GAS Journal of Multidisciplinary Studies
(GASJMS)

Volume- 02 | Issue- 08 | 2024 Homepage: https://gaspublishers.com/gasjms/ ISSN: 2583-8970

# Impact of Noise on an E-Epidemic Scenario: A Mathematical Approach

J Praveshika[1] , Y Divya Lakshmi[2] , B.S.N. Murthy[3] , M N Srinivas[4,*]

[1, 2, 4] *Department of Mathematics, School of Advanced Sciences, Vellore Institute of Technology, Vellore-632014, Tamil Nadu, India.*
[3] *Department of Mathematics, Aditya College of Engineering and Technology, Surampalem, India.*

*DOI: 10.5281/zenodo.13362634*

**Paper History**
Received: 20-08-2024
Accepted: 21-08-2024
Published: 23-08-2024

**Abstract:** In order to comprehend the rate at which computers in one network become infected by others and the role that antivirus software plays in recovery, we have developed a mathematical model for computer virus propagation that is susceptible to infection. In this research, we describe the interaction between susceptible and infected computers and use Fourier transform and numerical stimulations to understand its stochastic stability. The graphical comprehension of steadiness is provided by MATLAB.

**Keywords:** Susceptible, Infected, Antivirus, Stability, Fourier Transform, Variance,

## 1. INTRODUCTION

Malicious mobile code, which can take many different forms and include viruses, worms, trojan horses, and logic bombs, is referred to as a computer virus [1]. Different strategies are used by each kind of code to spread around the internet. Whereas worms employ system flaws to find and attack computers, viruses mostly target file systems. Trojan horses pose as trustworthy websites to trick people into downloading them unintentionally. Despite the fact that there are many different types of computer viruses, they all have traits including invisibility, latency, destructibility, unpredictability, and infectivity [2]. The word "latent" refers to the fact that viruses hide within a computer and propagate across the internet without the user's knowledge. Without authentication, anyone can transmit any kind of packet to any other person on the internet, requiring the recipient to process any packet that reaches a certain service.

Because there is no verification, attackers can fabricate identities and send malicious programs without repercussions. As a result, every system having an internet connection makes itself vulnerable to cyberattacks.

The susceptible-infectious-removed (SIR) classical epidemic models developed by Kermack and McKendrick [7] provide a means of investigating the basic ideas of mathematical models pertaining to the spread of illnesses and/or dangerous software. Numerous mathematical models that depict both the attacking behavior and the spread of malware across networks have been developed, building on this conventional epidemic framework [8–9]. The Internet was found to exhibit a range of power-law degree distributions ten years ago [10–14]. The unexpected conclusion that the epidemic threshold vanishes for scale-free networks of indefinite size was the result of this discovery, which stimulated interest in the propagation of viruses within complex networks [15].

But previous studies mainly concentrated on three fundamental epidemic models: the SI model [16, 17], the SIS model [18–21], and the SIR model [22–24]. When endemic equilibrium was present, studies of its global stability were mostly experimental.

There hasn't been a lot of research on more logical epidemic models, despite Pastor-Satorras and Vespignani's [13] emphasis on their significance. The threshold parameter and the idea of computer viruses spreading via email were first presented by Newman et al. [25], which paved the way for the simulation of viral propagation intended to stop malware infestations [26]. More recently, studies have attempted to improve the way that virus propagation models and anti-virus strategies are integrated to investigate problems including virus immunization, quarantine tactics, and the intrinsic fuzziness of these models.

To prevent any potential threat of damaging attack, anti-malware tools are installed on the system that can detect and eliminate malware. Viral infections and other dangerous objects can be recognized by anti-malware software by using a set of malware signature definitions. It searches through the computer's memory and discs for files, matching them to a database of malware signatures. Thus, the only malwares that are protected against on a machine are those that were known before the last malware definition update. As a result, the efficacy of anti-malware software is significantly impacted by how frequently these virus definitions are updated. Maintaining an up-to-date malware signature database is essential for maximizing the efficacy of anti-malware software against new threats. Pandemic is gaining a comprehensive grasp of its mode of transmission in order to design effective containment strategies. To lessen network vulnerabilities and ensure security, similar defenses are employed against computer viruses, such as intrusion detection systems [31], anti-virus software [27–29], and antidotal computers [30].

## 2. NOISE FORMULATION FOR COMPUTER VIRUS SUSCEPTIBLE-INFECTED MODEL:

Antivirus software is widely recognized for its ability to successfully recover compromised systems. The number of computers it can repair in a predetermined amount of time can be used to gauge its effectiveness. Generally speaking, this software's price and performance are related. The level of a network's anti-virus efficacy is limited by financial constraints. As a result, it makes sense to think about the recovery function listed below:

$$T(I) = \begin{cases} \varepsilon I & if\ 0 \le I \le I_O \\ m & if\ \ I \le I_O \end{cases}$$

where ε is the recovery rate when the anti-virus ability is not fully utilized. The mathematical model is given by two equations where one gives idea about the susceptible computers (S) over a period of time and the other gives us idea about the infected computers (I) over a period of time denoted by $S'(t)$ and $I'(t)$ respectively. The dynamics of the model is given by non-linear differential equation with noise as follows:

$$\begin{cases} S'(t) = rs\left(1 - \frac{S}{k}\right) - \lambda SI - dS + \eta_1\Psi_1(\mathrm{t}) \\ I'(t) = \lambda SI - T(I) - dI + \eta_2\Psi_2(\mathrm{t}) \end{cases} \tag{1}$$

In system of equations (1), $S$ represents the total number of susceptible computers, $I$ represents the total number of infected computers, λ represents the rate at which a connection to an infected computer facilitates recovery. $d$ represents the rate at which one computer is removed from network, $k$ is the carrying capacity which is >0, $r$ is the intrinsic growth rate >0, $\eta_1\Psi_1(\mathrm{t})$ & $\eta_2\Psi_2(\mathrm{t})$ are noise disturbances.

## 3. ANALYSIS OF WHITE NOISE FOR S-I MODEL

We will now explore stochastic models to illustrate how random environmental variables impact stability. Due to random fluctuations, the model's parameters vary around their average values. We will consider the effects of additive white noise and the inherent randomness of the model. White noise perturbations will affect any parameter in the model, represented as , $\eta_i\Psi_i(\mathrm{t})$, where $\Psi_i(\mathrm{t})$ signifies Gaussian white noise at a specific time t, and , $\eta_i$ represents the noise amplitude. Despite this, the equilibrium states of both deterministic and stochastic models will remain the same, though they will now fluctuate around their mean states.

We analyse model dynamics (1) around the interior equilibrium point $\tilde{\mathrm{P}}\ (S^*, I^*)$.Let

$$\mathrm{S(t)}=h_1(t) + S^*; \tag{3.1}$$

$$\mathrm{I(t)}=h_2(t) + I^* \tag{3.2}$$

$$S'(t) = h_1'(t)\ ;\ I'(t) = h_2'(t)$$

Case (i):

$$\begin{cases} S'(t) = rs\left(1 - \frac{S}{k}\right) - \lambda SI - dS + \eta_1\Psi_1(\mathrm{t}) \\ I'(t) = \lambda SI - \varepsilon I\ - dI + \eta_2\Psi_2(\mathrm{t}) \end{cases} \tag{3.3}$$

Case (ii):

$$\begin{cases} S'(t) = rs\left(1 - \frac{S}{k}\right) - \lambda SI - dS + \eta_1\Psi_1(\mathrm{t}) \\ I'(t) = \lambda SI - m - dI + \eta_2\Psi_2(\mathrm{t}) \end{cases} \tag{3.4}$$

By concentrating just on the consequences of stochastic linear perturbations. Using (3.1) and (3.2),

$$h_1'(t) = r(h_1(t) + S^*)\left(1 - \frac{(h_1(t)+S^*)}{k}\right) - \lambda(h_1(t) + S^*)(h_2(t) + I^*) - d(h_1(t) + S^*) + \eta_1\Psi_1(\mathrm{t}) \tag{3.5}$$

$$I'(t) = \lambda(h_1(t) + S^*)(h_2(t) + I^*) - \varepsilon(h_2(t) + I^*) - d(h_2(t) + I^*) + \eta_2\Psi_2(\mathrm{t}) \tag{3.6}$$

Model (1) is therefore condensed to the simple linear arrangement illustrated below.

$$h_1'(t) = -\frac{2r}{k}h_1(t)S^* - \lambda h_2(t)S^* + \eta_1\Psi_1(\mathrm{t}) \tag{3.7}$$

$$h_2'(t) = \lambda h_1(t)I^* + \eta_2\Psi_2(\mathrm{t}) \tag{3.8}$$

Taking Fourier transform for (3.6)-(3.7) we get,

$$\eta_1\widetilde{\Psi_1}(\omega) = (i\omega)\widetilde{h_1}(\omega) + \frac{2r}{k}\widetilde{h_1}(\omega)S^* + \lambda\widetilde{h_2}(\omega)S^* \tag{3.9}$$

$$\eta_2\widetilde{\Psi_2}(\omega) = (i\omega)\widetilde{h_2}(\omega) - \qquad \widetilde{\quad zzz}\lambda h_1(\omega)I^* \tag{3.10}$$

The matrix form of the equations (3.8) and (3.9) as $\mathrm{P}(\omega)\tilde{h}(\omega) = \widetilde{\Psi}(\omega)$ (3.11)

where P $(\omega)$ $=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

| P $(\omega)$ |=ad-cb

$\tilde{\mathrm{h}}(\omega) = [\widetilde{\mathrm{h}_1}(\omega)\,, \widetilde{\mathrm{h}_2}(\omega)\,]^{\mathrm{T}}$;

$\widetilde{\Psi}(\omega)$= $[\eta_1\Psi_1(\mathrm{t}), \eta_2\Psi_2(\mathrm{t})]^{\mathrm{T}}$;

a=iω $+\frac{2r}{k}$ $S^*$; b=λ$S^*$; c=- λ$I^*$; d= iω;

$$\mathrm{P}\ (\omega) = \begin{bmatrix} i\omega\ + \frac{2r}{k}\ S^* & \lambda S^* \\ -\ \lambda I^* & i\omega \end{bmatrix}$$

$$|\ \mathrm{P}\ (\omega)\ | = -\omega^2 + \frac{2r}{k}\ S^*(i\omega) + \lambda^2 S^* I^*$$

$$\mathrm{adj}[\mathrm{P}(\omega)] = \begin{bmatrix} i\omega & -\lambda S^* \\ \lambda I^* & i\omega + \frac{2r}{k}\ S^* \end{bmatrix}$$

As an alternative, equation (3.10) can be expressed as

$$\tilde{h}(\omega) = [\ \mathrm{P}\ (\omega)]^{-1}\widetilde{\Psi}(\omega) \tag{3.12}$$

$$[\ \mathrm{P}\ (\omega)]^{-1} = \mathrm{Q}(\omega) \tag{3.13}$$

Where $\mathrm{Q}(\omega) = \frac{\mathrm{adj}[\ \mathrm{P}(\omega]}{|\mathrm{P}(\omega)|}$ (3.14)

$$\mathrm{Q} = \frac{1}{-\omega^2 + \frac{2r}{k}S^*(i\omega) + \lambda^2 S^* I^*}\begin{bmatrix} i\omega & -\lambda S^* \\ \lambda I^* & i\omega + \frac{2r}{k}\ S^* \end{bmatrix}$$

$a_{11} = i\omega;\ a_{12} = -\lambda S^*; b_{11} = \lambda I^*; b_{12} =\ i\omega + \frac{2r}{k}\ S^*$

The variations in the intensity of the variable, denoted as $h_{\mathrm{i}}$ where i ranges from 1 to 2, are provided.

$$\sigma_{h_i}{}^2 = \frac{1}{2\pi}\sum_{i=1}^{2}\int_{-\infty}^{\infty} \propto_i \left|\mathrm{Q}_{ij}(\omega)\right|^2 d\omega;\ \mathrm{i=1,2} \tag{3.15}$$

Variance of $h_i$ , i =1,2 are calculated as

$$\sigma_{h_1}{}^2 = \frac{1}{2\pi}\int_{-\infty}^{\infty} \propto_1 \left|\frac{a_{11}}{|\mathrm{P}(\omega)|}\right|^2 d\omega + \int_{-\infty}^{\infty} \propto_2 \left|\frac{a_{12}}{|\mathrm{P}(\omega)|}\right|^2 d\omega \tag{3.16}$$

$$\sigma_{h_1}{}^2 = \frac{1}{2\pi}\int_{-\infty}^{\infty} \propto_1 \left|\frac{i\omega}{-\omega^2 + \frac{2r}{k}S^*(i\omega) + \lambda^2 S^* I^*}\right|^2 d\omega + \int_{-\infty}^{\infty} \propto_2 \left|\frac{-\lambda S^*}{-\omega^2 + \frac{2r}{k}S^*(i\omega) + \lambda^2 S^* I^*}\right|^2 d\omega \tag{3.17}$$

$$\sigma_{h_2}{}^2 = \frac{1}{2\pi}\int_{-\infty}^{\infty} \propto_1 \left|\frac{b_{11}}{|\mathrm{P}(\omega)|}\right|^2 d\omega + \int_{-\infty}^{\infty} \propto_2 \left|\frac{b_{12}}{|\mathrm{P}(\omega)|}\right|^2 d\omega \tag{3.18}$$

$$\sigma_{h_2}{}^2 = \frac{1}{2\pi}\int_{-\infty}^{\infty} \propto_1 \left|\frac{\lambda I^*}{-\omega^2 + \frac{2r}{k}S^*(i\omega) + \lambda^2 S^* I^*}\right|^2 d\omega + \int_{-\infty}^{\infty} \propto_2 \left|\frac{i\omega + \frac{2r}{k}S^*}{-\omega^2 + \frac{2r}{k}S^*(i\omega) + \lambda^2 S^* I^*}\right|^2 d\omega \tag{3.19}$$

(i)When $\propto_1 = 0; \propto_2 = 0$ then $\sigma_{h_1}{}^2 = \sigma_{h_2}{}^2 = 0$ (3.20)

(ii)When $\propto_2 = 0$, then

$$\sigma_{h_1}{}^2 = \frac{\propto_1}{2\pi}\int_{-\infty}^{\infty} \frac{\omega^2}{(-\omega^2 + \frac{2r}{k}S^*(i\omega) + \lambda^2 S^* I^*)^2}\ d\omega \tag{3.21}$$

$$\sigma_{h_2}{}^2 = \frac{\propto_1}{2\pi}\int_{-\infty}^{\infty} \frac{(\lambda I^*)^2}{(-\omega^2 + \frac{2r}{k}S^*(i\omega) + \lambda^2 S^* I^*)^2}\ d\omega \tag{3.22}$$

(iii)When $\propto_1 = 0$, then

$$\sigma_{h_1}{}^2 = \frac{\propto_2}{2\pi}\int_{-\infty}^{\infty} \frac{(\lambda S^*)^2}{(-\omega^2 + \frac{2r}{k}S^*(i\omega) + \lambda^2 S^* I^*)^2}\ d\omega \tag{3.23}$$

$$\sigma_{h_2}{}^2 = \frac{\propto_2}{2\pi}\int_{-\infty}^{\infty} \frac{(i\omega + \frac{2r}{k}S^*)^2}{(-\omega^2 + \frac{2r}{k}S^*(i\omega) + \lambda^2 S^* I^*)^2}\ d\omega \tag{3.24}$$

Larger the intensity more chance for network to get unstable or infected.

## 4. NUMERICAL SIMULATIONS:

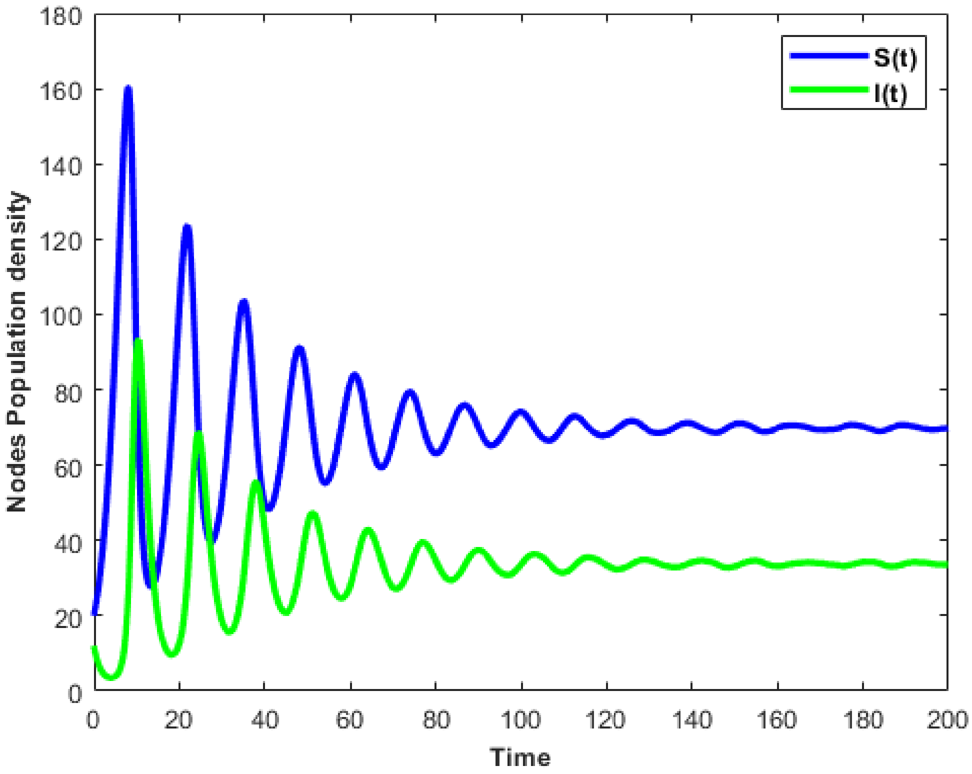

Fig 1(a)

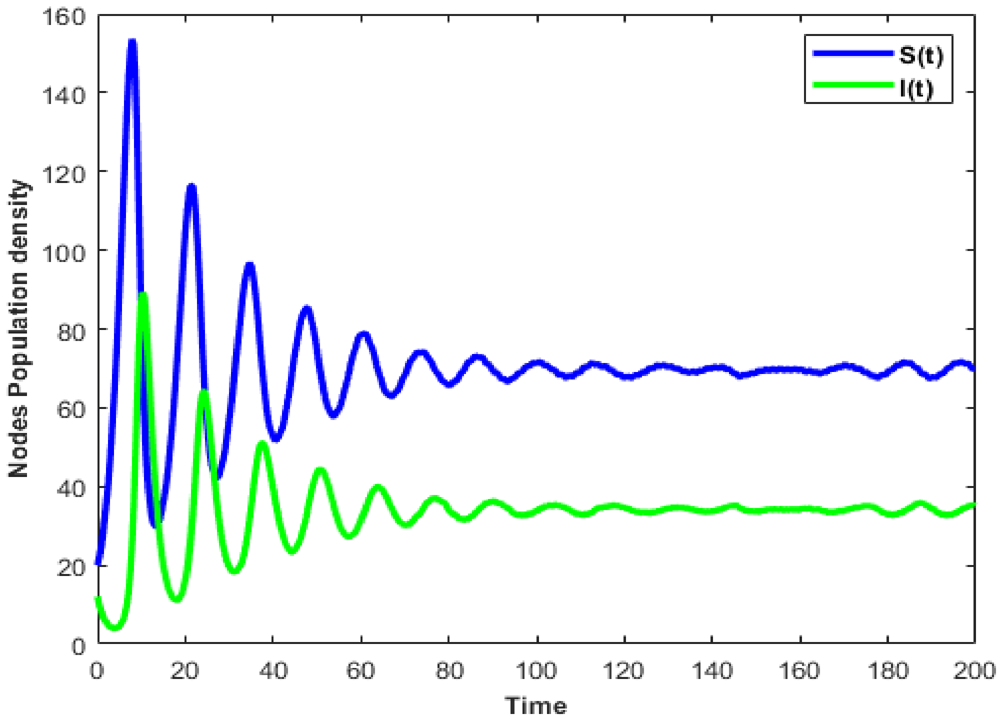

Fig 1(b)

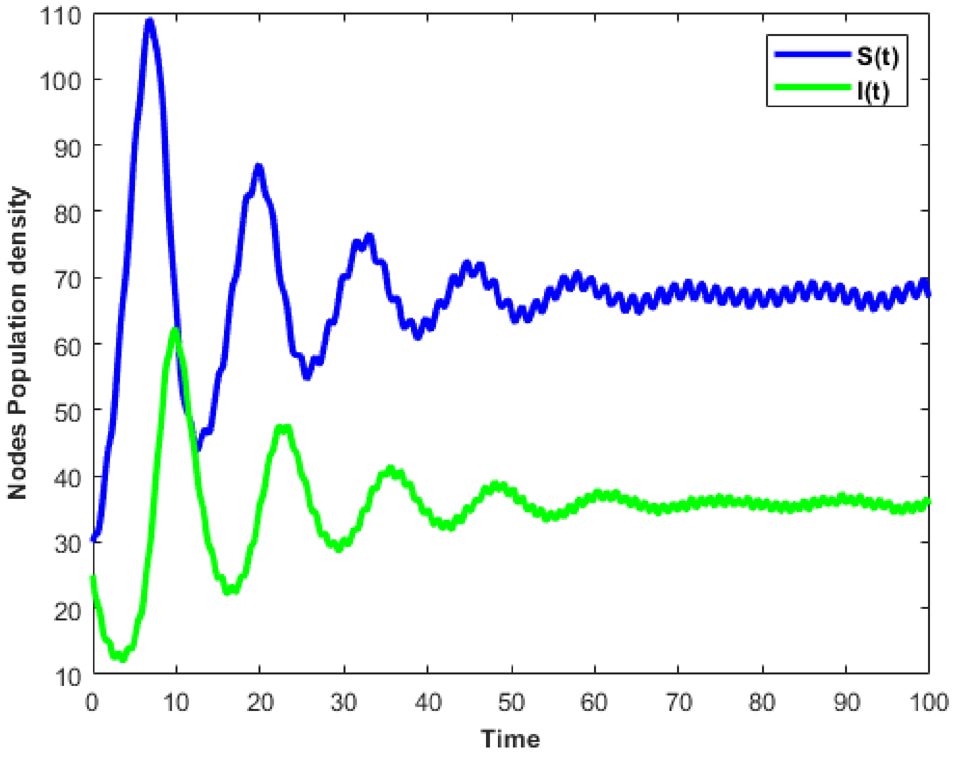
Nodes Population density
Time
S(t)
I(t)
110
100
90
80
70
60
50
40
30
20
10
0
10
20
30
40
50
60
70
80
90
100

Fig 1(c)

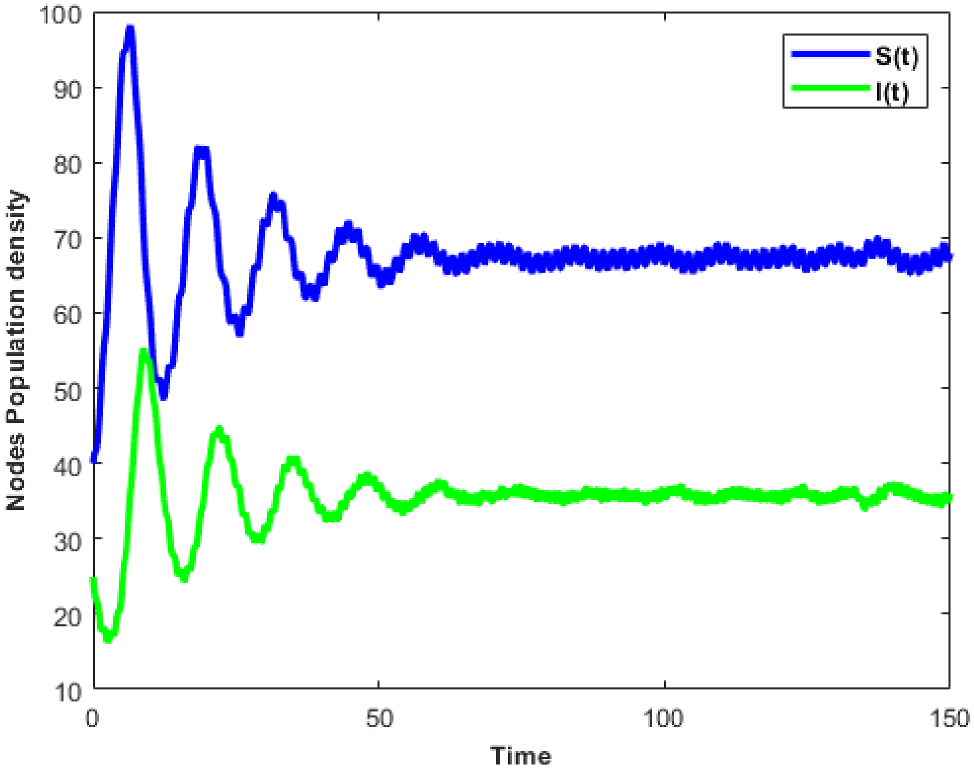
Nodes Population density
Time
S(t)
I(t)
100
90
80
70
60
50
40
30
20
10
0
50
100
150

Fig 1(d)

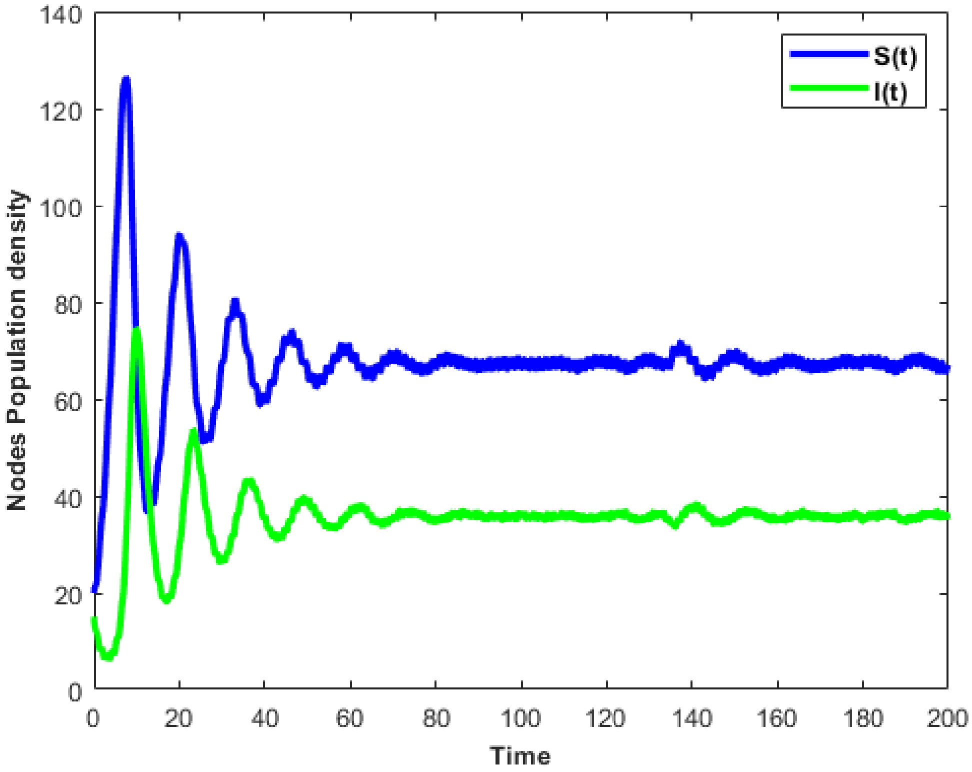
S(t)
I(t)
Nodes Population density
Time
0
20
40
60
80
100
120
140
0
20
40
60
80
100
120
140
160
180
200

Fig 1(e)

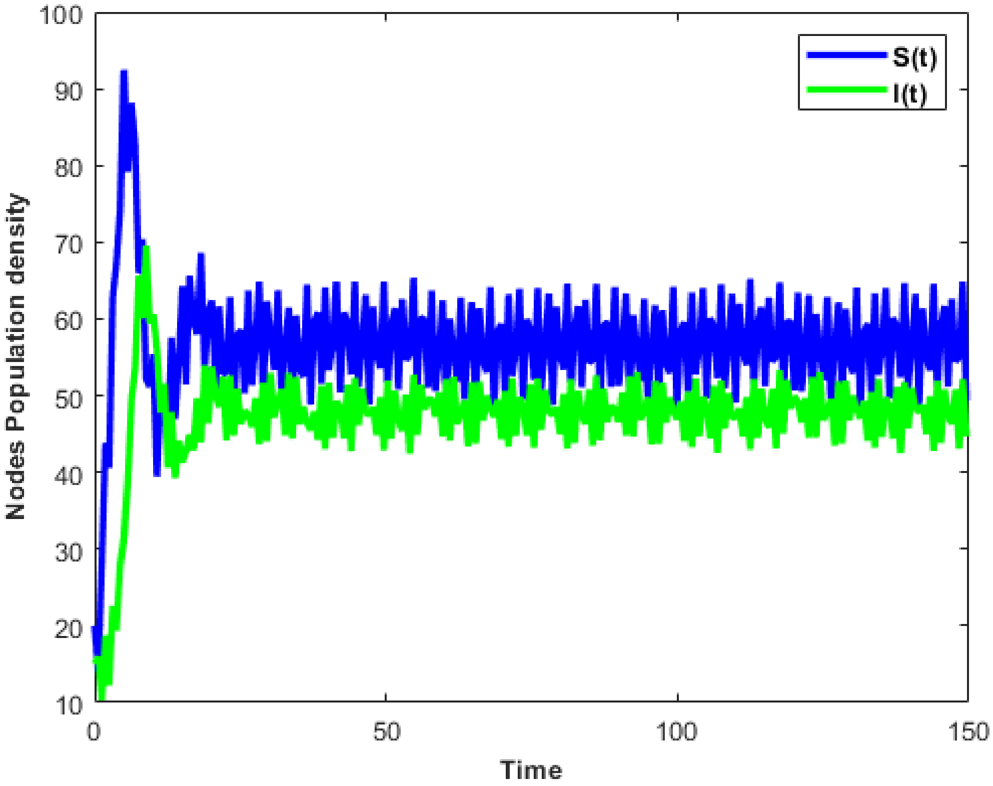
S(t)
I(t)
Nodes Population density
Time
10
20
30
40
50
60
70
80
90
100
0
50
100
150

Fig 1(f)

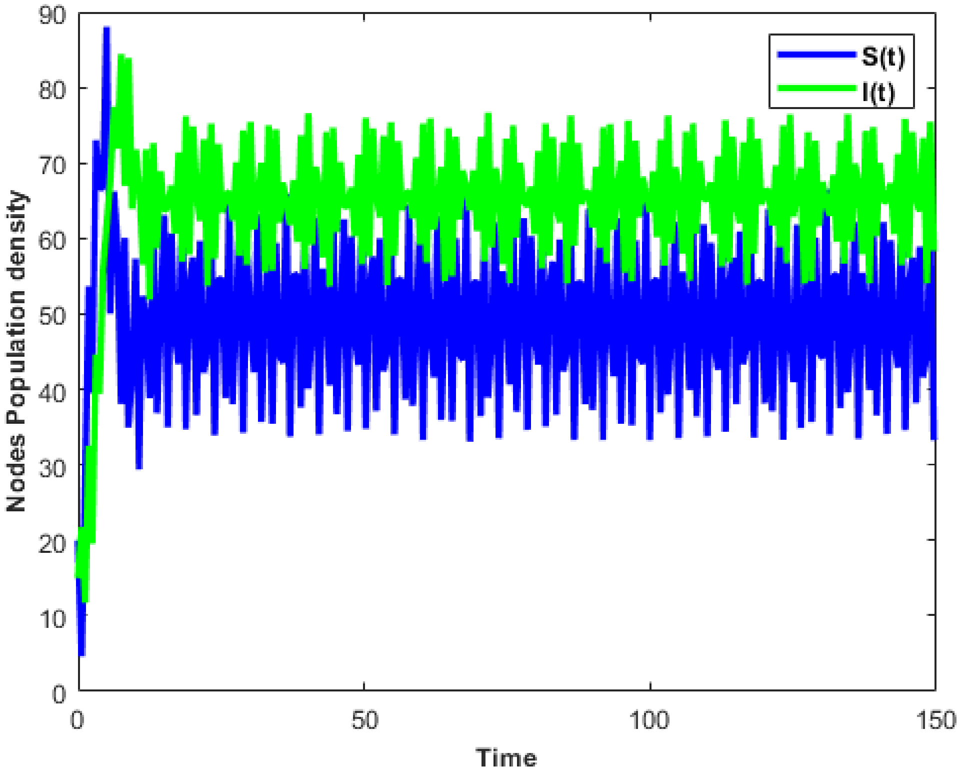
S(t)
I(t)
Nodes Population density
Time
0
10
20
30
40
50
60
70
80
90
0
50
100
150

Fig 1(g)

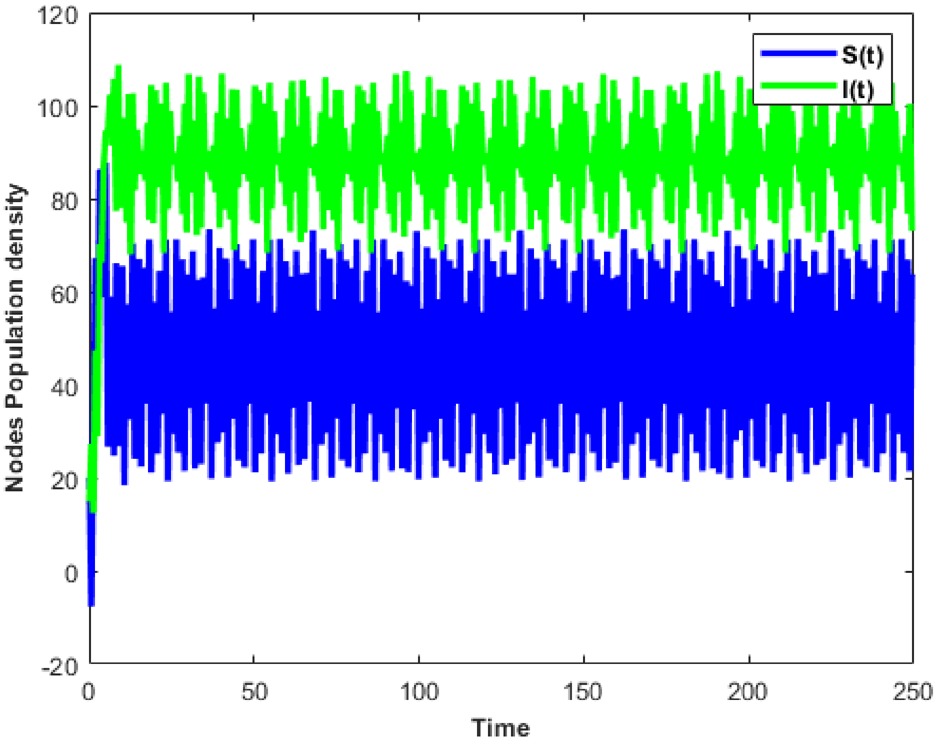
S(t)
I(t)
Nodes Population density
Time
-20
0
20
40
60
80
100
120
0
50
100
150
200
250

Fig 1(h)

Figures 1(a) to 1(h) are the time series projections of susceptible and infected nodes population with the values of attributes as $k$=1000; $\lambda$=0.01; $\varepsilon$=0.2; d=0.1; r=0.9; for various noise intensities 0.002;0.001 (for Fig 1(a)), 0.02;0.01(for Fig 1(b)), 1;0.9 (for Fig 1(c)), 6;5 (for Fig 1(d)), 12;10 (for Fig 1(e)), 30;25(for Fig 1(f)), 60;55 (for Fig 1(g)), 100;85 (for Fig 1(h)).

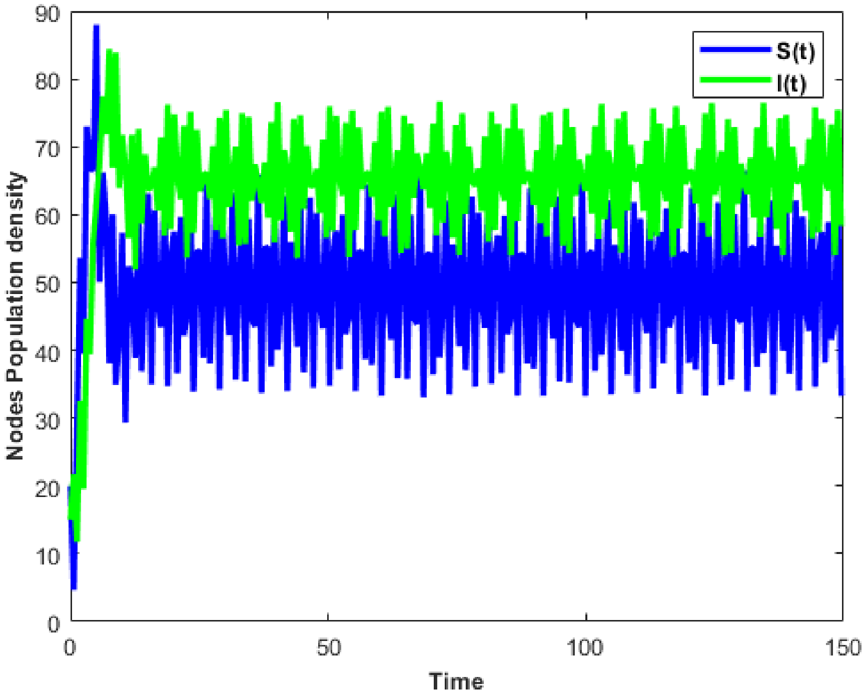

Fig 1(g)

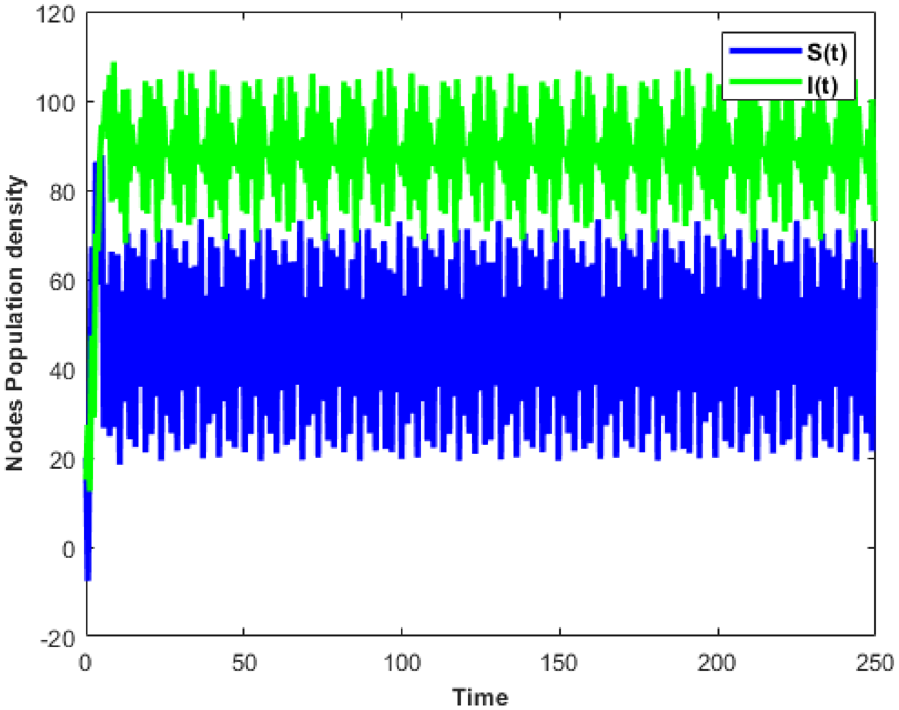

Fig 1(h)

Figures 1(g) and 1(h) are the time series projections of susceptible and infected nodes population with the values of attributes as k=1000; λ=0.01; ε=0.2; d=0.1; r=0.9; for various noise intensities 60;55 (for Fig 1(g)), 100;85 (for Fig 1(h)).

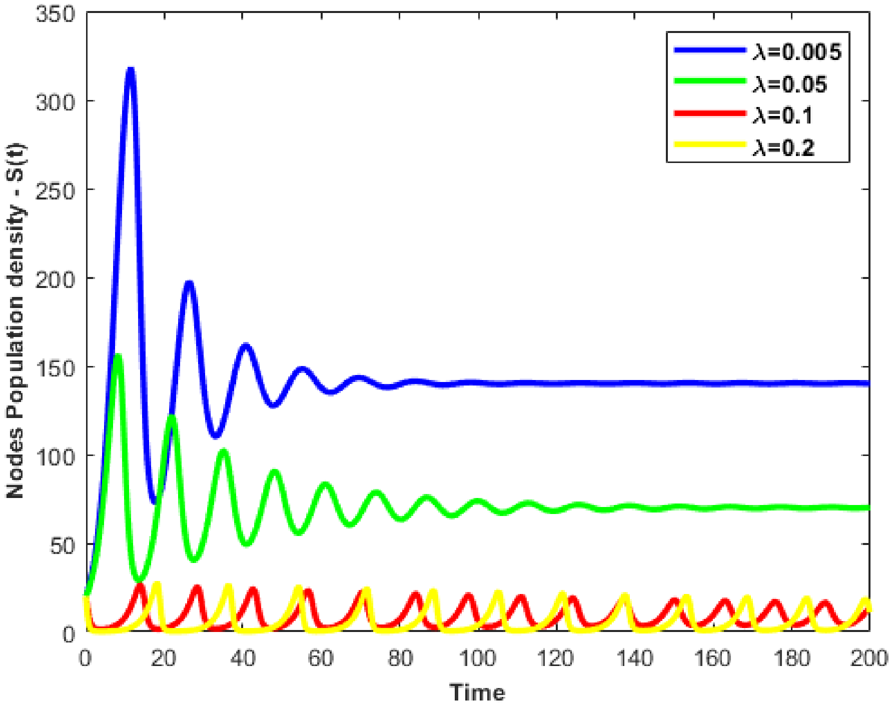

Fig 2(a)

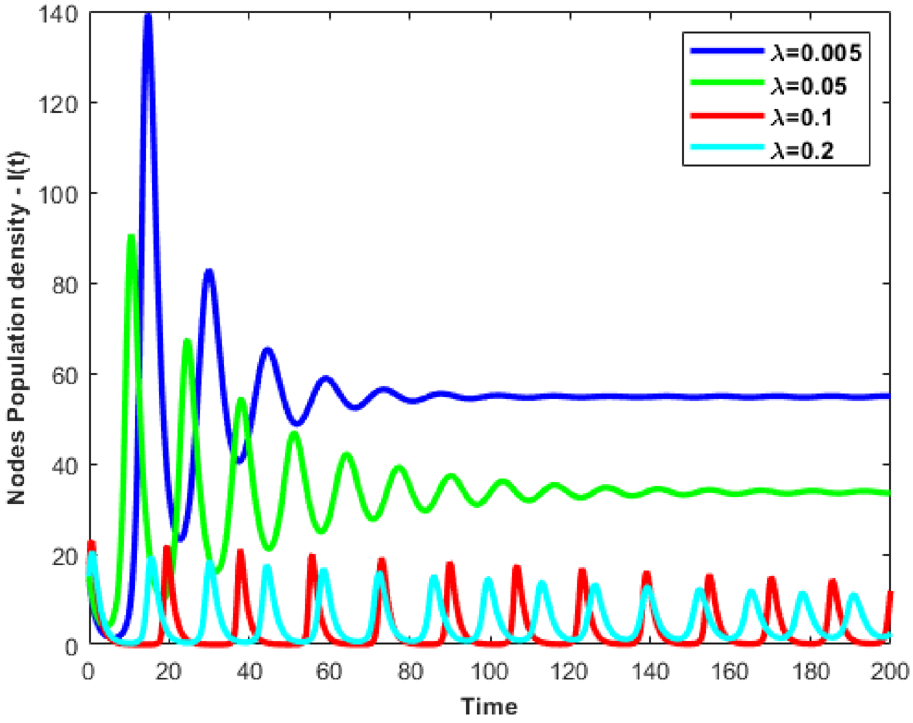

Fig 2(b)

Figure 2(a) shows the variation in susceptible nodes and Figure 2(b) shows the variation in infected nodes for various values of $\lambda$=0.005;0.05;0.1;0.2 along with other attributes $k$=1000; $\varepsilon$=0.2; d=0.1; r=0.9.

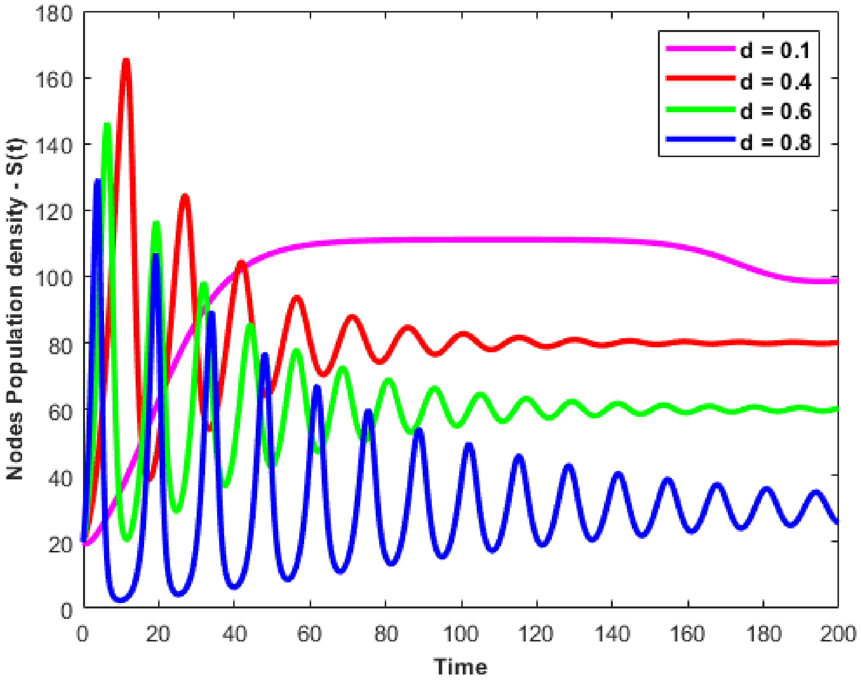

Fig 3(a)

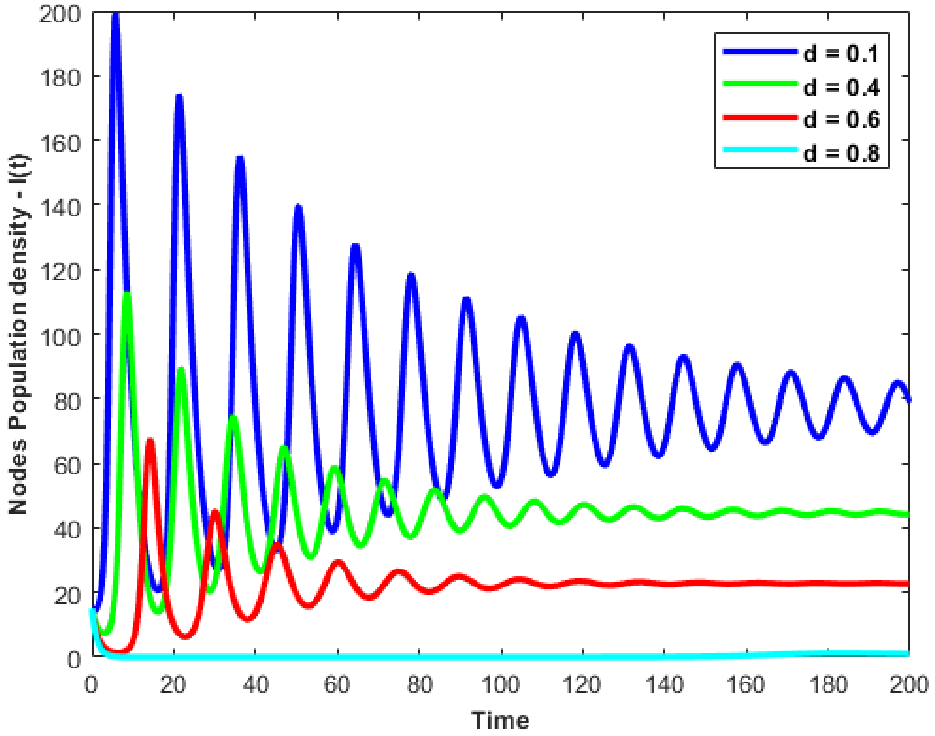

Fig 3(b)

Figure 3(a) shows the variation in susceptible nodes and Figure 3(b) shows the variation in infected nodes for various values of d=0.1;0.3;0.6;0.9 along with other attributes $k$=1000; $\lambda$=0.01; $\varepsilon$=0.2; r=0.9;.

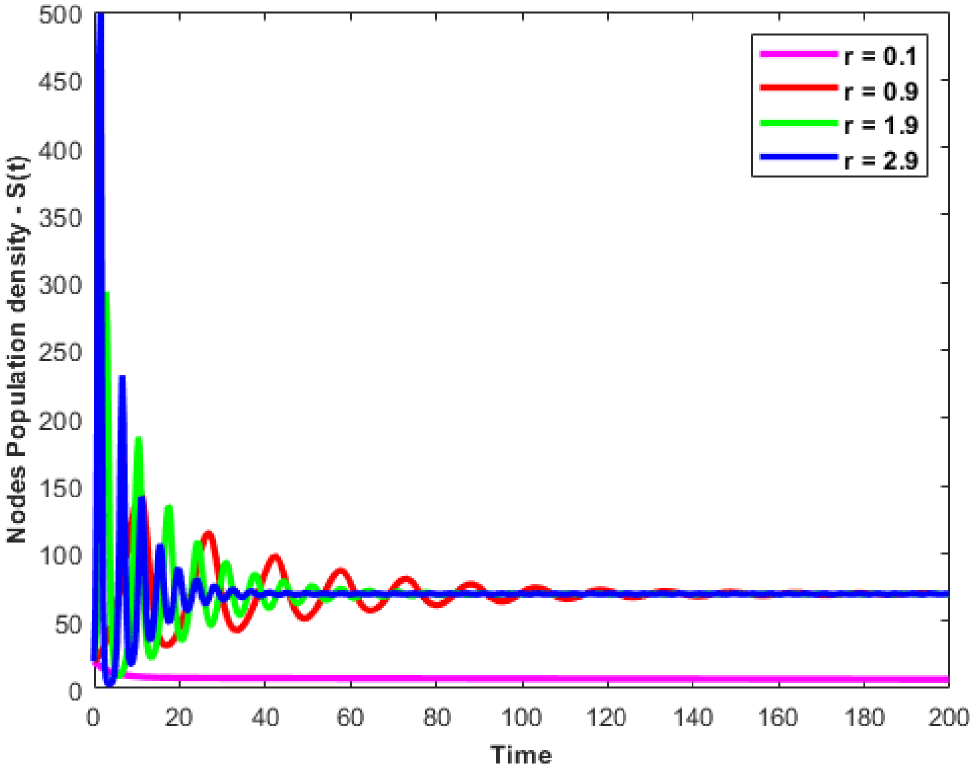

Fig 4(a)

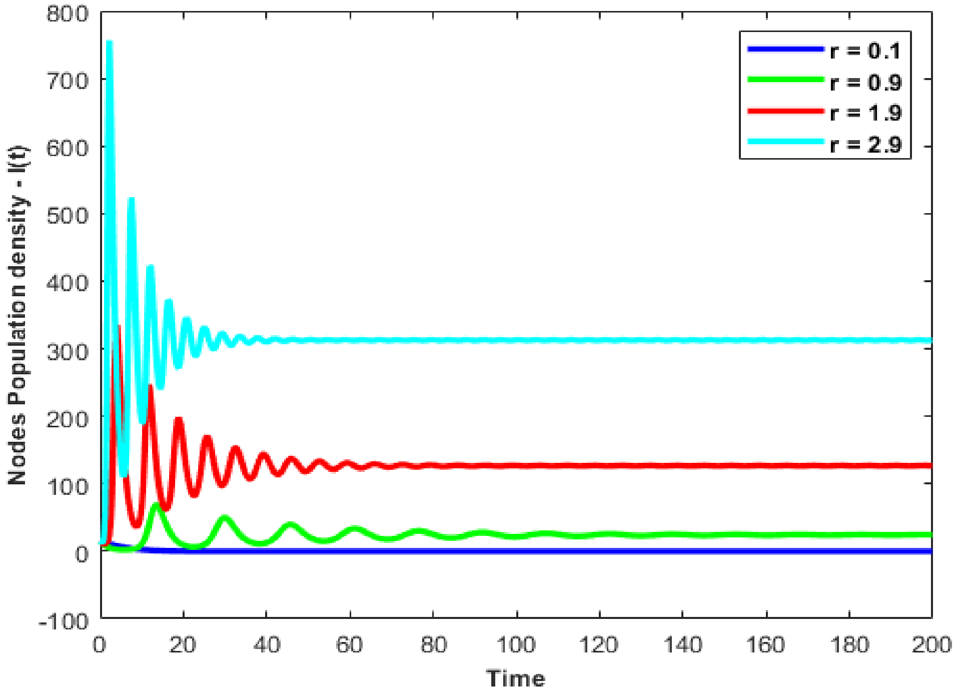

Fig 4(b)

Figure 4(a) shows the variation in susceptible nodes and Figure 4(b) shows the variation in infected nodes for various values of r=0.1;0.9;1.9;2.9 along with other attributes *k*=1000; $\lambda$=0.01; $\varepsilon$=0.2; d=0.1.

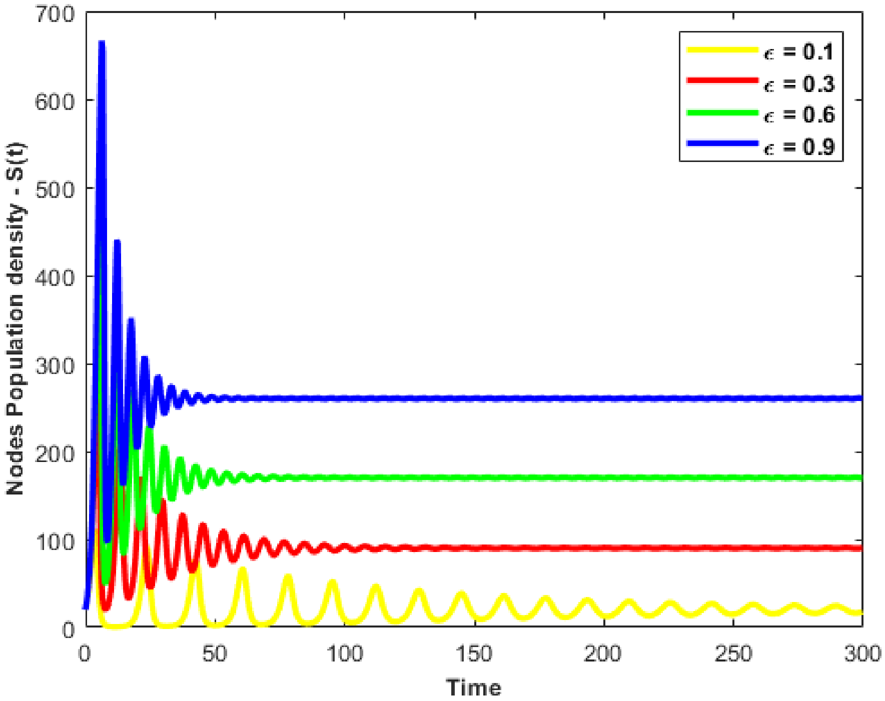

Fig 5(a)

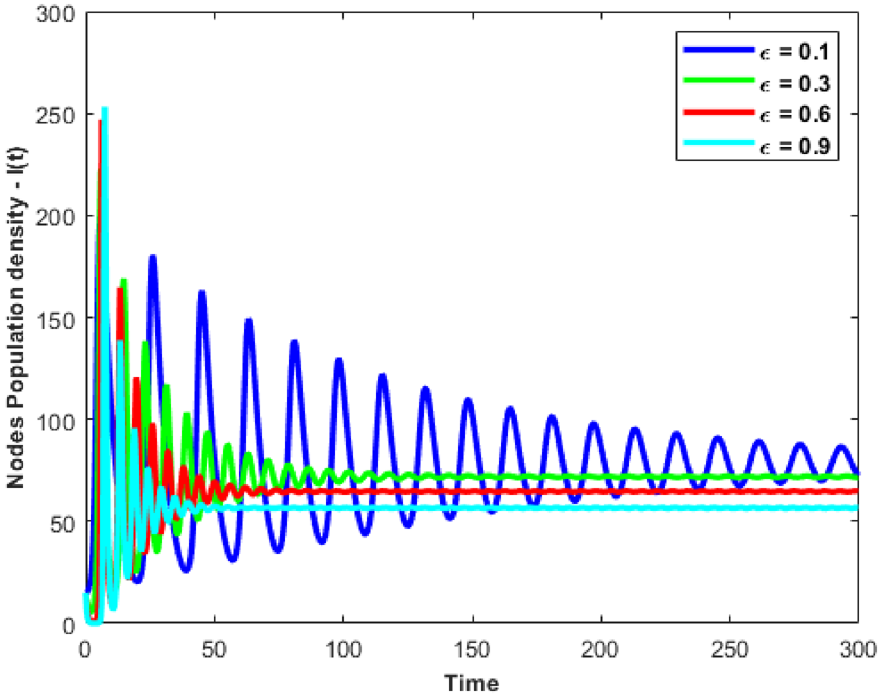

Fig 5(b)

Figure 5(a) shows the variation in susceptible nodes and Figure 5(b) shows the variation in infected nodes for various values of $\varepsilon$=0.1;0.3;0.6;0.9 along with other attributes $k$=1000; $\lambda$=0.01; d=0.1; r=0.9.

## 5. CONCLUDING REMARKS

In this paper, we consider the impact of anti-virus capability on the network and offer a unique computer virus propagation model over a network. Among our principal contributions are the following: We examined the stochastic analysis using Fourier transform and derived a set of standards for evaluating its stability. These findings could contribute to our understanding of the regulations controlling the transmission of computer viruses over networks. It is crucial to gather a significant amount of pertinent data, estimate the model's parameters using stochastic analysis, the network's behaviour using our model, and observed that  the network in order to assess the efficacy of our model when applied to a real-world network. The model may be effective if the network's behaviour closely matches to our observations of stochastic graphs. Stochasticity remarkably influences the proposed system at higher values of noise intensities. Parameter variation also influences the system greatly, which is presented well with the help of graphical results using simulation software MATLAB.  Hacking and different practices and process involved in hacking are the main gateways for the malware enter into any devices which collapse the system greatly is addressed in this article with the help of stochastic modelling and graphical parameter variation analysis on the proposed system.

## REFERENCES

1. J.L. Aron, M. O'Leary, R.A. Gove, S. Azadegan, M.C. Schneider, The benefits of a notification process in addressing the worsening computer virus problem: results of a survey and a simulation model, Computers and Security 21 (2002) 142–163.
2. Y.B. Kafai, Understanding virtual epidemics: children's folk conceptions of a computer virus, Journal of Science Education and Technology 6 (2009) 523–529.
3. B. Mishra, N. Jha, Fixed period of temporary immunity after run of anti-malicious software on computer nodes, Applied Mathematics and Computation 190 (2007) 1207–1212.
4. B.K. Mishra, N. Jha, Fixed period of temporary immunity after run of anti-malicious software on computer nodes, Applied Mathematics and Computation 190 (2007) 1207–1212.
5. Wierman JC, Marchette DJ. Modelling computer virus prevalence with a susceptible-infected-susceptible model with reintroduction. Compute Stat Data An 2004;45: 3–23.
6. B.K. Mishra, S.K. Pandey, Effect of anti-virus software on infectious nodes in computer network: a mathematical model phys. Lett. A 376 (2012) 2389-2393.
7. W.O. Kermack, A.G. McKendrick, Proc. R. Soc. London – Series A 141 (1933) 94.
8. Barthélemy M, Barrat A, Pastor-Satorras R, Vespignani A. Velocity and hierarchical spread of epidemic outbreaks in scale-free networks. Phys Rev Lett 2004;92(7) (Article ID 178701).
9. Karsai M, Kivelä M, Pan RK, Kaski K, Kertész J, Barabási A-L, Saramäki J. Small but slow world: How network topology and burstiness slow down spreading. Phys Rev E 2011;83(2) (Article ID 025102).
10. Pastor-Satorras R, Vespignani A. Epidemic spreading in scale-free networks. Phys Rev Lett 2001;86(14):3200–3.
11. Pastor-Satorras R, Vespignani A. Epidemic dynamics and endemic states in complex networks. Phys Rev E 2001;63(6) (Article ID 066117).
12. Lloyd AL, May RM. How viruses spread among computers and people. Science 2001;292(5520):1316–7.
13. Pastor-Satorras R, Vespignani A. Immunization of complex networks. Phys Rev E 2002;65(3) (Article ID 036104).
14. Dezsö Z, Barabási A-L. Halting viruses in scale-free networks. Phys Rev E 2002;65(5) (Article ID 055103).
15. Billings L, Spears WM, Schwartz IB. A unified prediction of computer virus spread in connected networks. Phys Lett A 2002;297(3–4):261–6.
16. Boguñá M, Pastor-Satorras R, Vespignani A. Absence of epidemic threshold in scale-free networks with degree correlations. Phys Rev Lett 2003;90(2) (Article ID 028701).
17. Wierman JC, Marchette DJ. Modeling computer virus prevalence with a susceptible-infected-susceptible model with reintroduction. Comput Stat Data Anal 2004;45(1):3–23.

18. Griffin C, Brooks R. A note on the spread of worms in scale-free networks. IEEE Trans Syst Man Cybern – Part B: Cybern 2006;36(1):198–202.
19. Fu X, Small M, Walker DM, Zhang H. Epidemic dynamics on scale-free networks with piecewise linear infectivity and immunization. Phys Rev E 2008;77(3) (Article ID 036113).
20. Castellano C, Pastor-Satorras R. Thresholds for epidemic spreading in networks. Phys Rev Lett 2010;105(21) (Article ID 218701).
21. Moreno Y, Pastor-Satorras R, Vespignani A. Epidemic outbreaks in complex heterogeneous networks. Eur Phys J B 2002;26(4):521–9.
22. Chen L-C, Carley KM. The impact of countermeasure propagation on the prevalence of computer viruses. IEEE Trans Syst Man Cybern – Part B 2004; 34(2):823–33.
23. Draief M, Ganesh A, Massouilié L. Thresholds for virus spread on networks. Ann Appl Probab 2008; 18(2):359–78
24. Erol Gelenbe, in: Computer and Information Sciences – ISCIS 2005, 20th International Symposium, in: Lecture Notes in Computer Science, vol. 3733, Springer, 2005, pp. 304–311.
25. M.E.J. Newman, S. Forrest, J. Balthrop, Phys. Rev. E 66 (2002) 232.
26. C.C. Zou, W.B. Gong, D. Towsley, L.X. Gao, The monitoring and early detection of internet worms, IEEE/ACM Trans. Network 13 (5) (2005) 961–974.
27. N. Madar, T. Kalisky, R. Cohen, D. Ben Avraham, S. Havlin, Immunization and epidemic dynamic in complex networks, Eur. Phys. J.B 38 (2004) 269–276.
28. Bimal Kumar Mishra, Prasant Kumar Nayak, Navnit Jha, Effect of quarantine nodes in SEQIAmS model for the transmission of malicious objects in computer network, Int. J. Math. Model. Simul. Appl. 2 (1) (2009) 102–113.
29. J. Ren, X. Yang, Q. Zhu, C. Zhang L-X Yang, A novel computer virus model and its dynamics, Nonlinear Anal. RWA 13 (2012) 376–384.
30. J.R.C. Piqueira, V.O. Araujo, A modified epidemiological model for computer viruses, Appl. Math. Comput. 213 (2009) 355–360.
31. D.K. Saini, A mathematical model for the effect of malicious object on computer network immune system, Appl. Math. Model. 35 (2011) 3777–3787.