# A Reliable Numerical Analysis for Computer Virus Transmission Model

M.Rafiq[1], A.Raza[2] ,M.S.Arif[2]

[1*]*Faculty of Engineering University of Central Punjab Lahore, Pakistan*

[2]*Department of Mathematics Air University Islamabad, Pakistan*

***Abstract*— Numerical Analysis involves construction and implementation of reliable numerical schemes to solve continuous models. These schemes are constructed with the aim that they remain consistent with the continuous model and preserve all of its essential properties .In this paper, a reliable numerical analysis is presented for the dynamics of computer virus in a network. Results are compared with already existing schemes which do not behave well in certain scenarios.**

***Key Words*: Computer virus, Continuous Dynamical System, Numerical Analysis, Convergence**

## I. INTRODUCTION

The rapid development in almost all fields of computers, internet, communication and network technology has made the information system more efficient and it is p laying the vital role in development of many countries and their industries too[1]. In the era of information technology, it has become a challenge to maintain the information security[4,5]. The most common security threat among all is computer viruses. Computer viruses are hi ghly ruinous and transmissible. As soon as the virus enters the system it generates its copies and it becomes very difficult to control the speed of its functioning. In the scientific field biology, the virus can be transmitted from one organism to another. Cohen, Kephart and White has defined many similarities in both biological and computer viruses [1-3]. If the b iological virus finds the su itable conditions it grow s quickly in the i nfected organisms, the symptoms are shown and even may die. In the same way the computer virus works. It transfers itself from an infe cted computer system to another computer system and generates its copies. In some computers it m ay destroy the data of computer or the computer system may disable[6-8]. Computer virus is a software replicates itself when executed. Different viruses have different effects. When they enter in an uninfected computer they find the other storage media and programs according to their set ta rget and inserts the code and achieve the target of self-reproduction. As long as t his virus remains in the computer and no treatment is done it keeps on working and targets more files usually which are executable. The file which gets infected becomes a virus too (a new source of infection) and exchanges the data to other systems[9,10]. There a re many ways in which a c omputer virus can enter into your computer system. It may enter into your system by an infected external hard drive, any download from infected website, by connecting an infected mobile phone or even by visiting an infected website. When a computer has a virus, it may infect the mobile hard drive which attached to it also gets infected. The other computers which are conn ected to the infected system will also be infected. Therefore, there is al ways a risk present that a device has a virus [11-13].

## II. MATHEMATICAL MODEL

*A: Parameters and Variables*

$S(t)$: expresses as the susceptible computers.

$A(t)$: expresses as the non-infected computers or ability of antivirus.

$I(t)$: expresses as the infected computers.

$R(t)$: expresses as those computers who are detached due to virus.

$C$: expresses the rate of those computers who are newly joined the computer network.

$\beta$ : expresses the rate of infection.

$\mu$: expresses the rate of detached computer due to other than virus.

$\delta$ : expresses the rate of removal of computers due to virus.

$\sigma$: expresses the rate of recover computers due to ability of antivirus.

$\alpha_{SA}$: expresses the rate of susceptible computers into antidotal computers.

$\alpha_{IA}$: expresses the rate of infected computers.

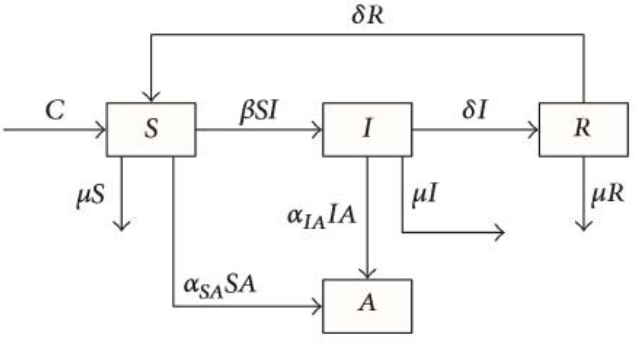


**Fig.1 Flow chart of computer network model**

The mathematical formulation of computer network Model is given by [14]:

$$S' = C - \alpha_{SA}\, SA - \beta SI - \mu S + \sigma R$$
$$I' = \beta SI - \alpha_{IA}\, IA - \delta I - \mu I \quad (1)$$
$$R' = \delta I - \sigma R - \mu R$$
$$A' = \alpha_{SA} SA + \alpha_{IA} IA - \mu A$$

$$N(t) = S(t) + I(t) + R(t) + A(t) \quad (2)$$

The reduced form of the model is

$$S' = C - \alpha_{SA}\, SA - \beta SI - \mu S + \sigma R$$
$$I' = \beta SI - \alpha_{IA}\, IA - \delta I - \mu I \quad (3)$$
$$R' = \delta I - \sigma R - \mu R$$
$$A' = \alpha_{SA} SA + \alpha_{IA} IA - \mu A$$

There are two following equlibrium states of the the model. $\mathcal{E}_1 = (C/\mu, 0, 0, 0)$ and $\mathcal{E}_2 = (S^*, I^*, R^*, A^*)$

$$S^* = \left(\frac{\delta + \mu}{\beta}\right),$$

$$I^* = \frac{(C_0 - 1)(\delta + \mu)(\sigma + \mu)}{\beta(\sigma + \delta + \mu)}$$

$$R^* = \frac{\delta}{\sigma + \mu I\, 3}$$

$$A^* = \frac{\beta S^* - (\delta + \mu)}{\alpha_{IA}}$$

Where $C_0 = \frac{C\alpha_{SA}}{\mu^2}$

$C_0$ is called the reproductive number of the model which tells us the virus eradicate from computer population if $C_0 < 1$ and virus infect the computer population if $C_0 > 1$.

## III. Numerical Modeling

### A: Forward Euler Method

Following is the forward Euler's scheme for model (3):

$$S^{n+1} = S^n + h[C - \alpha_{SA}\, S^n A^n - \beta S^n I^n - \mu S^n + \sigma R^n]$$
$$I^{n+1} = I^n + h[\beta S^n I^n - \alpha_{IA}\, I^n A^n - \delta I^n - \mu I^n]$$
$$R^{n+1} = R^n + h[\delta I^n - \sigma R^n - \mu R^n]$$
$$A^{n+1} = A^n + h[\alpha_{SA} S^n A^n + \alpha_{IA} I^n A^n - \mu A^n]$$

### B:Numerical Experiments

The numerical experiments have been performed for values of parameters given in Table 1 [14].

**Table 1**

| Parameters | Values | |
|---|---|---|
| | VFE | EE |
| $\beta$ | 0.05 | 0.05 |
| C | 1 | 6 |
| $\alpha_{SA}$ | 0.00045 | 0.00045 |
| $\mu$ | 0.05 | 0.05 |
| $\sigma$ | 0.8 | 0.8 |
| $\alpha_{IA}$ | 0.0025 | 0.0025 |
| $\delta$ | 0.96 | 0.96 |

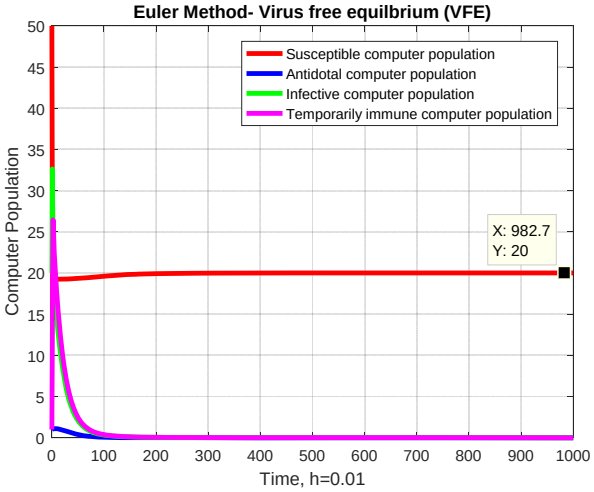


**Fig. 2 Euler Method (VFE), $h = 0.01$**

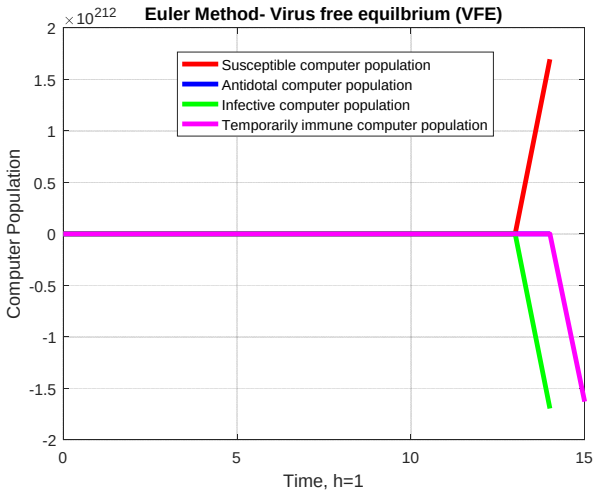


**Fig.3 Euler Method (VFE), $h = 1$**

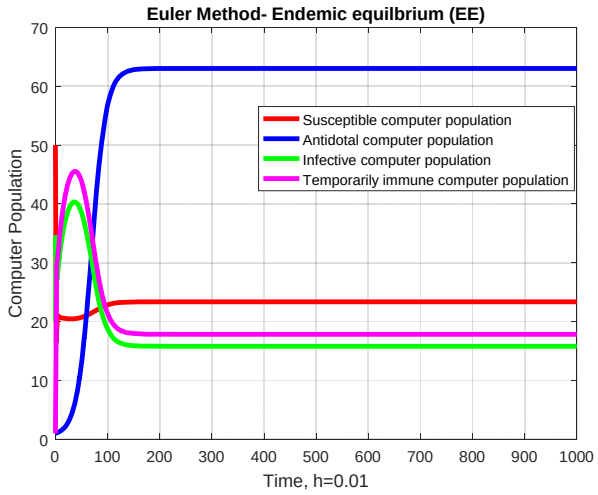


**Fig.4 Euler Method (EE), $h = 0.01$**

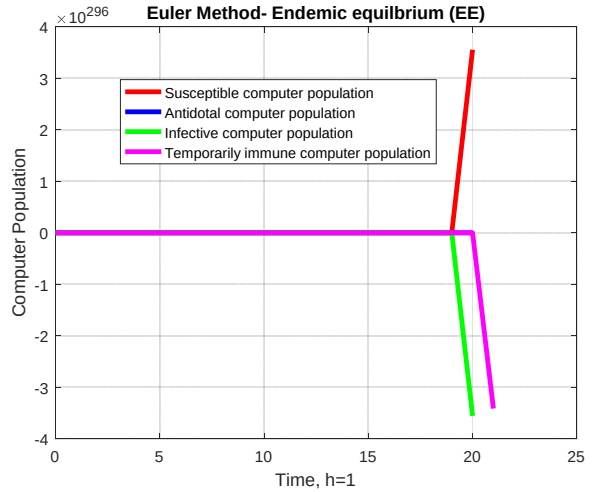


**Fig. 5 Euler Method (EE), $h = 1$**

*C: Fourth Order Runge-Kutta Scheme*

For Stage-1

$$K_1 = h[C - \alpha_{SA} S^n A^n - \beta S^n I^n - \mu S^n + \sigma R^n]$$
$$m_1 = h[\beta S^n I^n - \alpha_{IA} I^n A^n - \delta I^n - \mu I^n]$$
$$n_1 = h[\delta I^n - \sigma R^n - \mu R^n]$$
$$o_1 = h[\alpha_{SA} S^n A^n + \alpha_{IA} I^n A^n - \mu A^n]$$

For Stage-2

$$K_1 = h\left[C - \alpha_{SA}(S^n + \frac{K_1}{2})(A^n + \frac{n_1}{2}) - \beta - \mu(S^n + \frac{K_1}{2})(I^n + \frac{l_1}{2}) + \sigma(R^n + \frac{m_1}{2})\right]$$
$$m_2 = h\left[\beta_1(S^n + \frac{K_1}{2})(I^n + \frac{l_1}{2}) + \alpha_{IA}(I^n + \frac{l_1}{2})(A^n + \frac{n_1}{2}) - \delta(I^n + \frac{l_1}{2}) - \mu(I^n + \frac{l_1}{2})\right]$$
$$n_2 = h\left[\delta(I^n + \frac{l_1}{2}) - \sigma(R^n + \frac{m_1}{2}) - \mu(R^n + \frac{m_1}{2})\right]$$
$$o_2 = h\left[\alpha_{SA}(S^n + \frac{K_1}{2})(A^n + \frac{n_1}{2}) + \alpha_{IA}(I^n + \frac{l_1}{2})(A^n + \frac{n_1}{2}) - \mu(A^n + \frac{n_1}{2})\right]$$

For Stage-3

$$K_1 = h[C - \alpha_{SA}(S^n + K_3)(A^n + n_3) - \beta - \mu(S^n + K_3)(I^n + l_3) + \sigma(R^n + m_3)]$$
$$m_2 = h[\beta_1(S^n + K_3)(I^n + l_3) + \alpha_{IA}(I^n + l_3)(A^n + n_3) - \delta(I^n + l_3) - \mu(I^n + l_3)]$$
$$n_2 = h[\delta(I^n + l_3) - \sigma(R^n + m_3) - \mu(R^n + m_3)]$$
$$o_2 = h[\alpha_{SA}(S^n + K_3)(A^n + n_3) + \alpha_{IA}(I^n + l_3)(A^n + n_3) - \mu(A^n + n_3)]$$

For Stage-4

$$K_1 = h\left[C - \alpha_{SA}(S^n + \frac{K_2}{2})(A^n + \frac{n_2}{2}) - \beta - \mu(S^n + \frac{K_2}{2})(I^n + \frac{l_2}{2}) + \sigma(R^n + \frac{m_2}{2})\right]$$
$$m_2 = h\left[\beta_1(S^n + \frac{K_2}{2})(I^n + \frac{l_2}{2}) + \alpha_{IA}(I^n + \frac{l_2}{2})(A^n + \frac{n_2}{2}) - \delta(I^n + \frac{l_2}{2}) - \mu(I^n + \frac{l_2}{2})\right]$$
$$n_2 = h\left[\delta(I^n + \frac{l_2}{2}) - \sigma(R^n + \frac{m_2}{2}) - \mu(R^n + \frac{m_2}{2})\right]$$
$$o_2 = h\left[\alpha_{SA}(S^n + \frac{K_2}{2})(A^n + \frac{n_2}{2}) + \alpha_{IA}(I^n + \frac{l_2}{2})(A^n + \frac{n_2}{2}) - \mu(A^n + \frac{n_2}{2})\right]$$

Finally

$$S^{n+1} = S^n + \frac{1}{6}[K_1 + 2K_2 + 2K_3 + K_4]$$
$$E^{n+1} = E^n + \frac{1}{6}[m_1 + 2m_2 + 2m_3 + m_4] \quad (5)$$
$$I^{n+1} = I^n + \frac{1}{6}[n_1 + 2n_2 + 2n_3 + n_4]$$
$$A^{n+1} = A^n + \frac{1}{6}[o_1 + 2o_2 + 2o_3 + o_4]$$

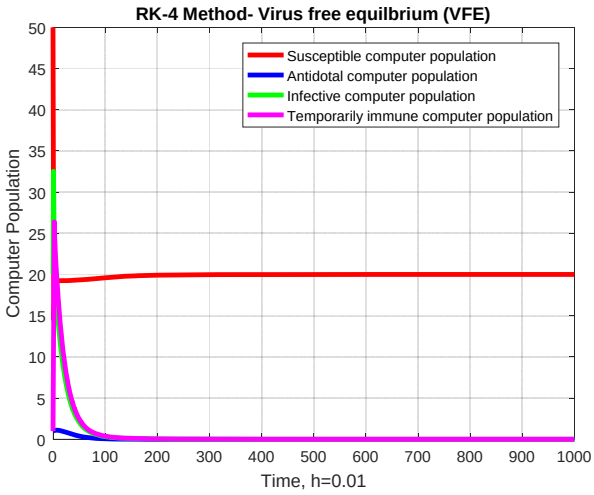


**Fig.6 RK-4 Method (VFE), $h = 0.01$**

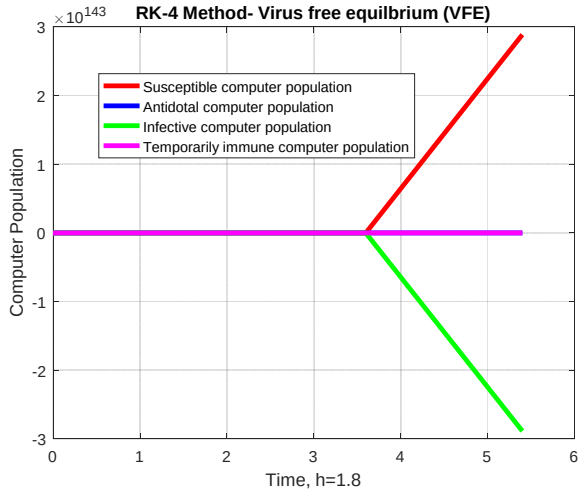


**Fig.7 RK-4 Method (VFE), $h = 1.8$**

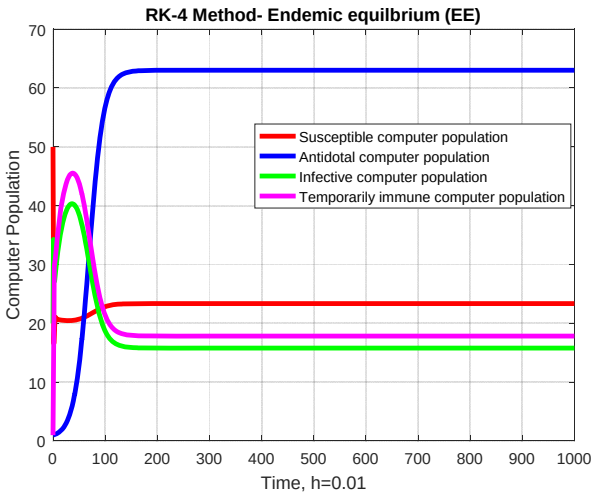


**Fig.8 RK-4 Method (EE), $h = 0.01$**

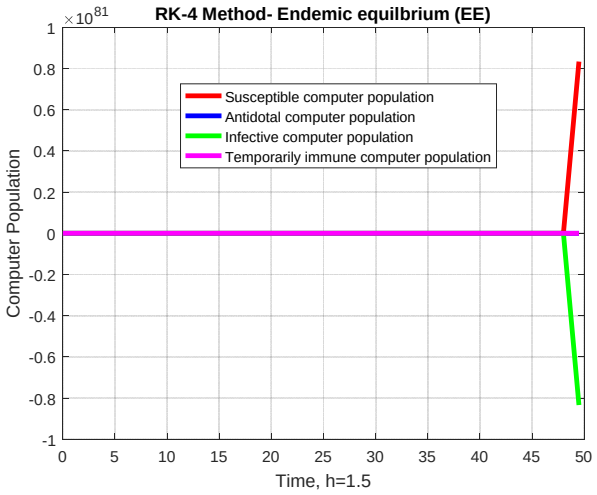


**Fig.9 RK-4 Method (EE), $h = 1.05$**

## IV. Non-Standard Finite Difference Model

Non-Standard Finite Difference (NSFD) theory introduced by R.E. Mickens [15,16]. We constructed the NSFD scheme for computer virus transmission model which is given by:

$$S^{n+1} = \frac{(S^n + hC + \sigma R^n)}{1 + \alpha_{SA} A^n + h\beta I^n + h\,\mu)}$$

$$I^{n+1} = \frac{I^n}{1 + h\alpha_{SI} A^n - h\beta S^n + h\delta + h\,\mu)}$$

$$R^{n+1} = \frac{R^n + h\delta I^n}{1 + h\sigma + h\,\mu)}$$

$$A^{n+1} = \frac{A^n}{1 - h\alpha_{SA} S^n - h\alpha_{IA} I^n + h\,\mu}$$

### *A: Numerical Experiments*

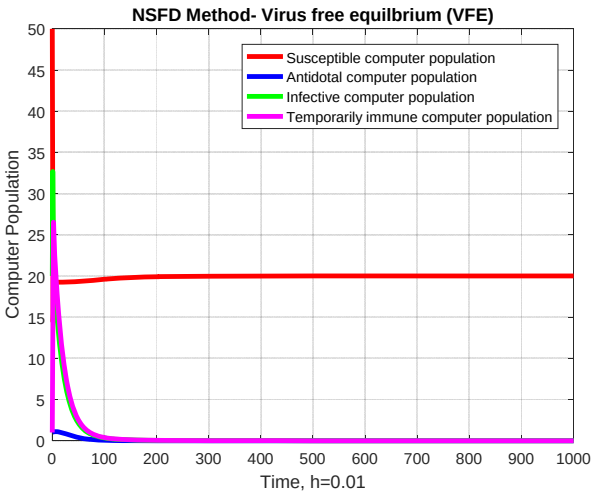


**Fig.10 NSFD Method (VFE), $h = 5$**

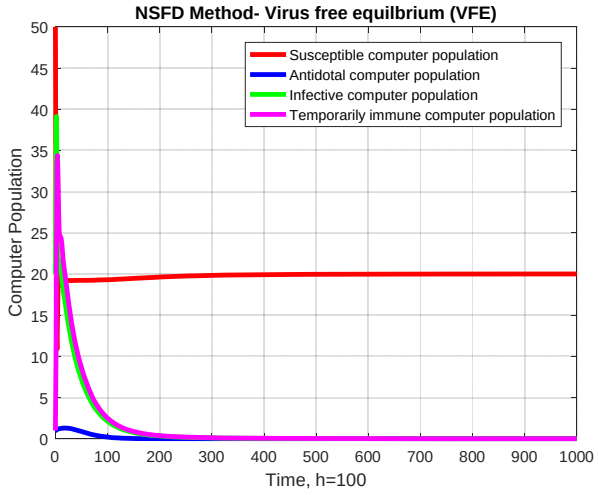


**Fig.11 NSFD Method (VFE), $h = 100$**

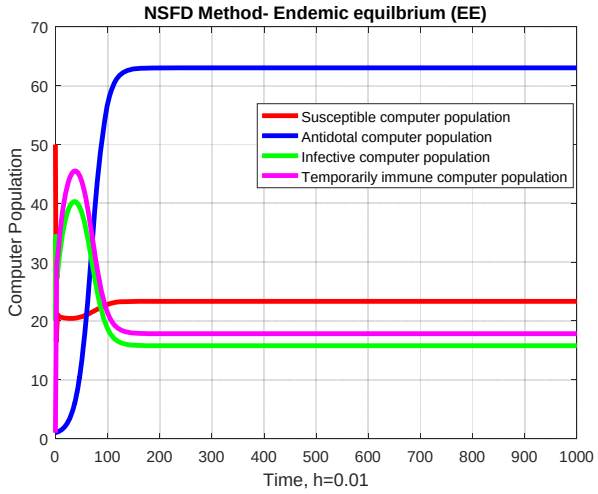


**Fig.12 NSFD Method (EE), $h = 0.01$**

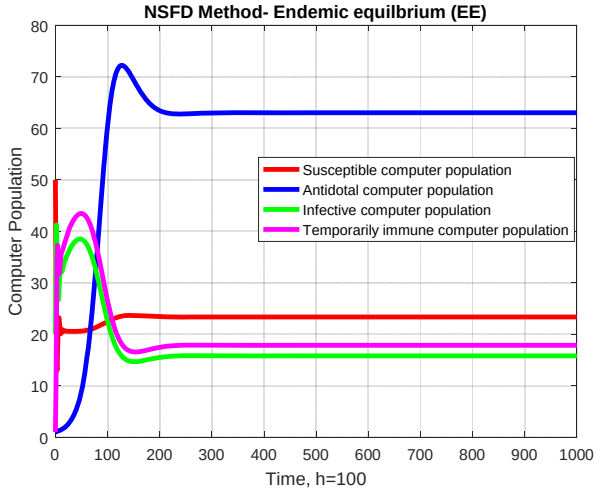


**Fig.13 NSFD Method (EE), $h = 100$**

## V. Results and Discussion

The transmission dynamics of a c omputer virus has been analyzed numerically. There ar e two ste ady states of the computer network model i.e v irus free equilibrium and endemic equilibrium points. When $C_0 < 1$, virus free equilbrium is locally asmpotatically stable and When $C_0 > 1$, the endemic equilibrium point of computer network model is stable.

We introduced the unconditionally stable Non-Standard Finite Difference (NSFD) scheme for the c ontinuous dynamical system of computer network model. The proposed scheme has satisfy the essential properties of continous model of computer network as positivity, boundedness and dynamical consistency remains consrved. Numerical experiments have shown that well known standard finie difference schemes fail to preserve these properties.

## VI. References

[1]. F. Cohen, "Computer viruses: theory and experiments," Computers & Security, vol.6, no.1, pp.22–35,1987.

[2]. J.O. Kephart and S.R. White, "Directed-gra ph epidemiological models of c omputer viruses," in Proceedings of the IEEE Co mputer Society Sym posium on Research in Security and Privacy, pp.343–358, May1991.

[3]. J.O. Kephart and S .R. White "Measuring and modeling computer virus pre valence," in Proceedings of the IEEE Computer Society Symposium on R esearch in Security and Privacy, pp.2–15, IEEE, Oakland, Calif, USA, May1993.

[4]. B. K. M ishra and N. Jha, "Fixed period of t emporary immunity after r un of anti-malicious software on computer nodes," Applied Mathematics and Computation, vol.190, no.2, pp.1207– 1212,2007.

[5]. B.K. Mishra and D.K. Saini, "SEIRS ep idemic model with delay for transmission of m alicious objects in computer network," Applied Mathematics and Computation, vol.188, no.2, pp.1476– 1482,2007.

[6]. J.R.C. Piqueira, B.F. Navarro, and H.A.M. Luiz, "Epidemiological models applied to viruses in computer networks, Journal of Computer Science, vol.1, no.1, pp.31–34,2005.

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

[8]. J.R.C. Piqueira, A.A.de Vasconcelos, C.E.C.J. Gabriel, and V.O. Araujo, Dynamic models for computer viruses, "Computers and Sec urity, vol.27, no.7-8, pp.355–359,2008.

[9]. F. W. Wang, Y. K. Zhang, C. G. Wang, J. F. Ma, and S. Moon, "Stability analysis of a SEIQV epidemic model for rapid spreading worms, Computers and Security, vol. 29, no. 4, pp. 410–418,2010.

[10]. 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.

[11]. B. K. M ishra and S. K. Pandey, Fuzzy e pidemic model for the transmission of worms in computer network," Nonlinear Analysis: Real World Applications, vol.11, no.5, pp.4335–4341, 2010.

[12]. B.K. Mishra and G.M . Ansari, Differential epidemic model of vi rus and worms in computer network, "International Journal of Network Security, vol.14, no.3, pp.149–155, 2012.

[13].Z. Zhang and H. Yang, Hopfbifurcation of an SIQR computer virus model with time delay, Discrete Dynamics in Nature and Society, vol.2015, ArticleID101874,8pages, 2015.

[14].P. Qin, Analysis of a M odelfor Computer Virus Transmission. Mathematical Problems in Engi neering Volume 2015, Article ID 720696, 10 pages.

[15].Mickens. R.E, Nonstandard Finite Difference Models of Differential Equations, World Scientific, 1994.

[16].Mickens, R.E., Applications of Nonstandard Finite Difference Schemes, Singapore: World Scientific, 2000.