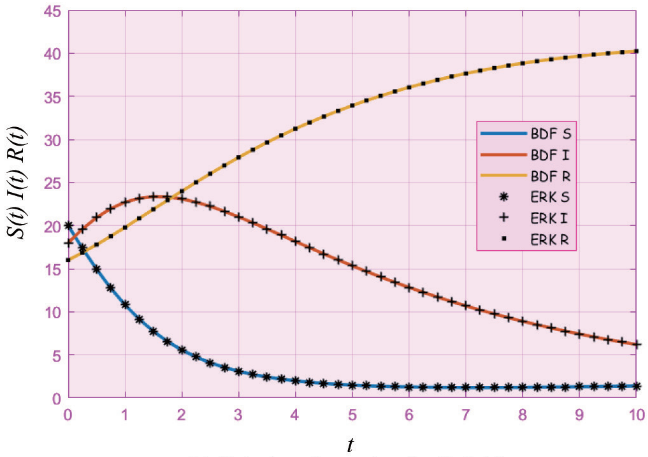
Fig. 6 The computing dynamics of the ERK method for the S*(t)*, *I(t)* and *R(t)* compartments in the nonlinear CVS model across all six cases of Scenario 1.



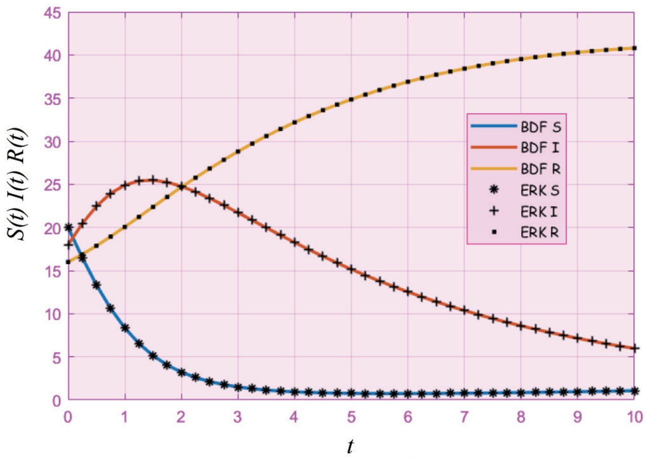
(a) Solution dynamics for β=0.01



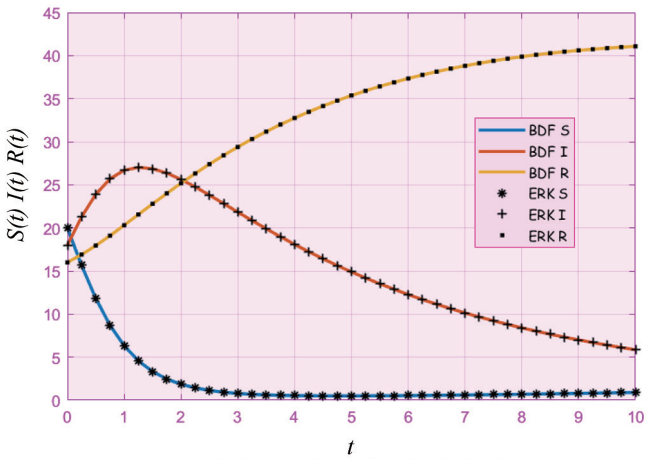
(b) Solution dynamics for β=0.02



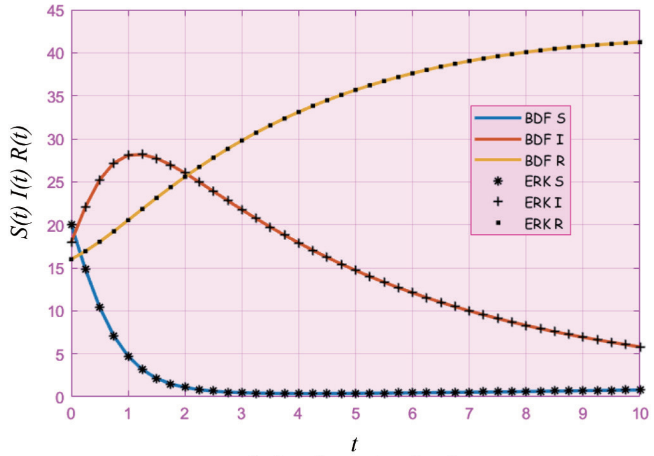
(c) Solution dynamics for β=0.03



(d) Solution dynamics for β=0.04

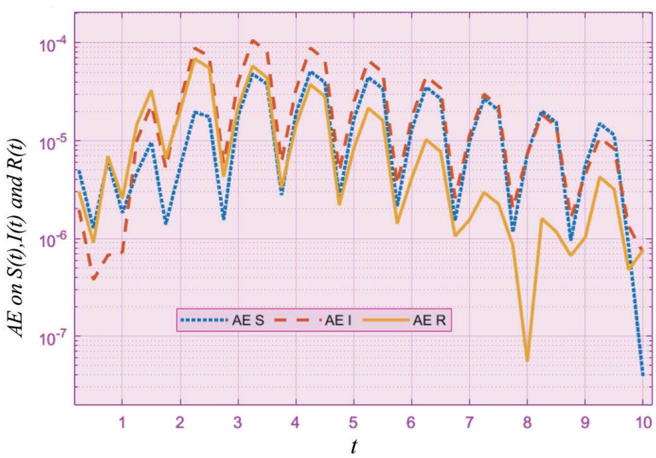


(e) Solution dynamics for β=0.05

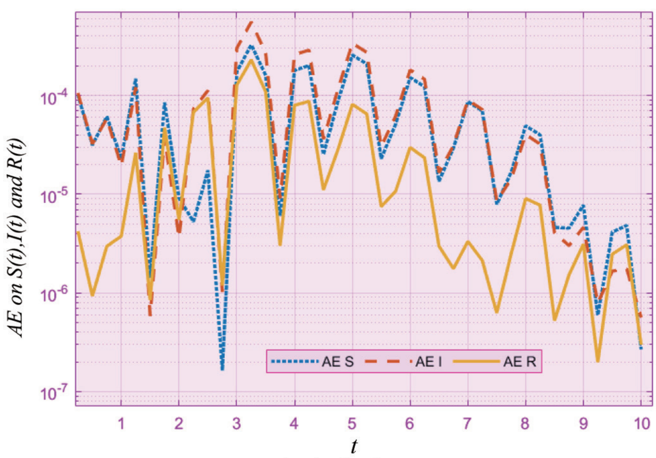


(f) Solution dynamics for β=0.06

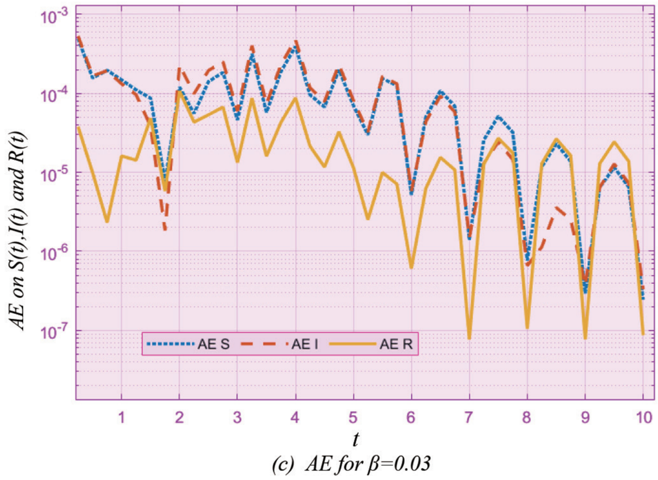
Fig. 7 The solution dynamics of ERK and BDF methods for the nonlinear SIR model across all six cases of scenario 2



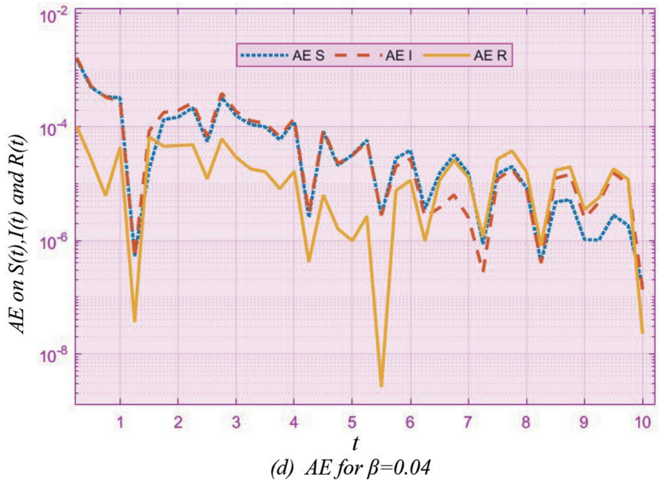
(a) AE for β=0.01



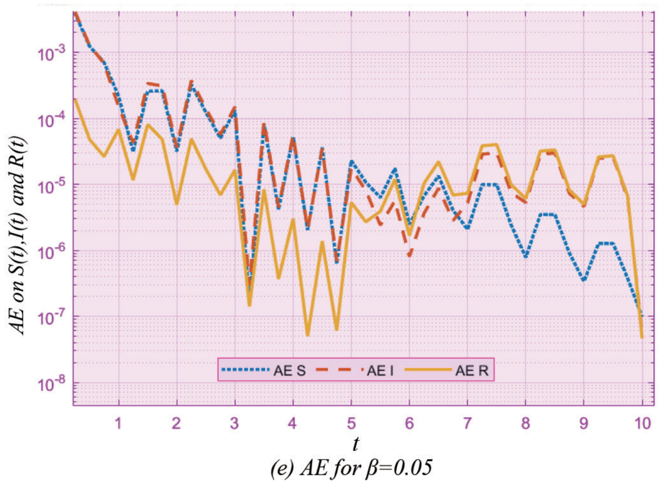
(b) AE for β=0.02



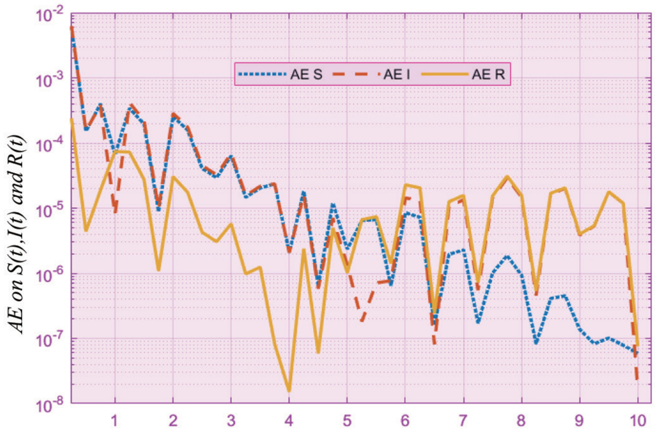
(c) AE for β=0.03



(d) AE for β=0.04



(e) AE for β=0.05



(f) AE for β=0.06

Fig. 8 Comparison on AE for ERK and BDF for nonlinear CVS model across all six cases of the scenario 2

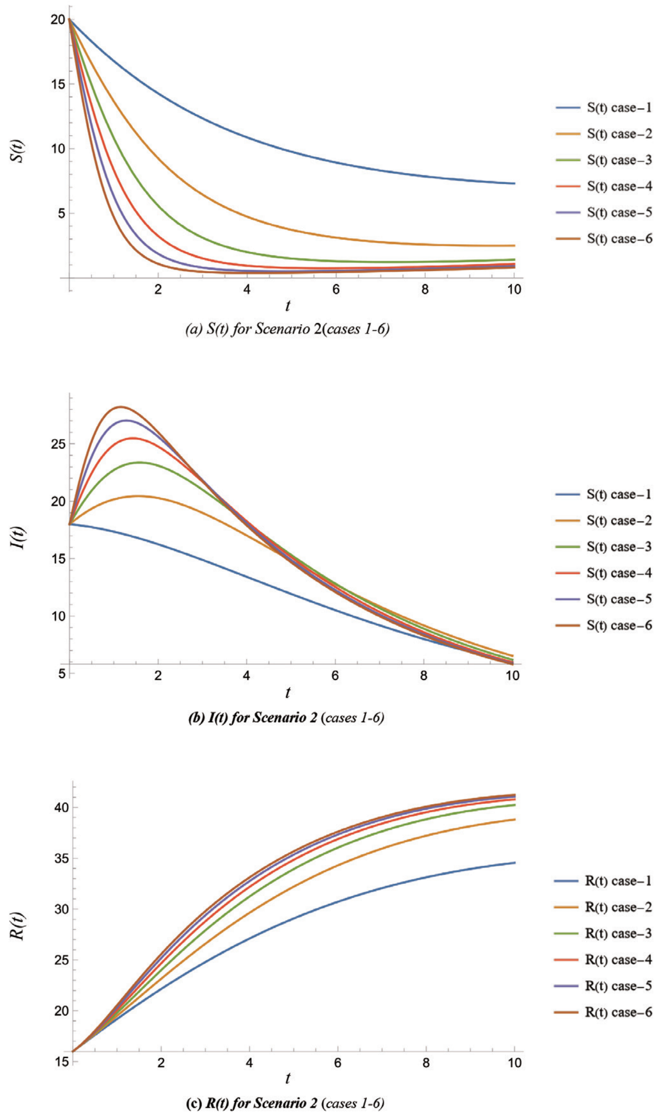


Fig. 9 The computing dynamics of the BDF method for the *S(t)*, I(t) and *R(t)* compartments in the nonlinear CVS model across all six cases of Scenario 2.

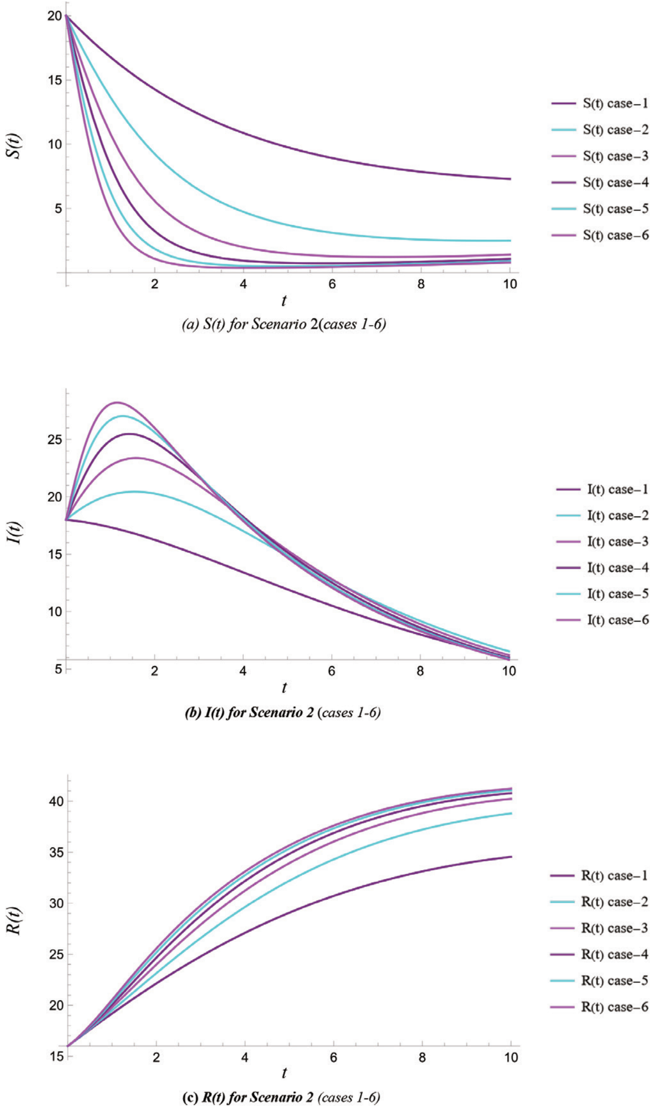
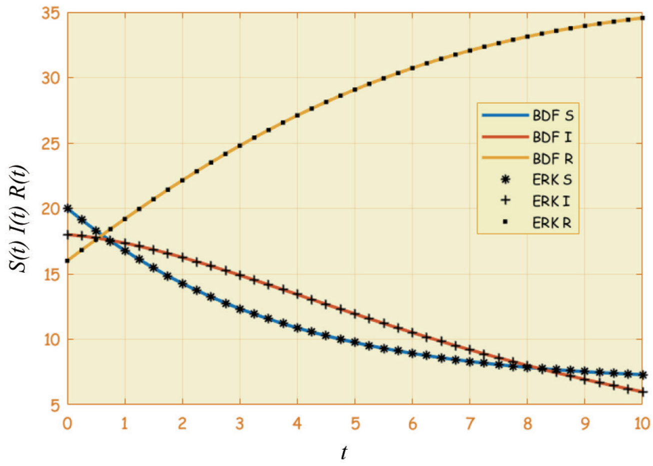


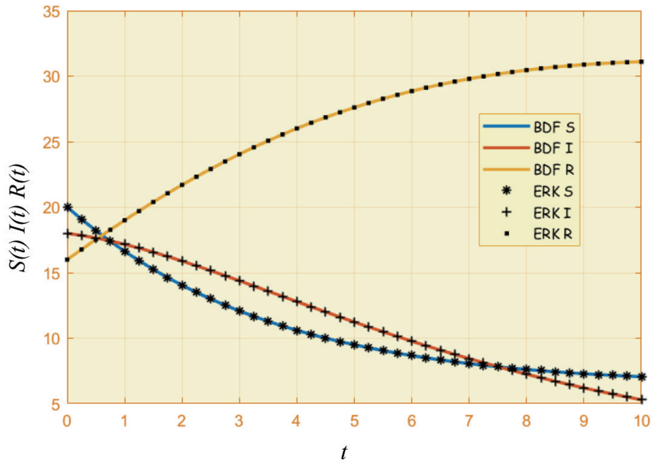
Fig. 10 The computing dynamics of the ERK method for the *S(t)*, *I(t)* and *R(t)* compartments in the nonlinear CVS model across all six cases of Scenario 2.

Fig. 11 portrayed the outcomes of ERK and BDF methods for the solution *S(t)* of nonlinear epidemiological system for CVS for all six cases μ=0.02 subfigure-11a, μ=0.03 subfigure-11b, μ=0.04 subfigure-11c, μ=0.05 subfigure-11d, μ=0.07 subfigure-11e and μ=0.09 subfigure-11f of scenario 3. To achieve the accuracy of the ERK method the scrutiny on AE is directed and results are plotted in Fig. 12 for all the cases of nonlinear CVS model for six variations of μ. The range of AE found 10^{-07} to 10^{-04} for μ=0.02 subfigure-12a, 10^{-08} to 10^{-05} for μ=0.03 subfigure- 12b, 10^{-07} to 10^{-05} for μ=0.04 subfigure- 12c, 10^{-07} to 10^{-04} for μ=0.05 subfigure-12d, 10^{-07} to 10^{-04} for μ=0.07 subfigure-12e and 10^{-07} to 10^{-04} for μ=0.09 subfigure-12f. It may observe a close matched is consistently achieved by ERK and BDF scheme for scenario 1 of CVS model. Fig. 13 presents the computational dynamics of the BDF method for the *S(t)*, *I(t)*, and *R(t)* compartments in a nonlinear CVS model through six different cases in Scenario 3. The plotted results shows that the susceptible computers are decreases over time subfigure-13a, the infected computers are increases initially and then decreases with time subfigure-13b, and the number of recovered computers increases gradually over time subfigure-13c. This information is important for understanding the dynamics of computer virus spread in a network. Fig.14 demonstrates the computing dynamics of the ERK method for the three compartments *S(t)*, *I(t)*, and *R(t)* of nonlinear CVS model across six different cases in Scenario 3. Fig. 14 illustrates that the number of susceptible computers decreases gradually for all cases as time progresses, it directs the spread of the virus in a network subfigure-14a. The number of infected computers increases first and reaches a peak, then decreases with the passage of time, indicating the infection progression and eventual control subfigure-14b. The number of recovered computers increases over time, indicating the removal and recovery of the infection from the network subfigure-14c. It efficiently shows how the ERK method is exploited to simulate the spread of a computer virus over time within a network. For each susceptible, infected, and recovered compartment, the behaviour over time is plotted for six cases.

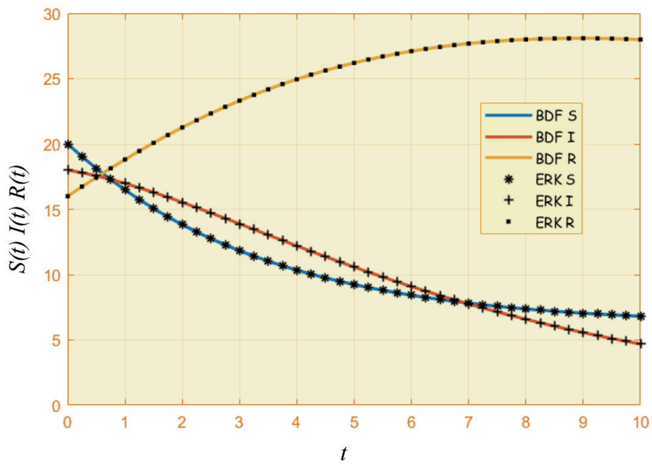
Fig.15 portrayed the outcomes of ERK and BDF methods for the solution *S(t)* of nonlinear epidemiological system for CVS for all six cases γ=0.2 subfigure- 15a, γ=0.3 subfigure-15b, γ=0.4 subfigure-15c, γ=0.5 subfigure- 15d, γ=0.7 subfigure- 15e and γ=0.9 subfigure-15f of scenario 4. To achieve the accuracy of the ERK method the scrutiny on AE is directed and results are plotted in Fig.16 for all the cases of nonlinear CVS model for six variations of γ. The range of AE found 10-07 to 10-04 for γ = 0.2 subfigure- 16a, 10-07 to 10-04 for γ = 0.3 subfigure- 16b, 10^{-07} to 10^{-04} for γ = 0.4 subfigure- 16c, 10^{-07} to 10^{-04} for γ= 0.5 subfigure- 16d, 10-07 to 10^{-04} for γ = 0.7 subfigure-16e and 10^{-07} to 10^{-04} for γ = 0.9 subfigure-16f. It may observe a close matched is consistently achieved by ERK and BDF scheme for scenario 1 of CVS model. Fig.17 presents the computational dynamics of the BDF method for the *S(t)*, *I(t)*, and *R(t)* compartments in a nonlinear CVS model through six different cases in Scenario 4. The plotted results show that the susceptible computers decrease over time Subfigure- 17a, the infected computers increase initially and then decrease with time Subfigure- 17b, and the number of recovered computers increases gradually over time Subfigure- 17c. This information is important to understand the dynamics of computer viruses spread in a network. Fig.18 demonstrates the computing dynamics of the ERK method for the three compartments *S(t)*, *I(t)*, and *R(t)* of nonlinear CVS model across six different cases in Scenario 4. Fig. 18 illustrates that the number of susceptible computers decreases gradually for all cases as time progresses; it directs the spread of the virus in a network subfigure-18a. The number of infected computers increases first and reaches a peak, then decreases with passage of time, indicating the infection progression and eventual control subfigure-18b. The number of recovered computers increases over time, indicating the removal and recovery of the infection from the network subfigure-18c. It efficiently shows how the ERK method is exploited to simulate the spread of a computer virus over time within a network. For each susceptible, infected, and recovered compartment, the behaviour over time is plotted for six cases.



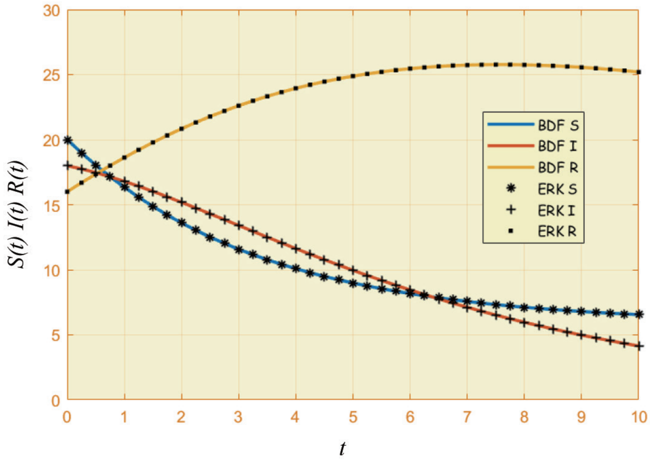
(a) Solution dynamics for μ=0.02



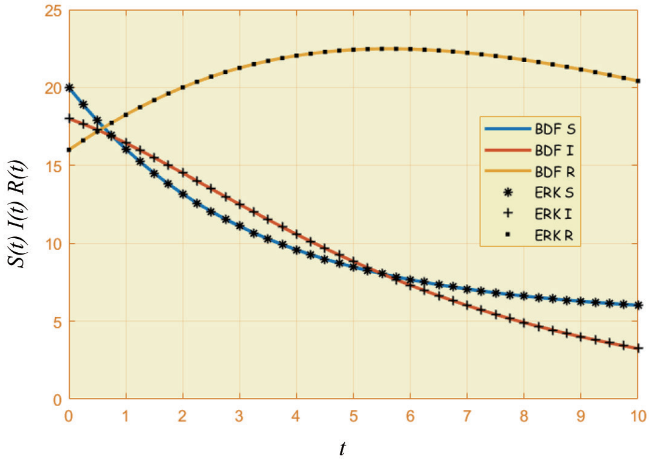
(b) Solution dynamics for μ=0.02



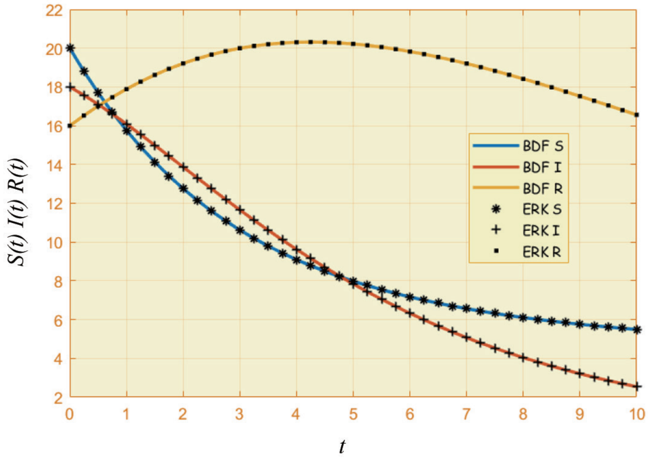
(c) Solution dynamics for μ=0.04



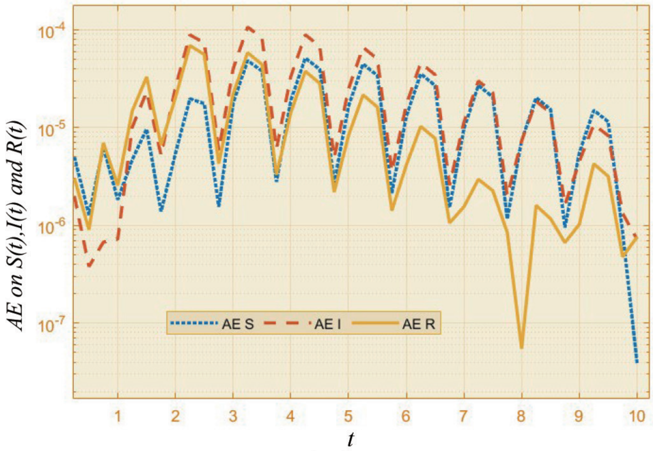
(d) Solution dynamics for μ=0.05



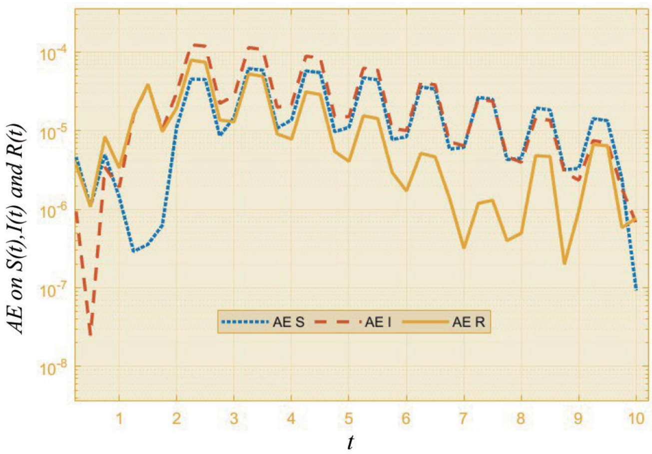
(e) Solution dynamics for μ=0.07



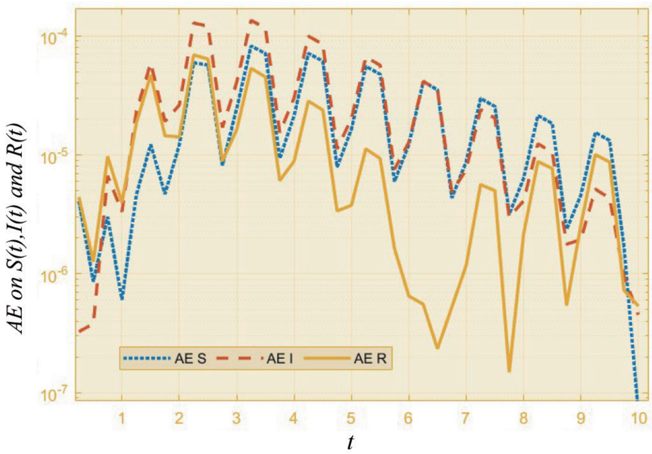
(f) Solution dynamics for μ=0.09



(a) AE for =0.02

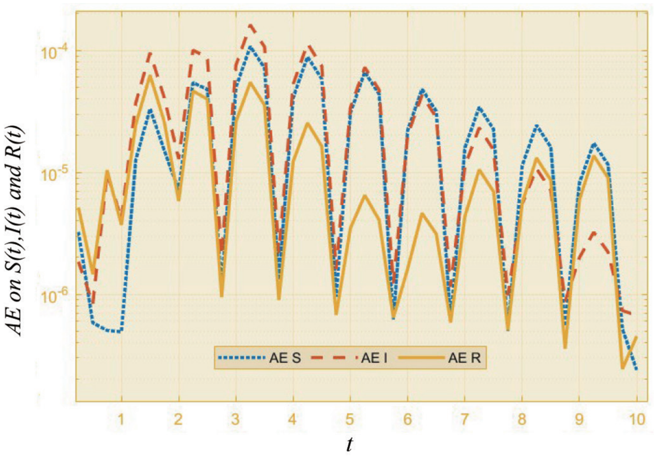


***(b)** AE for μ=0.02*

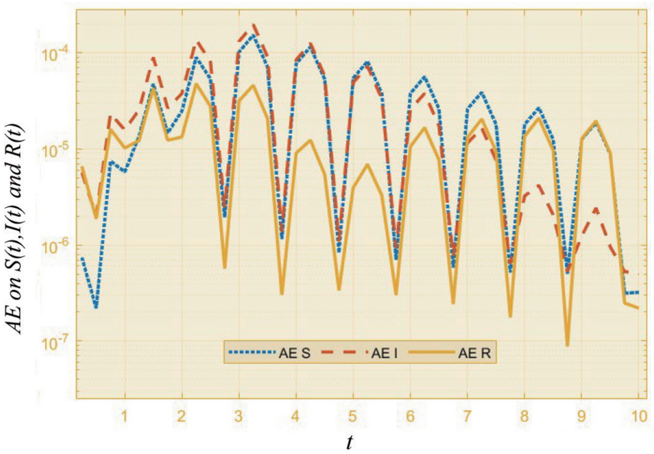


***(c)** AE for μ=0.04*

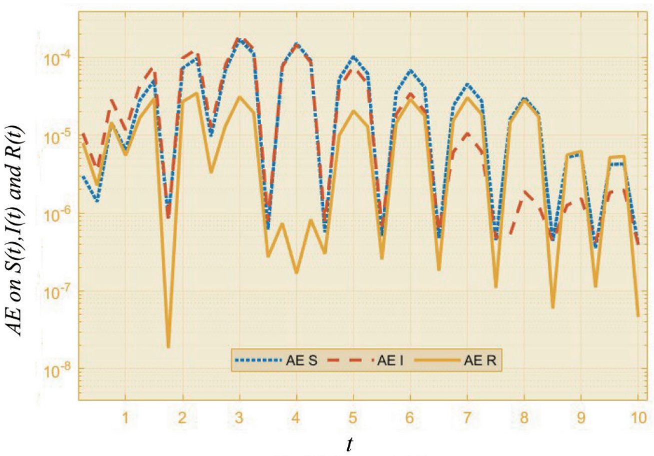
Fig. 11 The solution dynamics of ERK and BDF methods for nonlinear CVS model across all six cases of the scenario 3



***(d)** AE for μ=0.05*

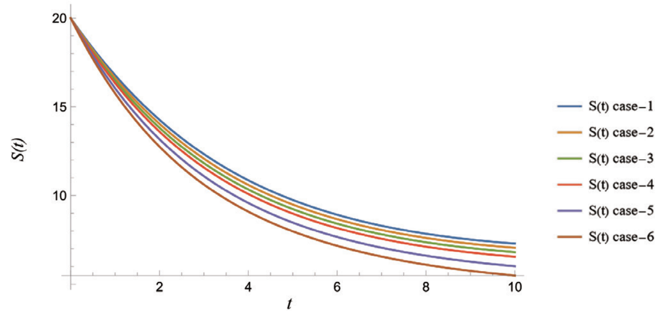


***(e)** AE for μ=0.07*

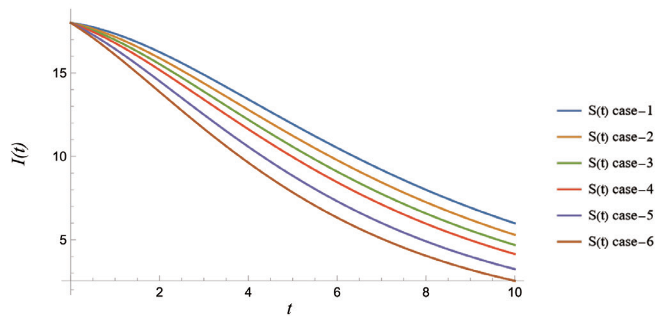


***(f)** AE for μ=0.09*

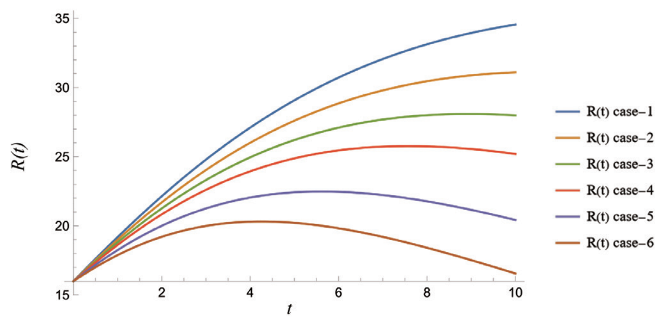
Fig. 12 Comparison on AE for ERK and BDF for nonlinear CVS model across all six cases of the scenario 3



(a) S(t) for Scenario 3 case 1-6

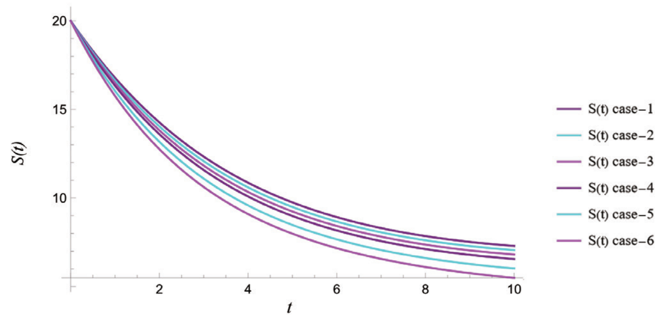


(b) I(t) for Scenario 3(cases 1-6)

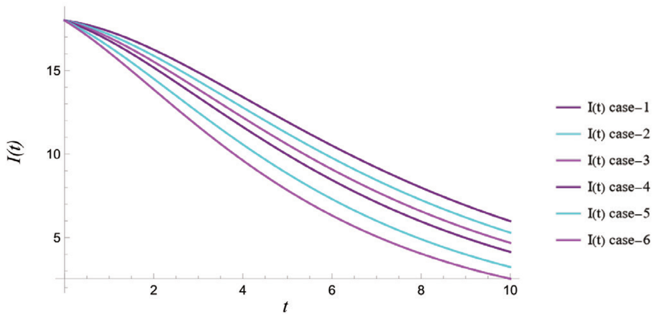


(c) *R(t) for Scenario* 3*(cases 1-6)*

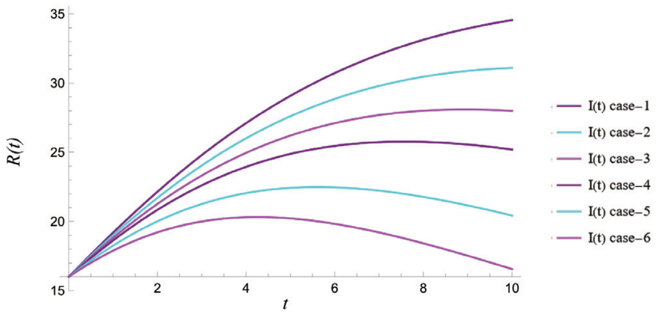
Fig. 13 The computing dynamics of the BDF method for the *S(t)*, *I(t)* and *R(t)* compartments in the nonlinear CVS model across all six cases of Scenario 3.



(a) S(t) for Scenario 3 case 1-6

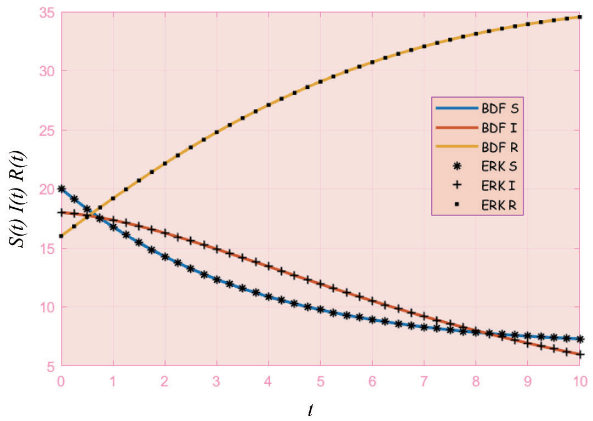


(b) I(t) for Scenario 3 (cases 1-6)

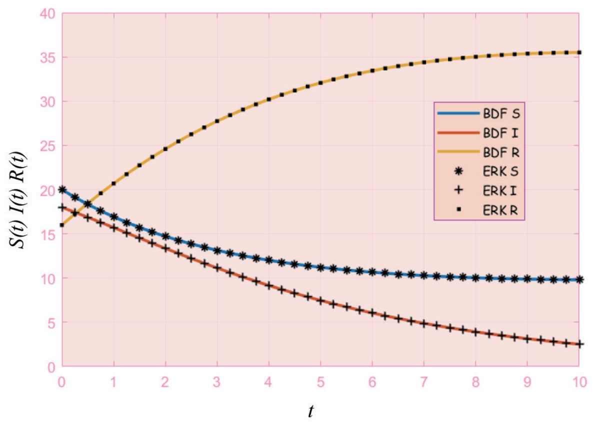


(c) R(t) for Scenario 3 (cases 1-6)

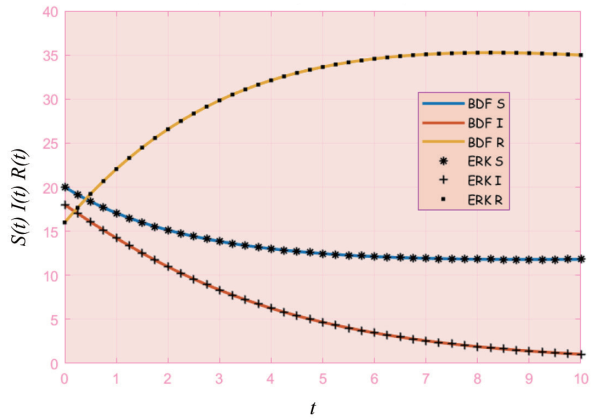
Fig. 14 The computing dynamics of the ERK method for the S(t), *I(t)* and *R(t)* compartments in the nonlinear CVS model across all six cases of Scenario 3.



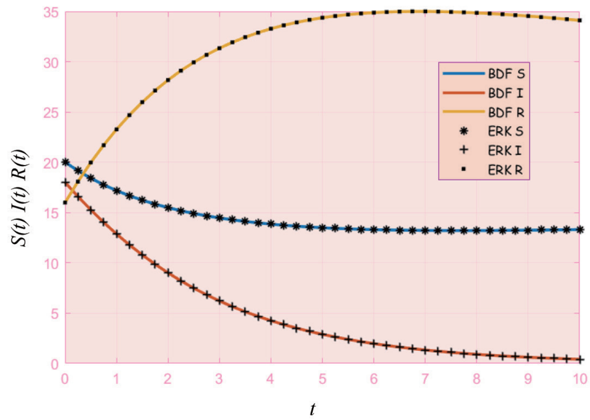
(a) Solution dynamics for b=0.1



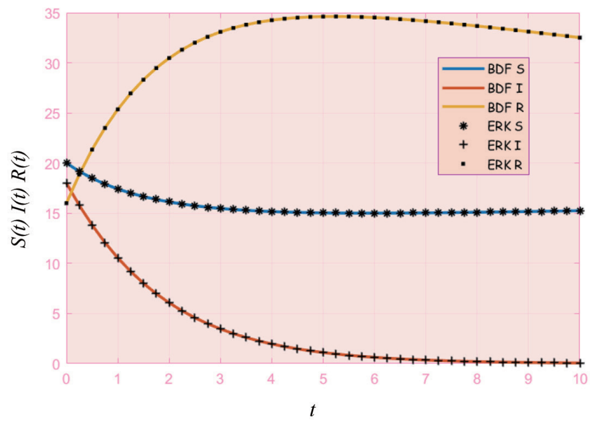
(b) solution dynamics for γ=0.3



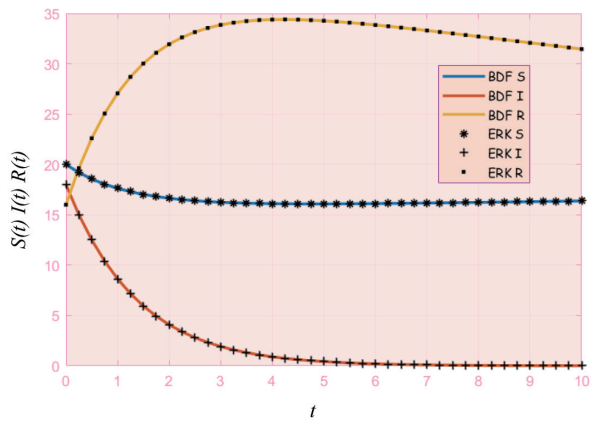
(c) solution dynamics for γ=0.4



(d) solution dynamics for γ=0.5

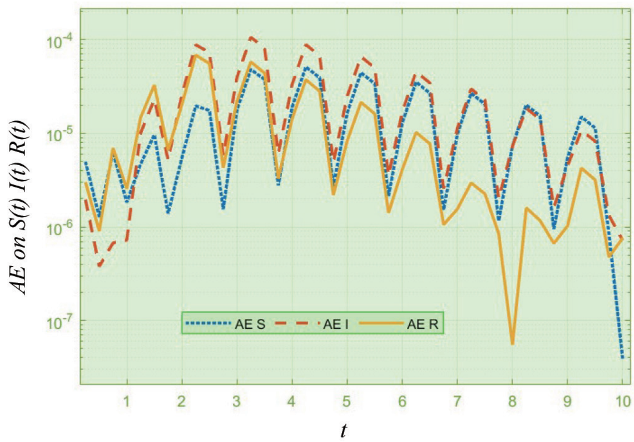


(e) solution dynamics for γ=0.7

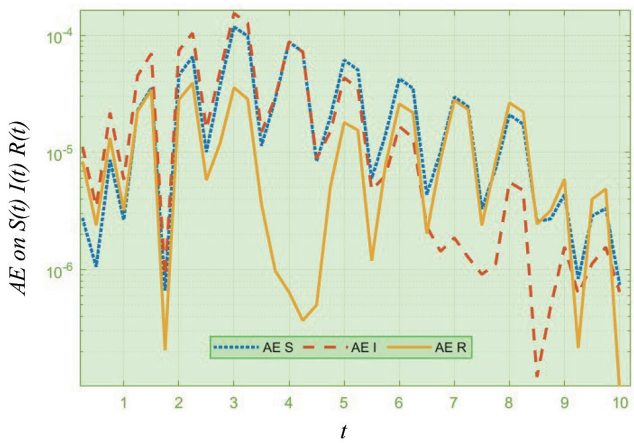


(f) solution dynamics for γ=0.9

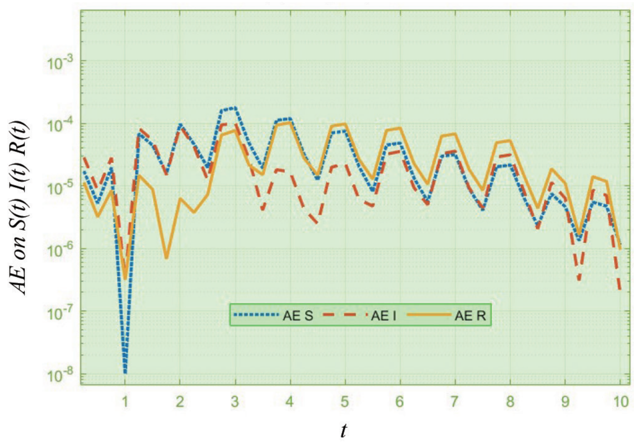
Fig. 15 The computing dynamics of ERK and BDF methods for the nonlinear CVS model for all six cases of the scenario 4



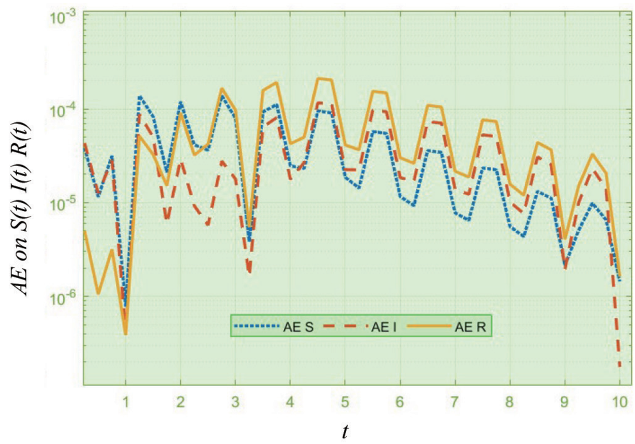
(a) AE for γ=0.2



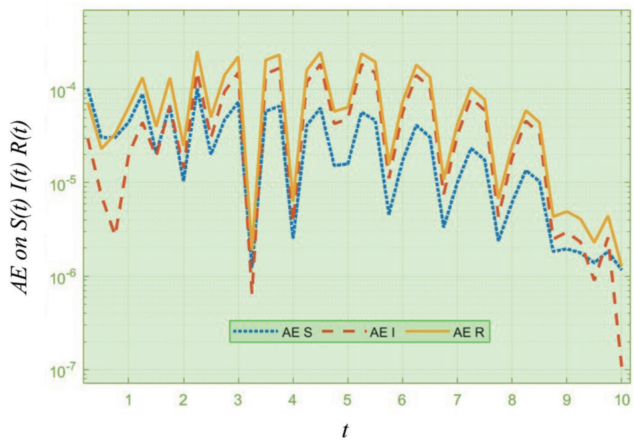
(b) AE for γ=0.3



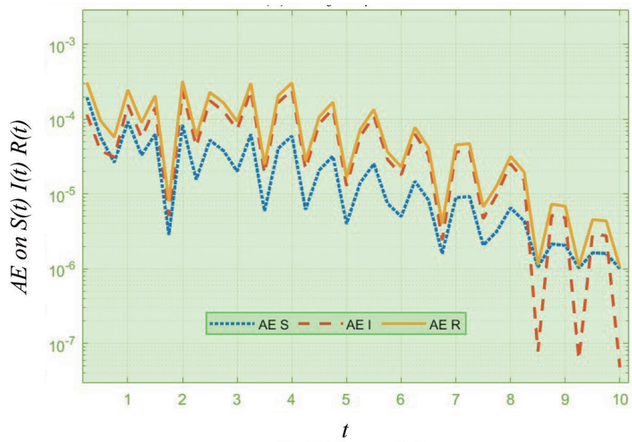
(c) AE for γ=0.4



(d) AE for γ=0.5

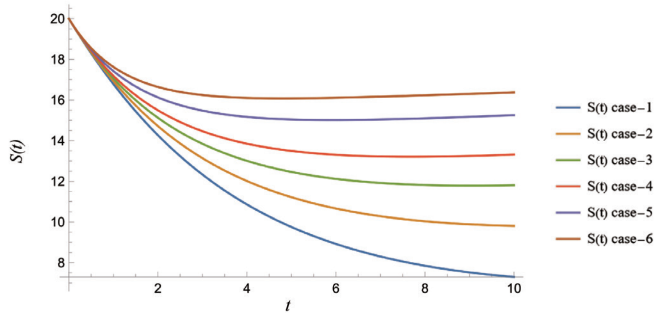


(e) AE for γ=0.7

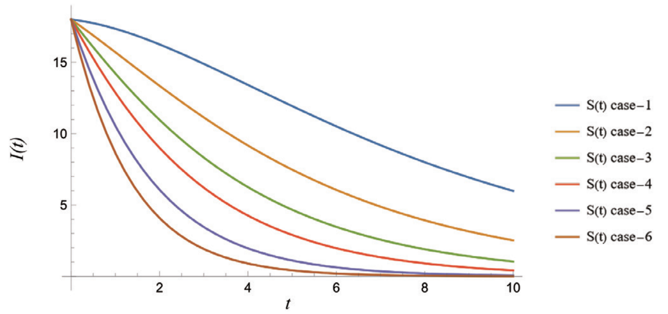


(f) AE for γ=0.9

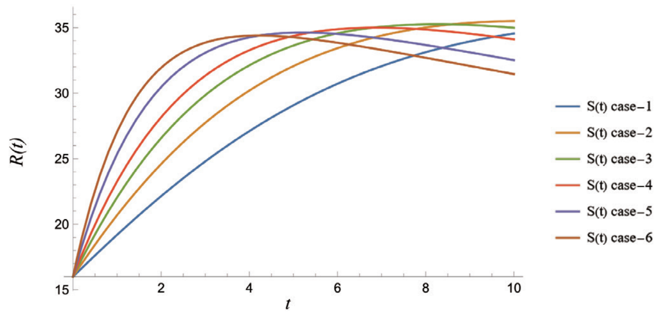
Fig. 16 Comparison on AE for ERK and BDF for nonlinear CVS model across all six cases of the scenario 4



(a) S(t) for Scenario 4 (cases 1-6)

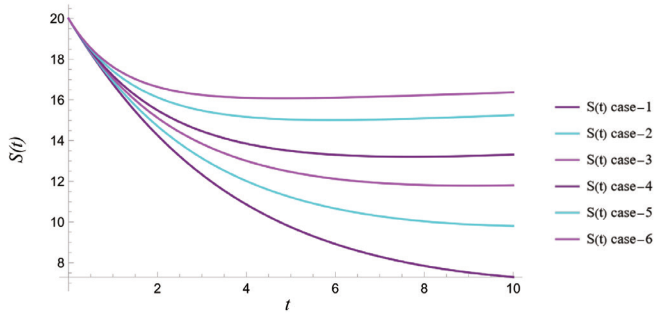


(b) I(t) for Scenario 4 (cases 1-6)

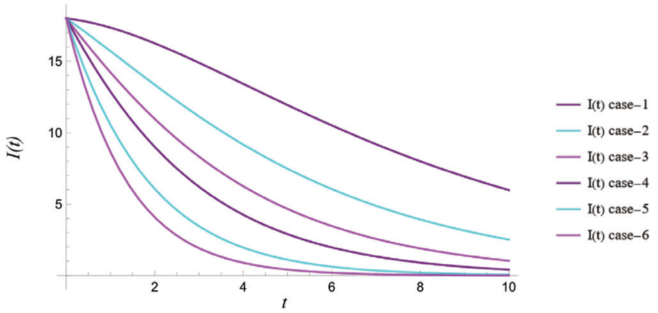


(c) R(t) for Scenario 4 (cases 1-6)

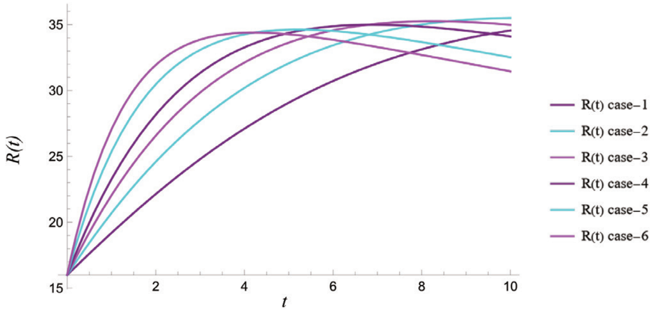
Fig. 17 The computing dynamics of the BDF method for the *S(t)*, *I(t)* and *R(t)* compartments in the nonlinear CVS model across all six cases of Scenario 4.



(a) S(t) for Scenario 4 (cases 1-6)



(b) I(t) for Scenario 4 (cases 1-6)



(c) R(t) for Scenario 4 (cases 1-6)

Fig. 18 The computing dynamics of the ERK method for the S(t), I(t) and R(t) compartments in the nonlinear CVS model across all six cases of Scenario 4.

CONCLUSION

In this study, a novel approach is introduced that leverages the Mathematica execution of ODEs using the ERK method and the BDF method to solve the epidemiological model of CVS. The proposed scheme of study utilizes the NDSolve function to numerically execute the system over a specified time interval, signifying three differential compartments: susceptible *(S)*, infected *(I)*, and recovered *(R)* computers. The dynamics of these three differential compartments are observed by the variations in β (contact rate of susceptible computers to infected computers), γ (rate of recovery due to antivirus treatment), b (rate of external computers connected to the network), and μ (rate of removal of the computer from the network). The proposed methodology constructs accurate and precise numerical solutions by utilizing the robustness of both ERK and BDF methods, which provide a sophisticated analysis of virus spread patterns. The comprehensive simulations established the better accuracy of the proposed methodology, efficiently demonstrating the complicated dynamics of computer virus spread and producing an insightful observation of efficient mitigation schemes. The study significantly contributes to the field of computational epidemiology, particularly in understanding digital epidemics and enhancing cybersecurity measures. The research underscores the importance of sophisticated numerical systems in improving the understanding and prevention of computer virus spread.

Future Directions: This scheme of study will be contributory in moulding future research and the expansion of robust cybersecurity strategies. In the future, this methodology will be magnified to more complex models and scenarios of digital environments. The simulation results provide crucial information about virus spread, which will be essential for designing effective mitigation strategies in the future. This scheme of study will play a significant role in understanding and controlling the spread of computer viruses. In the future, incorporating BDF and ERK methods in the treatment of nonlinear CVS models will enhance the development of sophisticated tools for preventing cyber threats. These tools will be crucial for safeguarding the digital environment from catastrophic disruptions caused by computer viruses.

REFERENCES

[1] Miakhil, P. and Wazir, I., 2024. " Computer and Cyber Crimes. " *Integrated Journal for Researchin Arts and Humanities*, **4**(2), pp.133-136.

[2] Brom, C., Hannemann, T., Tetourová, T., Drobná, A., Kopáňková, N., Volná, K., Kačerovská, K., Děchtěrenko, F., Ježek, P. and Stárková, T., 2024. Eight-year-olds' naïve and acquired knowledge about computer viruses: a mixed methods study. International Journal of Technology and Design Education, **34**(3), pp.903-938.

[3] Wagle, P., 2024. *Investigation and Evaluation of the Impact of Antivirus Protection on the Performance of a Personal Computer* (Doctoral dissertation, Vilniaus Gedimino technikos universitetas.).

[4] İlhan, Ö. and Şahin, G., 2024. "A numerical approach for an epidemic SIR model via Morgan-Voyce series." *International Journal of Mathematics and Computer in Engineering*.

[5] Papageorgiou, V.E. and Tsaklidis, G., 2024. "A stochastic particle extended SEIRS model with repeated vaccination: Application to real data of COVID-19 in Italy." *Mathematical Methods in the Applied Sciences*, **47**(7), pp.6504-6538.

[6] Suantai, S., Sabir, Z. and Asif Zahoor Raja, M., 2023. "Numerical computation of SEIR model for the Zika virus spreading." *Comput Mater Con*, **75**, pp.2155-2170.

[7] Zhao, D., Wang, L., Wang, Z. and Xiao, G., 2018. "Virus propagation and patch distribution in multiplex networks: Modeling, analysis, and optimal allocation." *IEEE Transactions on Information Forensics and Security*, **14**(7), pp.1755-1767.

[8] Sawadogo, D.D.A., 2022. *Towards overcoming zero-day vulnerabilities in open-sourcesoftware: an automatic approach for security patches identification* (Doctoral dissertation, Université du Québec à Montréal).

[9] Gamboa, M. and Lopez-Herrero, M.J., 2020. "Measuring infection transmission in a stochastic SIV model with infection reintroduction and imperfect vaccine." *Acta biotheoretica*, **68**(4), pp.395-420.

[10] Essouifi, M., Lachgar, A., Vasudevan, M., B'ayir, C., Achahbar, A. and Elkhamkhami, J., 2024. Automated hubs-patching: Protection against malware spread through reduced scale-free networks and external storage devices." *IEEE Transactions on Network Science and Engineering*.

[10] Gupta, J.K. and Mishra, B.K., Transmission Dynamics of Malware in Networks Using Caputo Fractional Order Derivative.

[11] Zarin, R., Khaliq, H., Khan, A., Ahmed, I. and Humphries, U.W., 2023. "A numerical study based on haar wavelet collocation methods of fractional-order antidotal computer virus model." *Symmetry*, **15**(3), p.621.

[13] Sabir, Z., Raja, M.A.Z., Mumtaz, N., Fathurrochman, I., Sadat, R. and Ali, M.R., 2023. "An investigation through stochastic procedures for solving the fractional order computer virus propagation mathematical model with kill signals." *Neural Processing Letters*, **55**(2), pp.1783-1797.

[14] Yang, W., Li, D. and Chang, X., 2024. "Analysis and numerical simulation of computer virus propagation model based on limited resources." *Mathematics and Computers in Simulation*, **223**, pp.494-508.

[15] Tang, W., Yang, H. and Pi, J., 2024. "Dynamics and Control Strategies for SLBRS Model of Computer Viruses Based on Complex Networks." *International Journal of Intelligent Systems*, **2024**(1), p.3943882.

[16] Tang, W., Liu, Y.J., Chen, Y.L., Yang, Y.X. and Niu, X.X., 2020. "SLBRS: network virus propagation model based on safety entropy. *Applied Soft Computing*, **97**, p.106784.

[17] Zhao, X., 2023. "Optimal Control Strategy for SLBRS with Two Control Inputs." *Mathematics*, **11**(19), p.4036.

[18] Zhao, X. and Hou, W., 2023. "Optimal Control of SLBRS with Recovery Rates." *Mathematics*, **12**(1), p.132.

[19] Ju, Y., Xiao, M., Huang, C., Rutkowski, L. and Cao, J., 2024. "Hybrid control of Turing instability and bifurcation for spatial-temporal propagation of computer virus." *International Journal of Systems Science*, pp.1-24.

[20] Singh, J., Kumar, J. and Baleanu, D., 2024. "A reliable numerical algorithm based on an operational matrix method for treatment of a fractional order computer virus model." *AIMS Mathematics*, **9**(2), pp.3195-3211.

[21] Shah, H. and Comissiong, D.M.G., 2021. "Computer Virus Model with Stealth Viruses and Antivirus Renewal in a Network with Fast Infectors." *SN Computer Science*, **2**(5), p.407.

[22] Batistela, C.M. and Piqueira, J.R.C., 2018. "SIRA computer viruses propagation model: mortality and robustness." *International Journal of Applied and Computational Mathematics*, **4**, pp.1-9.

[23] Zhu, Q., Wan, W., Gan, C., Fan, Z. and Yang, L.X., 2024. "Simulating Bluetooth virus propagation on the real map via infectious attenuation algorithm and discrete dynamical system." *Iran Journal of Computer Science*, pp.1-22.

[24] Niu, W. and Fan, M., 2024. "Control and Research of Computer Virus by Multimedia Technology." *International Journal of Information Systems and Supply Chain Management (IJISSCM)*, **17**(1), pp.1-17.

[25] Manohara, G. and Kumbinarasaiah, S., 2024. "Numerical solution of a modified epidemiological model of computer viruses by using Fibonacci wavelets." *The Journal of Analysis*, **32**(1), pp.529-554.

[26] Zhou, Y. and Liang, Y., 2024. "Application of artificial intelligence technology in network security." *Highlights in Science, Engineering and Technology*, **92**, pp.479-485.

[27] Ozkan-Ozay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I. and Beloev, I., 2024. "A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. *IEEE*

Access.

[28] Chen, Y., Wu, J., Yu, P. and Wang, X., Network Security Empowered by Artificial Intelligence.

[29] Wei, K., Zang, H., Pan, Y., Wang, G. and Shen, Z., 2024. "Strategic application of ai intelligent algorithm in network threat detection and defense." *Journal of Theory and Practice of Engineering Science*, **4**(01), pp.49-57.

[30] Ying, X., Pan, M., Chen, X., Zhou, Y., Liu, J., Li, D., Guo, B. and Zhu, Z., 2024. "Research on Virus Propagation Network Intrusion Detection Based on Graph Neural Network." *Mathematics*, **12**(10), p.1534.

[31] Nadella, G.S. and Gonaygunta, H., 2024. "Enhancing Cybersecurity with Artificial Intelligence: Predictive Techniques and Challenges in the Age of IoT." *International Journal of Science and Engineering Applications*, **13**(04), pp.30-33.

[32] Hedeving, A., Ekström, F., Johnson, M.D., Alexanderson, H., Baykal, Y. and Stevens, T., 2024. "Thin loess in Southwestern Sweden." *GFF*, pp.1-20.

[33] Dubey, V.P., Kumar, R. and Kumar, D., 2020. "A hybrid analytical scheme for the numerical computation of time fractional computer virus propagation model and its stability analysis." *Chaos, Solitons & Fractals*, **133**, p.109626.

[34] Li, D., Li, X. and Zhang, Z., 2023. "Implicit-explicit relaxation Runge-Kutta methods: construction, analysis and applications to PDEs." *Mathematics of Computation*, **92**(339), pp.117-146.

[35] Tuan, H.M., Hai, T.H. and Thu, P.H., 2023. "A new study for global dynamics and numerical simulation of a discrete-time computer virus propagation model." *Journal of Science and Technology on Information security*, pp.35-42.

[36] Din, S.U., Masood, Z., Samar, R., Majeed, K. and Raja, M.A.Z., 2017, "January. Study of epidemiological based dynamic model of computer viruses for sustainable safeguard against threat propagations." In *2017 14th International Bhurban Conference on Applied Sciences and Technology (IBCAST)* (pp. 434-440). IEEE.