

QUARANTINE-BASED SEIRA MALWARE PROPAGATION MODEL FOR COMPUTER NETWORKS

Md Mridul Haque Choudhury^{1*} and Hemen Bharali²

¹*Department of Mathematics, Assam Don Bosco University*

²*Department of Mathematics, Assam Don Bosco University*

*For correspondence (mridulchoudhury.bcm@gmail.com)

Abstract: One of the high-profile issue of computer networks is the propagation of Malware and it get disrupted by the malware's presence. In this study, we extend the classical SEIRA (Susceptible–Exposed–Infectious–Recovered–Antidotal) model by including a quarantined compartment (Q) to represent infected machines that are detected and isolated from the network. In the SEIQRA model, the quarantine approach has been used to halt the infection spread in computer networks. The model's basic reproduction number (R_0) is derived using next generation approach. We examined the model's local stability in terms in the system's Jacobian for malware free and endemic equilibrium based on the basic reproduction number. Numerical simulations demonstrate that higher quarantine rates and stricter isolation significantly reduce the peak infection size and overall outbreak impact. In order to effectively contain malware, the model emphasizes the significance of integrating quarantine with protective adoption and recovery methods. Finally, numerical methods and MATLAB are employed to solve and simulate the system of equations developed and analysis of the model gives remarkable exposure.

Keywords: Malware propagation, Epidemic model, Basic reproduction number, Mathematical modeling, Computer network, Stability, Numerical simulation.

1. Introduction:

At present, the secondary devices and Electronic mail constitute the primary sources of malware transmission in computer networks. Malware has emerged as one of the most persistent dangers to information security due to the quick expansion of computer networks and the increasing reliance on virtual infrastructure [1]. Malware propagation, near to infectious disease transmission in biological systems, can compromise large-scale networks within a brief period [2]. The technology of data networks has advanced significantly, offering both public and private facilities that are precise and quick. This advancement has transformed the mode of data transmission in society, leading to a strong reliance on communication services across all levels of interaction [3]. Researchers have chosen compartmental epidemic models like SIR, SEIR, and its extensions to comprehend and manage these dynamics [4, 5]. These models provide mathematical framework for analyzing malware spreads and designing efficient countermeasures.

Cohen [6] and Murray [7] presented new methods for exploring the infectious disease dynamics and epidemics that could be used to analyze the computer viruses spread, and is inspired by notable resemblance between digital viruses and their biological counterparts. Subsequently, to analyze the computer viruses spread through Internet, the authors in [8] used a biological epidemics model (the SIS model). It is possible to research how malware propagate via networks using several epidemiological models. The SIR classical epidemic model and Kermack and McKendrick [9–11] were used to examine the distribution of malware in networks [12–16]. The SEIR model, which was developed by the authors [17], is inconsistent with the actual scenario since it presupposes that the vaccination period for recovery hosts is permanent and has a set probability. Including the latent and transitory immune phases, the authors proposed a SEIRS model [18] that can be employed to detect common worm propagation. Recent studies have increasingly integrated virus propagation models with antivirus strategies, including virus immunization [19–25] and quarantine [26–29] to address the computer virus-dynamics. Employing quarantine within the epidemic framework, Mishra et al. developed the SEIQRS model [30]. The SEIRA model, which classifies the nodes into Susceptible (S), Exposed (E), Infectious (I), Recovered (R), and Antidotal (A), has been frequently used in research propagation patterns under various defensive

scenarios [5]. Though, a critical relief design—quarantine remains unknown in this context [1, 31]. In computer networks, quarantine corresponds to detecting infected machines and isolating them from the network, thereby reducing or eliminating their ability to propagate malicious code [1]. Quarantine is routinely applied in practice through intrusion detection systems, firewalls, and automated disconnection policies, but its theoretical integration into epidemic-style malware models has been limited [31, 32].

By including a confined compartment to the SEIRA model, this research aims to bridge the gap (Q) [1, 31]. This enhanced model facilitates a comprehensive assessment of how detection speed, impact of isolation, and remedial strategies affect malware propagation [5, 32]. Specially, we formulate the differential equation system, calculate the basic reproduction number, analyze equilibrium stability, and perform numerical simulations to assess the efficacies of quarantine under different conditions [32, 33]. Combining theoretical observations with numerical evidence, the present study underscores the crucial role of quarantine in lowering infection peaks and mitigating outbreaks [1, 33].

The structure of the paper: **Section 1** provides an introduction to the study. **Section 2** presents the formulation of the SEIQRA model. The model's equilibrium points are presented in **Section 3**. **Section 4** focuses on the stability analysis. **Section 5** illustrates the numerical methods and simulation results. **Section 6** concludes the paper with final remarks.

2. Formulation of SEIQRA model:

A population size $N(t)$ is partitioned into subclasses of nodes as susceptible, exposed (infected but not yet infectious), infectious, quarantined, recovered, and antidotal represented by $S(t)$, $E(t)$, $I(t)$, $Q(t)$, $R(t)$, and $A(t)$, respectively at any given time $t \geq 0$.

Figure 1 illustrates our predictions regarding malware transmission in computer nodes.

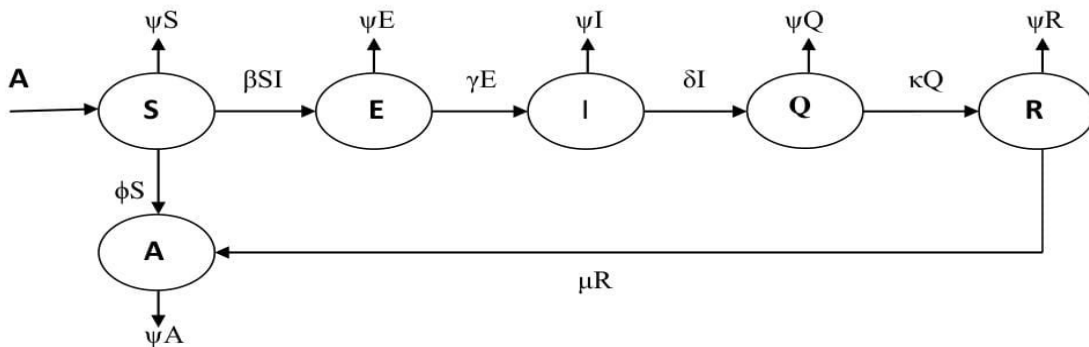


Figure 1: Malware Propagation Flow Diagram in Computer Networks.

The differential equations set governing the nodes' transition state in the SEIQRA model is as follows:

$$\frac{dS}{dt} = e - \beta SI - \phi S - \psi S$$

$$\frac{dE}{dt} = \beta SI - \gamma E - \psi E$$

$$\frac{dI}{dt} = \gamma E - \delta I - \psi I$$

$$\frac{dQ}{dt} = \delta I - \kappa Q - \psi Q$$

$$\frac{dR}{dt} = \kappa Q - \mu R - \psi R$$

$$\frac{dA}{dt} = \phi S + \mu R - \psi A \quad (1)$$

Where

e: recently added nodes to the network

Ψ : rate of natural death in each compartment

β : rate of contact from S to E

γ : exposure rate from E to I

ϕ : prophylactic patching rate from S to A

δ : rate of quarantine from I to Q

κ : recovery rate inside quarantine from Q to R

μ : rate of recovered nodes gain antidote from R to A

3. Points of equilibrium in the system:

Two distinct kinds of equilibrium points are analyzed. In the first condition, when the malware infection dies out, then $I=0$, and in the second condition, when the malware infection exists in the computer network, then $I \neq 0$. Hence, the system of equations (1) are presented as

$$\begin{aligned} \frac{ds}{dt} &= e - \beta SI - \phi S - \psi S &= 0 \\ \frac{dE}{dt} &= \beta SI - \gamma E - \psi E &= 0 \\ \frac{dI}{dt} &= \gamma E - \delta I - \psi I &= 0 \\ \frac{dQ}{dt} &= \delta I - \kappa Q - \psi Q &= 0 \\ \frac{dR}{dt} &= \kappa Q - \mu R - \psi R &= 0 \\ \frac{dA}{dt} &= \phi S + \mu R - \psi A &= 0 \end{aligned} \quad (2)$$

3.1. Malware Free Equilibrium:

When the system of equation (2) is solved for malware free equilibrium (MFE), we obtain $P_0 = (S_0, E_0, I_0, Q_0, R_0, A_0)$, where

$$S_0 = \frac{e}{\phi + \psi}, \quad E_0 = 0, \quad I_0 = 0, \quad Q_0 = 0, \quad R_0 = 0, \quad A_0 = \frac{e\phi}{\psi(\phi + \psi)}$$

3.2. The Basic Reproduction Number:

The estimated quantity of secondary cases that would result from introducing a single main spreading case into an area that is entirely susceptible is referred to as the basic reproduction number [34]. With the help of next-generation matrix technique the basic reproduction number (R_0) is determined. Since the model includes three infected classes E, I, and Q, we only need to consider the three corresponding equations from system (1) that describe these classes in order to derive the basic reproduction number (R_0). That is,

$$\begin{aligned}\frac{dE}{dt} &= \beta SI - \gamma E - \psi E \\ \frac{dI}{dt} &= \gamma E - \delta I - \psi I \\ \frac{dQ}{dt} &= \delta I - \kappa Q - \psi Q\end{aligned}\quad (3)$$

If $X = (E, I, R)$, (3) can be expressed as follows:

$$\frac{dX}{dt} = F - V \quad (4)$$

Where,

$$F = \begin{pmatrix} \beta SI \\ 0 \\ 0 \end{pmatrix} \text{ and } V = \begin{pmatrix} \gamma E + \psi E \\ -\gamma E + \delta I + \psi I \\ -\delta I + \kappa Q + \psi Q \end{pmatrix}$$

At the equilibrium point P_0 , which represents the malware-free state of the system, the Jacobian Matrices F and V are derived as follows:

$$f = \left(\frac{\partial F}{\partial X} \right) | P_0 = \begin{pmatrix} 0 & \beta S_0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \frac{e\beta}{\phi+\psi} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (5)$$

$$v = \left(\frac{\partial V}{\partial X} \right) | P_0 = \begin{pmatrix} \gamma + \psi & 0 & 0 \\ -\gamma & \delta + \psi & 0 \\ 0 & -\delta & \kappa + \psi \end{pmatrix} \quad (6)$$

Equation (7) provides the greatest matrix eigenvalue of the f_V^{-1} matrix, which is the basic reproduction number R_0

$$f_V^{-1} = \begin{pmatrix} \frac{e\beta\gamma}{(\phi+\psi)(\gamma+\psi)(\delta+\psi)} & \frac{e\beta}{(\phi+\psi)(\gamma+\psi)(\delta+\psi)} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (7)$$

We can then determine R_0 .

$$R_0 = \rho(f_V^{-1}) = \frac{e\beta\gamma}{(\phi+\psi)(\gamma+\psi)(\delta+\psi)}, \text{ with } \rho \text{ being the spectral radius.} \quad (8)$$

3.3. Endemic Equilibrium Point:

In a population where the disease is prevalent, $I \neq 0$. The model's endemic equilibrium point (EEP), $I \neq 0$, could have a number of critical points. The following points will be indicated by, $P_e^* = (S^*, E^*, I^*, Q^*, R^*, A^*)$ where $S^*, E^*, I^*, Q^*, R^*, A^*$ symbolize the set of system (2)'s positive solution.

When we solve equation (2), we obtain

$$S^* = \frac{(\gamma + \psi)(\delta + \psi)}{\beta\gamma}$$

$$E^* = \frac{e}{\gamma + \psi} - \frac{(\delta + \psi)(\phi + \psi)}{\beta\gamma} = \frac{e}{\gamma + \psi} \left(1 - \frac{1}{R_0} \right)$$

$$I^* = \frac{e\gamma}{(\gamma + \psi)(\delta + \psi)} - \frac{\phi + \psi}{\beta} = \frac{e\gamma}{(\gamma + \psi)(\delta + \psi)} \left(1 - \frac{1}{R_0} \right)$$

$$Q^* = \frac{\delta\{e\beta\gamma - (\phi + \psi)(\gamma + \psi)(\delta + \psi)\}}{\beta(\gamma + \psi)(\delta + \psi)(\kappa + \psi)} = \frac{e\gamma\delta}{(\gamma + \psi)(\delta + \psi)(\kappa + \psi)} \left(1 - \frac{1}{R_0}\right)$$

$$R^* = \frac{\delta\kappa\{e\beta\gamma - (\gamma + \psi)(\delta + \psi)(\phi + \psi)\}}{\beta(\gamma + \psi)(\delta + \psi)(\kappa + \psi)(\mu + \psi)} = \frac{e\gamma\delta\kappa}{(\gamma + \psi)(\delta + \psi)(\kappa + \psi)(\mu + \psi)} \left(1 - \frac{1}{R_0}\right)$$

$$A^* = \frac{e\beta\gamma\delta\kappa\mu + \psi(\gamma + \psi)(\delta + \psi)[\phi(\delta + \psi)(\kappa + \psi)(\mu + \psi) + \gamma\{\delta\kappa(-\mu + \phi) + \delta\phi(\mu + \psi) + \phi(\kappa + \psi)(\mu + \psi)\}]}{\beta\gamma\psi(\gamma + \psi)(\delta + \psi)(\kappa + \psi)(\mu + \psi)}$$

It is explicit that P_e^* will be exist uniquely if $R_0 > 1$.

4. The study of stability of the system:

Theorem 1:

If R_0 is less than 1, the system's malware-free equilibrium is locally stable; if R_0 is more than 1, it is unstable.

Proof:

Regarding the system (1)'s stability, the Jacobian matrix can be considered as

$$J = \begin{bmatrix} -\beta I - \phi - \psi & 0 & -\beta S & 0 & 0 & 0 \\ \beta I & -\gamma - \psi & \beta S & 0 & 0 & 0 \\ 0 & \gamma & -\delta - \psi & 0 & 0 & 0 \\ 0 & 0 & \delta & -\kappa - \psi & 0 & 0 \\ 0 & 0 & 0 & \kappa & -\mu - \psi & 0 \\ \phi & 0 & 0 & 0 & \mu & -\psi \end{bmatrix} \quad (9)$$

At the equilibrium point $P_0 = \left(\frac{e}{\phi + \psi}, 0, 0, 0, \frac{e\phi}{\psi(\phi + \psi)}\right)$

$$J(P_0) = \begin{bmatrix} -\phi - \psi & 0 & -\frac{A\beta}{\phi + \psi} & 0 & 0 & 0 \\ 0 & -\gamma - \psi & \frac{A\beta}{\phi + \psi} & 0 & 0 & 0 \\ 0 & \gamma & -\delta - \psi & 0 & 0 & 0 \\ 0 & 0 & \delta & -\kappa - \psi & 0 & 0 \\ 0 & 0 & 0 & \kappa & -\mu - \psi & 0 \\ \phi & 0 & 0 & 0 & \mu & -\psi \end{bmatrix}$$

The characteristic equation $|J(P_0) - \lambda I| = 0$ is expressed as

$$\begin{vmatrix} -\phi - \psi - \lambda & 0 & -\frac{e\beta}{\phi + \psi} & 0 & 0 & 0 \\ 0 & -\gamma - \psi - \lambda & \frac{e\beta}{\phi + \psi} & 0 & 0 & 0 \\ 0 & \gamma & -\delta - \psi - \lambda & 0 & 0 & 0 \\ 0 & 0 & \delta & -\kappa - \psi - \lambda & 0 & 0 \\ 0 & 0 & 0 & \kappa & -\mu - \psi - \lambda & 0 \\ \phi & 0 & 0 & 0 & \mu & -\psi - \lambda \end{vmatrix} = 0$$

$$\text{OR } (\psi + \lambda)(\mu + \psi + \lambda)(\kappa + \psi + \lambda)(\phi + \psi + \lambda)\{(\gamma + \psi + \lambda)(\delta + \psi + \lambda) - \frac{A\beta\gamma}{\phi + \psi}\} = 0$$

$$\text{OR } \lambda = -\psi, \lambda = -(\mu + \psi), \lambda = -(\kappa + \psi), \lambda = -(\phi + \psi) \text{ and}$$

$$\lambda^2 + (\gamma + 2\psi + \delta)\lambda + (\gamma + \psi)(\delta + \psi) - \frac{e\beta\gamma}{\phi + \psi} = 0$$

It is obvious that four eigenvalues are negative and other two eigenvalues are negative if

$$(\gamma + \psi)(\delta + \psi) - \frac{e\beta\gamma}{\phi + \psi} > 0$$

$$\text{or } \frac{e\beta\gamma}{(\phi + \psi)(\gamma + \psi)(\delta + \psi)} < 1$$

$$\text{i.e. } R_0 < 1$$

Therefore, each and every eigenvalues of the characteristic equations are negative. The equilibrium point P_0 is locally asymptotically stable or unstable if either $R_0 < 1$ or $R_0 > 0$.

Theorem 2:

If $R_0 > 1$, the endemic equilibrium P_e^* is locally asymptotically stable.

Proof:

For the stability of the system (1), the Jacobian matrix can be considered as

$$J = \begin{bmatrix} -\beta I - \phi - \psi & 0 & -\beta S & 0 & 0 & 0 \\ \beta I & -\gamma - \psi & \beta S & 0 & 0 & 0 \\ 0 & \gamma & -\delta - \psi & 0 & 0 & 0 \\ 0 & 0 & \delta & -\kappa - \psi & 0 & 0 \\ 0 & 0 & 0 & \kappa & -\mu - \psi & 0 \\ \phi & 0 & 0 & 0 & \mu & -\psi \end{bmatrix}$$

At the endemic equilibrium point $P_e^* = (S^*, E^*, I^*, Q^*, R^*, A^*)$

$$J(P_e^*) = \begin{bmatrix} -\beta I^* - \phi - \psi & 0 & -\beta S^* & 0 & 0 & 0 \\ \beta I^* & -\gamma - \psi & \beta S^* & 0 & 0 & 0 \\ 0 & \gamma & -\delta - \psi & 0 & 0 & 0 \\ 0 & 0 & \delta & -\kappa - \psi & 0 & 0 \\ 0 & 0 & 0 & \kappa & -\mu - \psi & 0 \\ \phi & 0 & 0 & 0 & \mu & -\psi \end{bmatrix}$$

Characteristic equation $|J(P_e^*) - \lambda I| = 0$ can be written as

$$\begin{vmatrix} -\beta I^* - \phi - \psi - \lambda & 0 & -\beta S^* & 0 & 0 & 0 \\ \beta I^* & -\gamma - \psi - \lambda & \beta S^* & 0 & 0 & 0 \\ 0 & \gamma & -\delta - \psi - \lambda & 0 & 0 & 0 \\ 0 & 0 & \delta & -\kappa - \psi - \lambda & 0 & 0 \\ 0 & 0 & 0 & \kappa & -\mu - \psi - \lambda & 0 \\ \phi & 0 & 0 & 0 & \mu & -\psi - \lambda \end{vmatrix} = 0$$

$$(\psi + \lambda)(\mu + \psi + \lambda)(\kappa + \psi + \lambda)[(\beta I^* + \phi + \psi + \lambda)\{(\gamma + \psi + \lambda)(\delta + \psi + \lambda) + \beta\gamma S^*\} - \beta^2\gamma I^* S^*] = 0$$

When $R_0 > 1$, the endemic equilibrium $(S^*, E^*, I^*, Q^*, R^*, A^*)$ is asymptotically stable, according to the Routh-Hurwitz criterion [35].

5. Numerical methods and simulation:

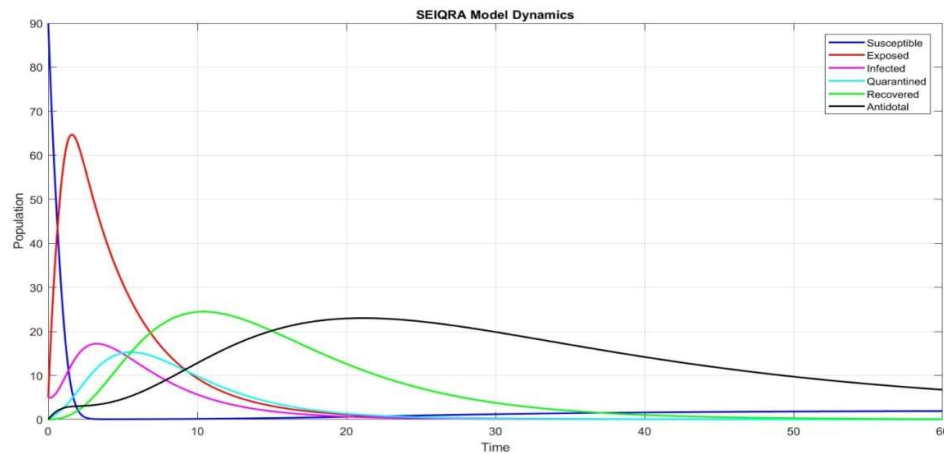


Figure 2: Malware propagation's dynamics with time when $R_0 < 1$.

In the first simulation, in order to confirm theoretical findings, we're going to perform a numerical simulation on MATLAB for the two parameter sets that show how the model behaves based on the value of the basic reproduction number. In both cases, it is assumed that $0 \leq t \leq 60$, and the overall quantity of devices is $N = 100$ where $S(0) = 90$, $E(0) = 5$, $I(0) = 5$, $Q(0) = 0$, $R(0) = 0$, and $A(0) = 0$. Additionally, the coefficients' numerical values are as follows: $e=0.2$, $\beta=0.2$, $\gamma=0.2$, $\phi=0.05$, $\psi=0.05$, $\delta=0.5$, $\kappa=0.4$, and $\mu=0.1$. The value of the basic reproduction number $R_0 = 0.58 < 1$, and a disease-free steady state (see Figure 2) was obtained. It is concluded that malware dies out from the computer networks. This is also confirmed by Theorem 1.

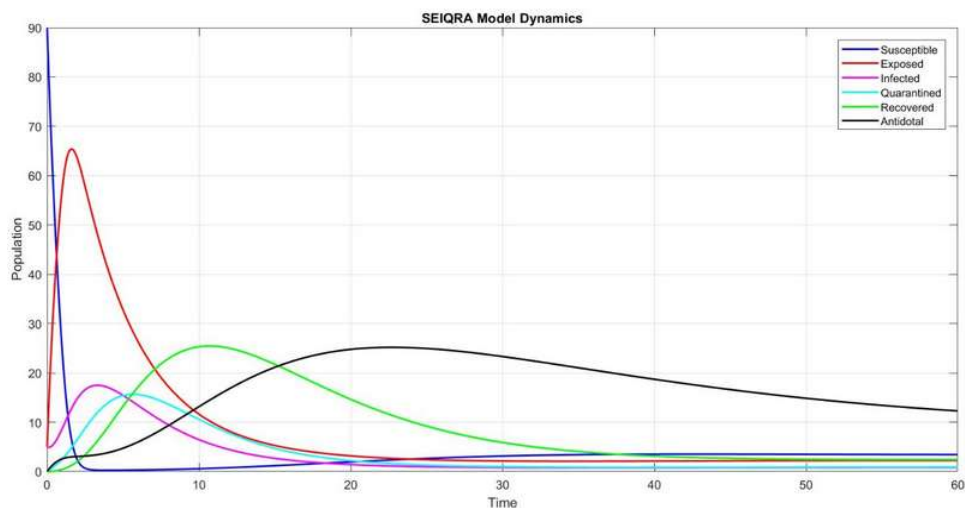


Figure 3: Malware propagation's dynamics with time when $R_0 > 1$.

In the second simulation, it is considered $e=0.9$, $\beta=0.2$, $\gamma=0.2$, $\phi=0.05$, $\psi=0.05$, $\delta=0.5$, $\kappa=0.4$, and $\mu=0.1$ and consequently $R_0 = 2.62 > 1$. The system consequently moves to the endemic stable state (see Figure 3). Under these circumstances, the malware repeatedly enters computer networks. This is also confirmed by Theorem 2.

6. Conclusion:

The proposed model's primary goal is to prevent malware from spreading throughout the network and increase computer networks' lifespan. In this paper, we have analyzed susceptible- exposed- infectious- quarantine-recovered-antidotal (SEIQRA) model with natural incidence rate and we observe that quarantine plays an important role to control the disease, when $R_0 < 1$, disease free equilibrium of the system is locally stable and if $R_0 > 1$, the endemic equilibrium is locally asymptotically stable.

In general, the SEIQRA model offers both theoretical understanding and useful advice for creating malware limitation methods. Our primary findings are also demonstrated through numerical simulations.

References:

- [1] B. K. Mishra and S. K. Pandey, A quarantine model on the propagation of malicious objects in computer network. *Applied Mathematical Modelling*, 35(2), 756–769, 2011.
- [2] L. Zhong, X. Xu and Y. Ma, Modeling self-propagating malware with epidemiological models in computer networks. *Applied Network Science*, 8, 67, 2023.
- [3] J.R. Piqueira and C.M. Batistela, Considering quarantine in the SIRA malware propagation model, *Mathematical Problems in Engineering*, 2019, 1–8, 2019.
- [4] H. Almeer and T. Alshammari, The SEIRS-NIMFA epidemiological model for malware propagation analysis in IoT networks, *Cybersecurity*, 7, 32, 2024.
- [5] L. Zhu, X. Wang and J. Ma, Modeling and analysis of the spread of malware with the influence of user awareness. *Security and Privacy*, 4(6), e146, 2021.
- [6] F. Cohen, Computer viruses: Theory and experiments. *Computers & Security*, 6(1), 22–35, 1987.
- [7] W.H. Murray, The application of epidemiology to computer viruses. *Computers & Security*, 7(2), 139–145, 1988.
- [8] J.O. Kephart and S.R. White, Directed-graph epidemiological models of computer viruses. In *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, 343–358, IEEE, 1991.
- [9] W.O. Kermack and A.G. McKendrick, Contributions to the mathematical theory of epidemics. *Proceedings of the Royal Society of London. Series A*, 115, 700–721, 1927.
- [10] W.O. Kermack and A.G. McKendrick, Contributions to the mathematical theory of epidemics. *Proceedings of the Royal Society of London. Series A*, 138, 55–83, 1932.
- [11] W.O. Kermack and A.G. McKendrick, Contributions to the mathematical theory of epidemics. *Proceedings of the Royal Society of London. Series A*, 141, 94–122, 1933.
- [12] J.R.C. Piqueira, A modified epidemiological model for computer viruses. *Applied Mathematics and Computation*, 213(1), 355–360, 2009.
- [13] J.R.C. Piqueira and F.B. Cesar, Dynamic models for computer virus propagation. *Mathematical Problems in Engineering*, 2008, 1–10, 2008.
- [14] J.R.C. Piqueira, B.F. Navarro and L.H.A. Monteiro, Epidemiological models applied to viruses in computer networks, *Journal of Computer Science*, 1(1), 31–34, 2005.
- [15] Y. Wang and C.X. Wang, Modeling the effect of timing parameters on virus propagation. In *Proceedings of the ACM Workshop on Rapid Malcode*, 61–66 ACM, 2003.
- [16] M.J. Keeling and K.T.D. Eames, Networks and epidemic models. *Journal of the Royal Society Interface*, 2(4), 295–307, 2005.
- [17] B.K. Mishra and D.K. Saini, SEIRS epidemic model with delay for transmission of malicious objects in computer networks. *Applied Mathematics and Computation*, 188(2), 1476–1482, 2007.
- [18] B.K. Mishra and D.K. Saini, SEIRS epidemic model with delay for transmission of malicious objects in computer network, *Applied Mathematics and Computation*, 188 (2) ,1476-1482,2007.
- [19] B.K. Mishra and N. Jha, Fixed period of temporary immunity after run of anti-malicious software on computer nodes. *Applied Mathematics and Computation*, 190(2), 1207–1212, 2007.
- [20] J.O. Kephart, A biologically inspired immune system for computers. In *Proceedings of the International Joint Conference on Artificial Intelligence* (pp. 1–7). Morgan Kaufmann, 1995.

- [21] N. Madar, T. Kalisky, R. Cohen, D. Ben-Avraham and S. Havlin, Immunization and epidemic dynamics in complex networks, *The European Physical Journal B*, 38, 269–276, 2004.
- [22] R. Pastor-Satorras and A. Vespignani, Epidemics and immunization in scale-free networks. In *Handbook of Graphs and Networks: From the Genome to the Internet*. Wiley-VCH, 2002.
- [23] R.M. May and A.L. Lloyd, Infection dynamics on scale-free networks, *Physical Review E*, 64(066112), 1–3, 2001.
- [24] S. Datta and H. Wang, The effectiveness of vaccinations on the spread of email-borne computer virus. In *IEEE CCECE/CCGEL*, 219–223, IEEE, 2005.
- [25] B.K. Mishra and S.K. Pandey, S.K. Dynamic model of worms with vertical transmission in computer networks. *Applied Mathematics and Computation*, 217, 8438–8446, 2011.
- [26] C.C. Zou, W. Gong and D. Towsley, Worm propagation modeling and analysis under dynamic quarantine defense. In *Proceedings of the ACM CCS Workshop on Rapid Malcode* (pp. 51–60). ACM, 2003.
- [27] D. Moore, C. Shannon, G.M. Voelker and S. Savage, Internet quarantine: Requirements for containing self-propagating code. In *Proceedings of IEEE INFOCOM*, 1901–1910, IEEE, 2003.
- [28] T. Chen and N. Jamil, Effectiveness of quarantine in worm epidemic. In *IEEE International Conference on Communications*, 2142–2147, IEEE, 2006.
- [29] B.K. Mishra and A.K. Singh, Two quarantine models on the attack of malicious objects in computer network. *Mathematical Problems in Engineering*, 1–13, 2012.
- [30] B.K. Mishra and N. Jha, SEIQRS model for the transmission of malicious objects in computer networks. *Applied Mathematical Modelling*, 34, 710–715, 2010.
- [31] L.X. Yang, X. Yang and Y. Ji, Epidemic spreading model with awareness and quarantined state in complex networks. *Nonlinear Dynamics*, 69(3), 1031–1038, 2012.
- [32] L. Chen, X. Li and W. Sun, Malware propagation model considering antivirus strategies and optimal control in computer networks. *Frontiers in Physics*, 11, 1201053, 2023.
- [33] K. Zekeriya and A. Ramadan, Delay effect of an e-epidemic SEIRS malware propagation model with saturation incidence and linear treatment. *Digital Communications and Networks*, 8(4), 456–466, 2022.
- [34] B.K. Mishra and A. Prajapati, Spread of malicious objects in computer network: A fuzzy approach. *Applications & Applied Mathematics*, 8(2), 684–700, 2013.
- [35] H. Zhang, R.K. Upadhyay, G. Liu and Z. Zhang, Hopf bifurcation and optimal control of a delayed malware propagation model on mobile wireless sensor networks. *Results in Physics*, 38, 105926, 2022.