**Palestine Journal of Mathematics**

**Vol. 15(1)(2026)** , 970–983 © Palestine Polytechnic University-PPU 2026

# DYNAMIC ANALYSIS OF MALWARE ATTACKS AND THEIR DEFENCE IN COMPUTER NETWORKS

Yerra Shankar Rao, Dhirendra Kumar Sahu, Binayak Dihudi, Mehmet Yavuz, Jayanta Kumar Dash , and Anasuya Nath

Communicated by Hijaz Ahmad

MSC 2010 Classifications: Primary 92C80; Secondary 37G10.

Keywords and phrases: Computer network, Malware, Basic Reproduction Number, Stability Analysis.

*The authors would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper.*

**Abstract** Computer networks have transformed modern society by enabling unprecedented connectivity and information sharing across various platforms and regions. This comprehensive analysis examines the fundamental concepts of computer networks, their operational mechanisms and their significant impact on contemporary society. While networks offer substantial economic, educational, and social benefits, they also introduce new vulnerabilities such cyberattacks, malware threats, and privacy concerns. This study uses an e-epidemic model to analyze the behavior and defense strategies against infected malware within networks. Initially, the model is assessed to determine the basic reproduction number, which indicates the presence of malware within network environments and provides insights into behavior and mitigation strategies that influence malware spread. The theoretical findings are validated through numerical simulations using real parameter values, offering valuable insights into the model's dynamics. This analysis helps in controlling infections and guides the development and prediction of effective network security measures.

## 1 Introduction

The empire of internet services is witnessing a remarkable panic onward in the number of users. Computer systems now house millions of records about various sectors, including commerce, healthcare, banking, defence, and personal data [1]. This vast array of information is vulnerable to misuse for fraudulent activities or alteration for harmful intents. The presence of malicious software, commonly called malware, is a major threat not only to online services such as e-mail and web browsing, but also to critical infrastructures such as transportation, health, and electricity, all of which increasingly depend on the Internet. One of the most pressing dangers to both the Internet and computer networks is the threat of malware attacks [2]. Malicious code encompasses any alterations made to a software system—whether through addition, modification, or deletion—intended to inflict damage. Although the issue of malicious code has been prevalent for many years, recent high-profile attacks and certain economic trends indicate that it is swiftly evolving into a major concern for industries, governments, and individuals alike [3]. The classic types of malicious code are Trojan Horses, worms, and viruses. In the connected world of today, malicious code frequently spreads via a variety of channels, such as the sneaker net, to compromise networks [4]. One of the many ways a computer system can be hacked is through the introduction of malware, such as viruses and worms. A malicious object is code that infects a computer system. Different types of malicious objects include worms, viruses, exploits, denial of service (DoS), floods, sniffers, spoofers, and Trojans, which vary in their attack methods and malicious actions. Historical examples have shown that such malicious software can effectively disable the internet. Today, email serves as a primary vector for distributing viruses, worms, and Trojans. Malware is embedded within a program or file, making it easier to spread from one

computer to another while leaving a trail of infection [5]. This malware can damage hardware, software, or files on your system. Although viruses have existed since the DOS era or even earlier, they became a significant threat after the 1990s, largely due to the widespread use of the Internet and removable storage devices. The transmission of malicious objects across computer networks is epidemic in nature. Mathematical models are used to understand node behavior and network dynamics concerning malware transmission. These models also provide suggestions for control strategies, predicting infections, and assessing the effectiveness of control measures in networks.

Many researchers have focused on controlling malicious objects in networks. In this paper, the authors used an automated mitigation process for the Internet's new worm with the help of a mathematical model. They took the network delay factor into account for worm mitigation [6]. The authors implemented an SEIRS-NIMFA model incorporating a latency period for the dissemination of malware infections in IoT networks [7]. They introduced a worm propagation model characterized by a saturation incidence rate. This saturation rate represents a nonlinear incidence rate, which is considered more rational compared to bilinear and standard incidence rates. The model also examines the interaction dynamics between computers and removable devices through a vaccination strategy [8]. Additionally, this article develops a model for the epidemic spread of malicious codes in Wireless Sensor Networks (WSNs), including a graded infection rate and two time delays. The results analyze the time delay needed for the recovery of infected and quarantined sensor nodes. They suggest that WSN administrators should implement strategies to delay or manage the onset of Hopf bifurcation to effectively mitigate malicious objects [9]. This research explores how malware viruses spread in mobile device networks, focusing on categorizing malware as either hostile or malicious. It also considers quarantining infected devices [10]. This model demonstrates ways to detect vulnerabilities and evaluate antivirus effectiveness. To prevent rapid worm proliferation within computer systems, effective antivirus software must be used [11]. The authors also focus on worm spread in wireless sensor networks, developing an enhanced stochastic SVEIR model that includes both white noise and Lévy noise, along with a general incidence rate, for more accurate analysis of worm propagation influenced by randomness [12]. Another study introduces a stochastic diffusive SIS model with an innovative numerical method for solving both deterministic and stochastic differential equations (PDEs). The method discretizes only the time-dependent parts of the PDEs [13]. The authors proposed simplifying the network by dividing nodes into higher-degree and lower-degree categories, then approximating their degrees to reduce the network's complexity. They developed an epidemic model for computer virus spread in these simplified scale-free networks [14]. This study also includes a comprehensive control analysis of the model, incorporating carrier devices to simulate malware propagation and reduce infections. Control strategies like recovery and vaccination are evaluated using the SUIQR model to optimize the propagation radius in wireless sensor networks [15]. An improved malware propagation model was created to enhance control measures like recovery and vaccination [16]. Incorporating interconnection network frameworks into epidemiological models offers valuable insights for epidemiologists to design containment strategies, leveraging network information dissemination principles [17]. The authors also addressed botnet attacks on critical infrastructure using a mathematical model, with anti-botnet software eliminating DDoS attacks [18]. Using supervised adaptive neural networks and the Levenberg-Marquardt algorithm, they examined interactions between computer viruses and defenses within the nonlinear SIC model [19]. A fractional epidemic model called SEIQR was used to calculate the basic reproduction number and communication radius of sensors to assess malware control effectiveness [20]. The performance of networks was evaluated using the DM mechanism, which helps identify and address information breaches [21]. Additionally, the SVIQRS model described cholera dynamics in both stochastic and deterministic settings, analyzing how vaccination and treatment reduce disease [22]. In another chapter, the authors discusses the use of fractional derivatives in malware propagation models and their stability analysis [23]. Özdemir et al. examined the dynamical analysis of fractional order model for computer virus propagation with kill signals. [24]. There have been a number of illustrative studies that recenlty performed mathematical modelling of real-life problems [25, 26, 27, 28, 29, 30, 31, 32, 33, 34]. Although much research has explored the dynamics of related models, they often do not examine the effects of stable vaccination (patches) influenced by the network. To address this, we introduce vaccination and quarantine nodes as control strategies in the network. Antivirus

patches are among the most effective methods for preventing malware spread. The distribution of patches is more advantageous than centralized methods, mainly because it reduces bandwidth demands. Within a distributed patching system framework, a new malware propagation model called SEIVQR, including vaccination and quarantine effects, is introduced. The model considers vaccination, quarantine, and treatment of malware-affected nodes, making it more realistic and closer to real-world scenarios of malware removal in networks. This approach can assist antivirus developers in practical network situations.

The following sections make up the organization of the paper. The model's assumption and formulation are presented in Section 2. Section 3 elaborates basic terminologies. The existence and positivity of the model's unique solution are examined in Section 4. The equilibrium points and the basic reproduction number were derived in Section 5. In contrast, the stability analysis is covered in Section 6. The discussion of the model's numerical results is distorted in Section 7. Section 8 provides the model's future scope and closing thoughts.

## 2 Mathematical Assumptions and Formulation of the Model

To avoid network crashes in computer networks, the entire network of system nodes can be segregated into six types of sub-nodes: vaccinated, Susceptible, exposed, Infectious, quarantined, and recovered nodes. The new nodes are entered into the network at the rate A that becomes susceptible. Some of the nodes in the network have been vaccinated through the auto-installation of protection, and nodes enter the vaccinated state at a rate B. The susceptible nodes increase as vaccinated nodes become vulnerable at a rate $\gamma$. The entire system, due to a network problem, may experience a natural crash of the hardware or software at the $d_1$. The infectious nodes increase based on the progression of the exposed nodes to active infection at a rate $\sigma$. The interaction between the exposed nodes and infected nodes becomes infectious at the rate $\sigma$. The nodes decrease due to malicious objects in the network at a rate $d_2$. Quarantined or isolation of the nodes increases based on the filtration of the infected nodes at the rate $\varepsilon$. The progression of the anti-malware software causes the isolated nodes to recover at a rate of $\theta$. Assuming the network displays a diagram and is regulated by a nonlinear set of ordinary differential equations.

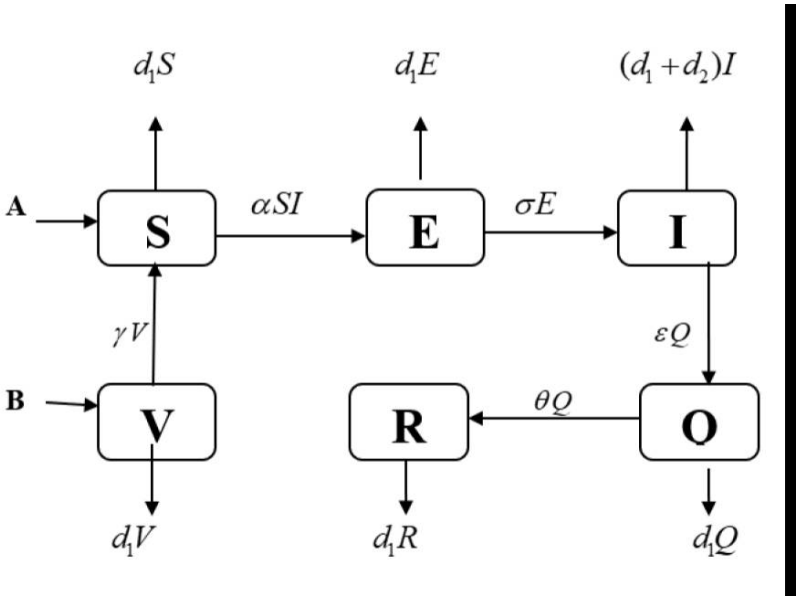


**Figure 1.** Schematic diagram of the model.

| Notation | Description |
|---|---|
| $S(t)$ | The number of devices that are not yet protected or infected with malware. |
| $E(t)$ | The Number of malware-connected but non-infected device nodes |
| $I(t)$ | The Number of systems that are actively infected and capable of spreading malware |
| $V(t)$ | The number of device nodes that have been patched, secured, and hardened. |
| $Q(t)$ | Through patches, the infected nodes are isolated. |
| $R(t)$ | The Number of device nodes recovered after treatment of anti-malware software |
| $A$ | The recruitment of new nodes occurs within susceptible nodes on a per capita basis through the network. |
| $B$ | The rate at which nodes enter the vaccinated nodes. |
| $\alpha$ | The ratio of susceptible nodes that become infected. |
| $\sigma$ | The ratio of exposed nodes that become infected. |
| $\varepsilon$ | The ratio of infected nodes that become isolated. |
| $\theta$ | The ratio of isolated nodes that become recovered. |
| $\gamma$ | The ratio of vaccinated nodes becomes susceptible |
| $d_1$ | Failure of nodes caused by hardware and software issues |
| $d_2$ | Failure of nodes due to a malware attack in the network. |

**Table 1.** Description of the variable and parameter of the malware model

## 3 Basic terminologies

$$\begin{cases} \frac{dS}{dt} = A - \alpha SI - d_1 S + \gamma V \\ \frac{dV}{dt} = B - d_1 V - \gamma V \\ \frac{dE}{dt} = \alpha SI - \sigma E - d_1 E \\ \frac{dI}{dt} = \sigma E - d_1 I - d_2 I - \varepsilon I \\ \frac{dQ}{dt} = \varepsilon I - d_1 Q - \theta Q \\ \frac{dR}{dt} = \theta Q - d_1 R \end{cases} \tag{3.1}$$

From system (3.1), all nodes are positive with respect to their initial conditions, i.e.,

$$S(t) > 0, V(t) > 0, E(t) > 0, I(t) > 0, Q(t) > 0, R(t) > 0$$

In this part, we examine the positive invariant of the region and the presence of solutions.

## 4 Analysis of the model propagation model

In this part, we examine the positive invariant of the region and the presence of solutions.

### Invariant Region and Positivity

**Theorem 4.1.** *All the solutions of system (3.1) with non-negative initial conditions are bounded, i.e., the set of regions* $\{\Delta = S(t) > 0, V(t) > 0, E(t) > 0, I(t) > 0, Q(t) > 0, R(t) > 0 : \Delta \in R_+^6\}$ *is positively invariant.*

*Proof.* It is clear that the sum of all nodes in the region is N, and in the absence of any infection of the system or the network, it is $\frac{dN}{dt} = A + B - d_1 N - d_1 I - d_2 I$ Since there is no infection in the network, $I = 0$. Then $\frac{dN}{dt} = A + B - d_1 N$.

The total number of nodes of the system is represented as $N(t) \leq N(0)e^{-d_1 t} + \frac{A+B}{d_1}(1-e^{-d_1 t})$, when $N(0) \leq \frac{A+B}{d_1}$, then $N(t) \leq \frac{A+B}{d_1}$ The region $\Delta$ is positively invariant. Therefore, the solution enters the region in finite time. Hence, the solution is to attract all the nodes in the region. The malware model of (3.1) is mathematically meaningful.

For the positivity of model (3.1), the nodes meet the initial condition

From the first equation of model (3.1)

$$\frac{dS}{dt} = A - \alpha SI - d_1 S \geq 0$$

This can be solved by the standard form of the differential equation we have

$$\frac{d}{dt}\left(S(t)e^{\left\{\int_0^t \alpha I(\omega)d\omega + d_1 t\right\}}\right) \geq 0$$

$$\Rightarrow S(t) \geq \left(S(0)e^{\left\{\int_0^t \alpha I(\omega)d\omega + d_1 t\right\}}\right) \geq 0, \forall t > 0$$

Using this procedure, the rest of the nodes are derived as positive.
Therefore, all nodes are positive and invariant in the region $\Delta$. □

## 5 Existence of equilibrium points and Basic Reproduction Number

This section covers the two equilibrium points and their stability analysis. The analytical and stability analyses of the model (3.1) determine this equilibrium point.

The stability analysis gives insight into the conditions under which the malware captures or can be controlled in the networks. By understanding these dynamics, the researchers and policymakers can target the interventions more effectively.

In case of malware-free equilibrium points, the infected, quarantined, and recovery nodes are treated as zero. So, we can analyze model (3.1). that we have in the region $\Delta_{\text{MFE}}$,

$\Delta_{MFE} = (S_0, V_0, 0, 0, 0, 0)$ , $\Delta_{MFE} = \left(\frac{A(d_1+\gamma)+\gamma B}{d_1(d_1+\gamma)}, \frac{B}{(d_1+\gamma)}, 0, 0, 0, 0\right)$

The endemic equilibrium point is $\Delta^*_{MEE} = (S^*, V^*, E^*, I^*, Q^*, R^*)$

Where

$$S^* = \frac{A(d_1+\gamma)+\gamma B}{(d_1+\alpha I^*)(d_1+\gamma)},$$
$$V^* = \frac{B}{(d_1+\gamma)},$$
$$E^* = \left(\frac{\alpha I^*[A(d_1+\gamma)+\gamma B]}{(d_1+\alpha I^*)(d_1+\gamma)(d_1+\sigma)}\right),$$
$$Q^* = \frac{\varepsilon I^*}{(d_1+\theta)},$$
$$R^* = \frac{\theta\varepsilon I^*}{(d_1+\theta)}.$$

**Calculation of Basic Reproduction Number**

The basic reproduction number is important in network analysis because it decides whether malware will remain or disappear within the network. This number can be calculated using next-generation matrix methods, where the infected nodes are evaluated at the malware-free equilibrium. It can be inferred from model (3.1) by examining two nodes, such as exposed and infectious nodes.

$$\begin{pmatrix} \frac{dE}{dt} \\ \frac{dI}{dt} \end{pmatrix} = \begin{pmatrix} \alpha SI \\ 0 \end{pmatrix} - \begin{pmatrix} \sigma E + d_1 E \\ d_1 I + d_2 I + \varepsilon I - \sigma E \end{pmatrix}$$

From the transmission matrix F and the transition matrix as V, where

$$F = \begin{pmatrix} 0 & \frac{A(d_1+\gamma)+\gamma B}{d_1(d_1+\gamma)} \\ 0 & 0 \end{pmatrix}$$

$$V = \begin{pmatrix} (\sigma + d_1) & 0 \\ -\sigma & (d_1 + d_2 + \varepsilon) \end{pmatrix}$$

The basic reproduction number is the dominant eigenvalue of $FV^{-1}$, which can be obtained as $R_0 = \rho(FV^{-1}) = \frac{\alpha\sigma[A(d_1+\gamma)+\gamma B]}{d_1(d_1+\gamma)}$

## 6 Analysis of Stability

Stability analysis aims to identify the conditions that enable controlling or removing malware from the network. Understanding these dynamics helps policymakers and anti-malware companies target their efforts more effectively.

In this section, we will examine the stability of the equilibrium points both locally and globally. To assess the local stability of both the malware-free equilibrium and the endemic equilibrium, we can apply the concept of eigenvalues and the Routh-Hurwitz criterion.

**Theorem 6.1.** *The System (3.1) is locally asymptotically stable around its malware-free equilibrium point* $\Delta_{MFE}$= $(\{S_0, V_0, 0, 0, 0, 0\})$, *when all the roots of the Jacobian matrix* $J_{MFE}$ *are negative real parts, iff* $A_1A_2$>0. *Otherwise unstable.*

*Proof.* Model (3.1) is linearized at the malware-free equilibrium point $\Delta_{MFE} = (S_0, V_0, 0, 0, 0, 0)$

$$J_{MFE}(S_0, V_0, 0, 0, 0, 0) = \begin{pmatrix} -d_1 & \gamma & 0 & -\alpha S_0 & 0 & 0 \\ 0 & (-d_1-\gamma) & 0 & 0 & 0 & 0 \\ 0 & 0 & (-\sigma-d_1) & \alpha S_0 & 0 & 0 \\ 0 & 0 & \sigma & (-d_1-d_2-\varepsilon) & 0 & 0 \\ 0 & 0 & 0 & \varepsilon & (-d_1-\theta) & 0 \\ 0 & 0 & 0 & 0 & \theta & -d_1 \end{pmatrix}$$

$$\Rightarrow J_{MFE}(S_0, V_0, 0, 0, 0, 0) = \begin{pmatrix} -d_1 & \gamma & 0 & -\alpha\frac{A(d_1+\gamma)+\gamma B}{d_1(d_1+\gamma)} & 0 & 0 \\ 0 & (-d_1-\gamma) & 0 & 0 & 0 & 0 \\ 0 & 0 & (-\sigma-d_1) & \alpha\frac{A(d_1+\gamma)+\gamma B}{d_1(d_1+\gamma)} & 0 & 0 \\ 0 & 0 & \sigma & (-d_1-d_2-\varepsilon) & 0 & 0 \\ 0 & 0 & 0 & \varepsilon & (-d_1-\theta) & 0 \\ 0 & 0 & 0 & 0 & \theta & -d_1 \end{pmatrix}$$

Then

$$\det(\lambda - J_{MFE}I) = 0$$

$$\det\begin{pmatrix} -d_1-\lambda & \gamma & 0 & -\alpha\frac{A(d_1+\gamma)+\gamma B}{d_1(d_1+\gamma)} & 0 & 0 \\ 0 & (-d_1-\gamma)-\lambda & 0 & 0 & 0 & 0 \\ 0 & 0 & (-\sigma-d_1)-\lambda & \alpha\frac{A(d_1+\gamma)+\gamma B}{d_1(d_1+\gamma)} & 0 & 0 \\ 0 & 0 & \sigma & (-d_1-d_2-\varepsilon)-\lambda & 0 & 0 \\ 0 & 0 & 0 & \varepsilon & (-d_1-\theta) & 0 \\ 0 & 0 & 0 & 0 & \theta & -d_1-\lambda \end{pmatrix} = 0$$

The eigenvalues of the matrix above are

$\lambda_1 = -d_1, \lambda_2 = -d_1, \lambda_3 = (-d_1-\gamma), \lambda_4 = (-d_1-\theta)$. All four eigenvalues are negative, and the other two can be found by solving the quadratic equations.

$\lambda^2 + A_1\lambda + A_2 = 0$, Where

$A_1 = \sigma + 2d_1 + d_2 + \varepsilon > 0$

$A_2 = (\sigma+d_1)(d_1+d_2+\varepsilon) - \frac{\alpha\sigma[A(d_1+\gamma)+\gamma B]}{d_1(d_1+\gamma)} > 0$

$\Rightarrow A_2 = (\sigma+d_1)(d_1+d_2+\varepsilon) - R_0 > 0$

It follows that the differential inequality $R_0 < 1$, so the malware-free equilibrium point is locally asymptotically stable. □

**Local Stability at Endemic Equilibrium**

**Theorem 6.2.** *The endemic equilibrium point* $\Delta^*_{MEE} = (S^*, V^*, E^*, I^*, Q^*, R^*)$ *is locally stable when* $R_0 > 1$.

*Proof.* At the endemic equilibrium point, linearize model (1.1). We have

$$J_{MEE}(S^*, V^*, E^*, I^*, Q^*, R^*) = \begin{pmatrix} -\alpha I^* - d_1 & \gamma & 0 & -\alpha S^* & 0 & 0 \\ 0 & -d_1 - \gamma & 0 & 0 & 0 & 0 \\ \alpha I^* & 0 & -\sigma - d_1 & \alpha S^* & 0 & 0 \\ 0 & 0 & \sigma & -d_1 - d_2 - \varepsilon & 0 & 0 \\ 0 & 0 & 0 & \varepsilon & -d_1 - \theta & 0 \\ 0 & 0 & 0 & 0 & \theta & -d_1 \end{pmatrix}$$

The three eigenvalues $\lambda_1 = -d_1, \lambda_2 = -d_1 - \theta, \lambda_3 = -d_1 - \gamma$. The other three eigenvalues can be determined from the cubic equation

$\lambda^3 + B_1\lambda^2 + B_2\lambda + B_3 = 0$. Where

$$B_1 = (\alpha I^* + 3d_1 + d_2 + \varepsilon) > 0$$

$$B_2 = \begin{pmatrix} (\alpha I^* + d_1)(\sigma + d_1) + (\alpha I^* + d_1)(d_1 + d_2 + \varepsilon) \\ +(\sigma + d_1)(d_1 + d_2 + \varepsilon) - \alpha\sigma S^* \end{pmatrix} > 0$$

$$B_3 = \begin{pmatrix} (\sigma + d_1)(\alpha I^* + d_1)(d_1 + d_2 + \varepsilon) \\ +(\alpha I^* + d_1)\alpha\sigma S^* + \alpha^2 I^*\sigma S^* \end{pmatrix} > 0$$

Since $B_1.B_2 - B_3 > 0$, so as per the Routh-Hurwitz principle $R_0 > 1$, the system is locally stable at the endemic equilibrium point.

□

**Global Stability of Endemic Equilibrium Point**

**Theorem 6.3.** *The endemic equilibrium point of the system is globally stable when* $R_0 > 1$.

With the help of the Lyapunov function, it is possible to derive the stability of the equilibrium point. The endemic equilibrium points were proved by the authors using the following approaches [35].

*Proof.* Consider the Lyapunov function $L : \Delta \in R^6_+ \to R^+$ is defined by

$$L = \frac{1}{2}\left\{ \begin{array}{l} (S - S^*) + (V - V^*) + (E - E^*) \\ +(I - I^*) + (Q - Q^*) + (R - R^*) \end{array} \right\}^2$$

Taking the derivative of both sides, we have

$$\frac{dL}{dt} = \left\{ \begin{array}{l} (S - S^*) + (V - V^*) + (E - E^*) \\ +(I - I^*) + (Q - Q^*) + (R - R^*) \end{array} \right\} \frac{d}{dt}(S + V + E + I + Q + R)$$

$$\frac{dL}{dt} = \left\{ \begin{array}{l} (S - S^*) + (V - V^*) + (E - E^*) \\ +(I - I^*) + (Q - Q^*) + (R - R^*) \end{array} \right\} ((A + B) - (S + V + E + I + Q + R)\, d_1 - d_2 I)$$

$$\frac{dL}{dt} \le \left\{ \begin{array}{l} (S - S^*) + (V - V^*) + (E - E^*) \\ +(I - I^*) + (Q - Q^*) + (R - R^*) \end{array} \right\} \left\{ (S + V + E + I + Q + R) - \frac{(A + B)}{d_1} \right\}$$

$$\frac{dL}{dt} \le \left\{ \begin{array}{l} (S - S^*) + (V - V^*) + (E - E^*) \\ (I - I^*) + (Q - Q^*) + (R - R^*) \end{array} \right\} \left\{ \begin{array}{l} (S + V + E + I + Q + R) - \\ (S^* + V^* + E^* + I^* + Q^* + R^*) \end{array} \right\}$$

$$\frac{dL}{dt} \le -d_1 \left\{ \begin{array}{l} (S - S^*) + (V - V^*) + (E - E^*) \\ +(I - I^*) + (Q - Q^*) + (R - R^*) \end{array} \right\} \left\{ \begin{array}{l} (S - S^*) + (V - V^*) + (E - E^*) \\ +(I - I^*) + (Q - Q^*) + (R - R^*) \end{array} \right\}$$

$$\frac{dL}{dt} \le -d_1 \left\{ \begin{array}{l} (S - S^*) + (V - V^*) + (E - E^*) \\ +(I - I^*) + (Q - Q^*) + (R - R^*) \end{array} \right\}^2$$

□

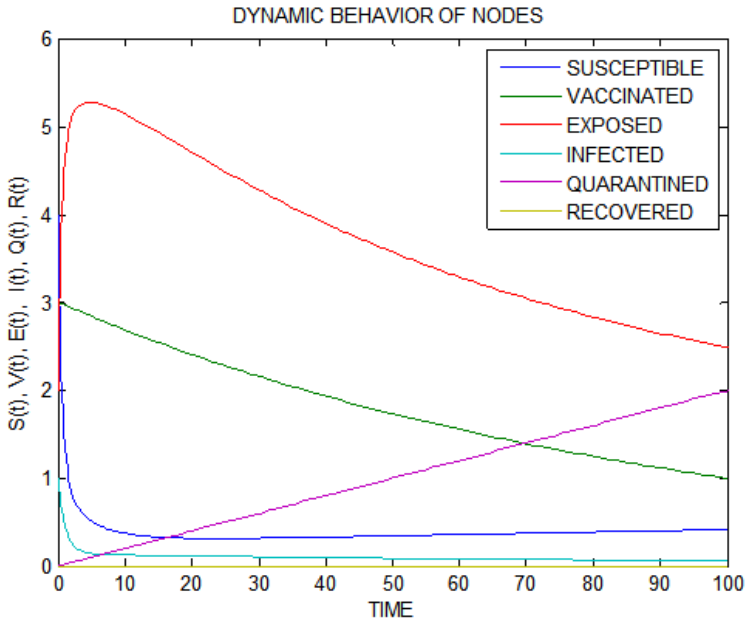


**Figure 2.** Dynamic Behavior of nodes. Numerical simulation of the SVEIQR model over 100 days (generated using ode 45 RK 45 methods). Behavior of nodes under assumed as (S=4, V=3, E=2, I=1, Q=0, R=0), $A = 0.29, B = 0.00006, \alpha = 1.5, \sigma = 0.02, \varepsilon = 0.00025, \theta = 0.002, \gamma = 0.01, d_1 = 0.011, d_2 = 0.001$

The differentiable function is negative semi-definite, i.e $L \leq 0$. Then a differentiable function $\frac{dL}{dt} \leq 0$. As per Lasalle's invariance principle, the largest invariant set of the network is globally stable at the endemic equilibrium point [36].

## 7 Result Discussion

In this section, we perform a numerical validation of the theoretical results for both suitable and actual parametric values. This process helps identify which parameters most significantly influence malware spread, guiding targeted intervention strategies. A model has been developed to analyze malware propagation within a network domain. MATLAB is used to solve system (3.1), demonstrating its dynamic behavior, as shown in Figure 2. It is clear from this figure that the system exhibits asymptotic stability. Additionally, Figure 2 highlights key nodes that can be targeted for infection control, isolation, or patch deployment within the network. Figure 3 shows that nodes in the exposed class E reach their peak during specific time periods, indicating the best times to run anti-malware software to protect these nodes. The effect of Q on infected nodes over time is analyzed and displayed in Figure 4. Figure 5 presents three-dimensional visualizations of vaccination and recovery nodes over time, highlighting the importance of patches in a proactive security strategy to mitigate malware threats. Lastly, Figure 6 compares isolation and infectious nodes over time, demonstrating that once a malware threat is detected, contaminated (infectious) nodes are isolated for a set period to enable quick response and control measures.

| Notation | Description | Values (Assumed) |
|---|---|---|
| $S(t)$ | The number of devices that are not yet protected or infected with malware | 4 |
| $E(t)$ | The Number of malware-connected but non-infected device nodes | 3 |
| $I(t)$ | The Number of systems that are actively infected and capable of spreading malware | 2 |
| $V(t)$ | The number of device nodes that have been patched, secured, and hardened | 1 |
| $Q(t)$ | Through patches, the infected nodes are isolated | 0 |
| $R(t)$ | The Number of device nodes recovered after treatment of anti-malware software | 0 |
| $A$ | The recruitment of new nodes occurs within susceptible nodes on a per capita basis through the network | 0.29 |
| $B$ | The rate at which nodes enter the vaccinated nodes | 0.000006 |
| $\alpha$ | The ratio of susceptible nodes that become infected | 1.5 |
| $\sigma$ | The ratio of exposed nodes that become infected | 0.02 |
| $\varepsilon$ | The ratio of infected nodes that become isolated | 0.00025 |
| $\theta$ | The ratio of isolated nodes that become recovered | 0.002 |
| $\gamma$ | The ratio of vaccinated nodes becomes susceptible | 0.01 |
| $d_1$ | Failure of nodes caused by hardware and software issues | 0.011 |
| $d_2$ | Failure of nodes due to a malware attack in the network | 0.001 |

**Table 2.** Parametric values and their descriptions

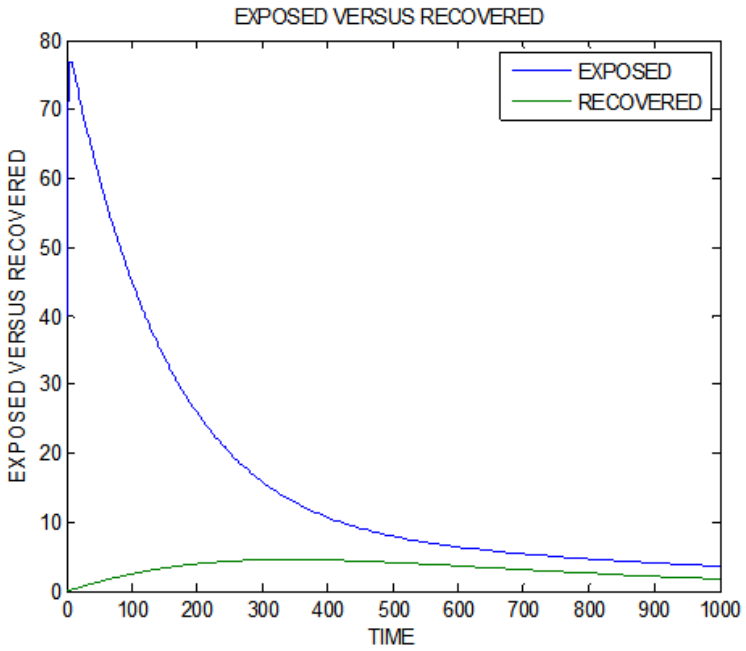


**Figure 3.** Effect of exposed and recovered nodes over the 1000 days with parametric values ( ode 45 RK 45 methods), $A = 0.29, B = 0.00006, \alpha = 1.5, \sigma = 0.02, \varepsilon = 0.00025, \theta = 0.002, \gamma = 0.01, d_1 = 0.011, d_2 = 0.001$

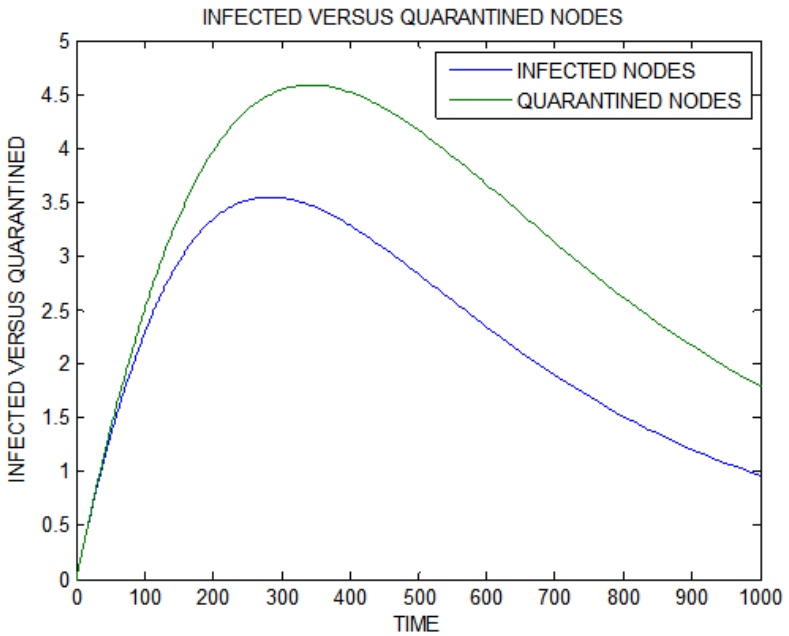


**Figure 4.** Effect of infected in quarantined nodes over the 1000 days with parametric values (using ode 45 RK 45 methods), $A = 0.29, B = 0.00006, \alpha = 1.5, \sigma = 0.02, \varepsilon = 0.00025, \theta = 0.002, \gamma = 0.01, d_1 = 0.011, d_2 = 0.001$

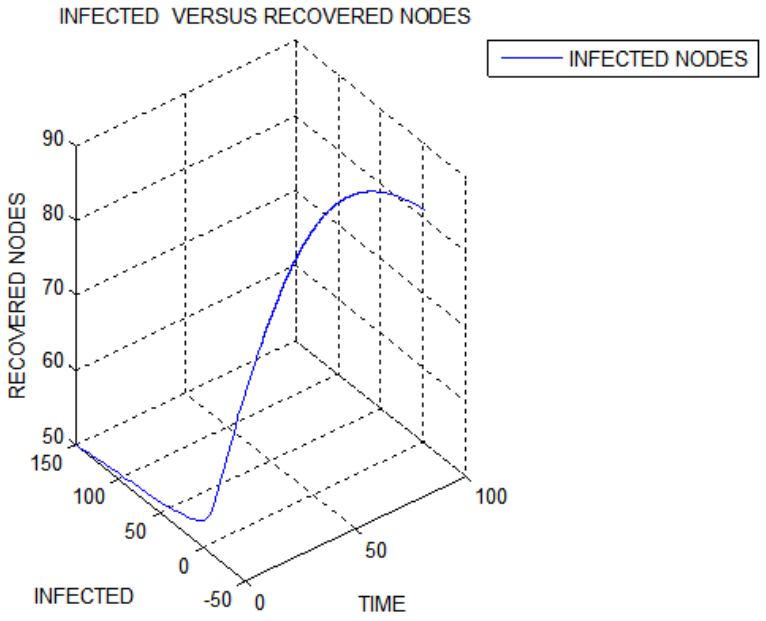


**Figure 5.** Effect of 3D form of infected and recovered nodes over the 100 days (using ode 45 RK 45 methods), $A = 0.29, B = 0.00006, \alpha = 1.5, \sigma = 0.02, \varepsilon = 0.00025, \theta = 0.002, \gamma = 0.01, d_1 = 0.011, d_2 = 0.001$

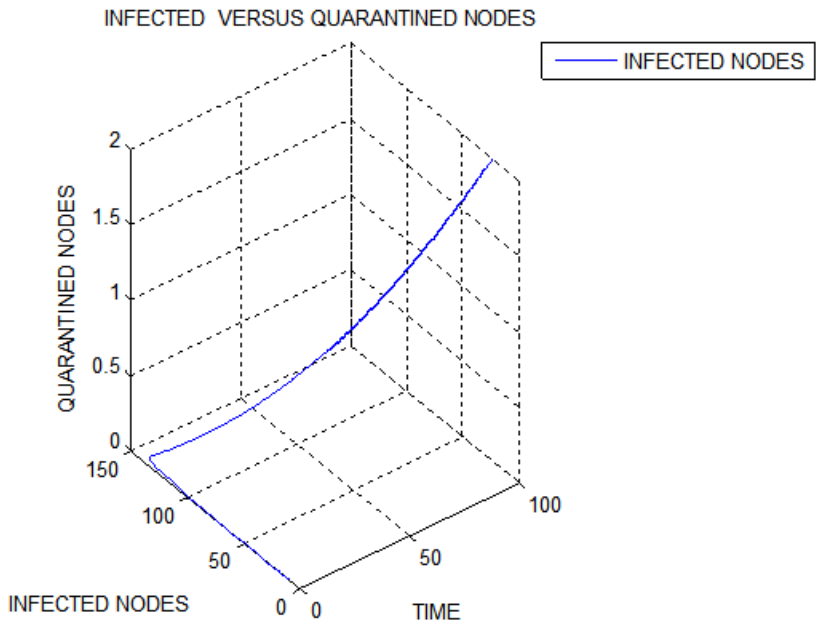


**Figure 6.** Effect of 3D form of infected and quarantined nodes over the 100 days (using ode 45 RK 45 methods), $A = 0.29, B = 0.00006, \alpha = 1.5, \sigma = 0.02, \varepsilon = 0.00025, \theta = 0.002, \gamma = 0.01, d_1 = 0.011, d_2 = 0.001$

## 8 Concluding Remarks and Future Scope

The spread of malware has become a major global concern, with outbreaks occurring worldwide. Predicting these transmissions is essential for developing effective control strategies, and mathematical modeling is recognized as a valuable tool for this purpose. This study focuses on the dynamic transmission of malware within a network, using a nonlinear system of differential equations. First, a quantitative analysis is performed on the model to verify its positivity and boundedness. The analytical solution reveals two equilibrium points, which are key for assessing the system's stability. Stability is examined through linearization and Lyapunov functions. The basic reproduction number is analyzed to evaluate the sensitivity of various parameters. This research highlights the importance of targeted interventions, such as optimizing recovery and vaccination (patch) strategies, in controlling malware outbreaks. The existence or non-existence of malware within the system affects the fundamental reproduction number. The effectiveness of vaccination and quarantining infected nodes an important indicator for eradicating or controlling malware. The proposed model provides practical insights for prompt responses to malware outbreaks, combining theoretical and sensitivity analyses. Numerical simulations, along with the impact of actual parameter values on malware transmission, show positive indicators for malware spread speeds alongside vaccination and quarantine efforts. Quarantine and surveillance, including vaccinations, are crucial for managing malware within networks. Our model demonstrates that quickly identifying and isolating infected nodes can significantly reduce secondary transmissions. Public awareness campaigns are crucial for controlling the spread of malware and reducing infection rates. Implementing integrated quarantines, timely system updates, and education on malware risks and prevention can greatly help reduce transmission and protect the public network. Future work will employ fractional multi-order and delay differential equations to improve modeling accuracy and validate the model.

## References


[1] Tang S. Tang and W. Li, *QoS supporting and optimal energy allocation for a cluster-based wireless sensor network* , *Computer Communications*, **29** , 2569–2577, (2006 ).

[2] M. S. Yousefpoor, E. Yousefpoor, H. Barati, A. Barati, A. Movaghar, and M. Hosseinzadeh, *Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review*, *Journal of Network and Computer Applications*, **190** , 103118, (2021).

[3] M. Mirjalili, A. Nowroozi, and M. Alidoosti, *Secure A survey on web penetration test*, *Advances in Computer Science: An International Journal*, **3(6)** , 107–121, (2014).

[4] H. Carvey, *Secure Malware Detection*, *Elsevier eBooks*, **3(6)** , 155–193, (2012).

[5] S. Kumari and R. K. Upadhyay, *Exploring the behavior of malware propagation on mobile wireless sensor networks: Stability and control analysis*, *Mathematics and Computers in Simulation*, **190**,246–269, (2021).

[6] F. Wang, Y. Zhang, C. Wang, J. Ma, and S. Moon, *Stability analysis of a SEIQV epidemic model for rapid spreading worms*, *Computers & Security*, **29(4)**, 410–418, (2009).

[7] L. Quiroga-Sánchez, G. A. Montoya, and C. Lozano-Garzon, *The SEIRS-NIMFA epidemiological model for malware propagation analysis in IoT networks*, *Cybersecurity*, **8(1)**, (2025).

[8] R. Wang and Y. Xue, *Stability analysis and optimal control of worm propagation model with saturated incidence rate*, *Computers & Security*, **125**,103063, (2022).

[9] J. Liu, N. Gul, A. Zeb, and T. Saeed, *Periodic solutions of a delayed model for propagation of malicious codes in WSNS with graded infection rate*, *Results in Physics*, **38**,105631, (2022).

[10] A. Lanz, D. Rogers, and T. L. Alford, *An Epidemic Model of Malware Virus with Quarantine*, *Journal of Advances in Mathematics and Computer Science*, **38**,1–10, (2019).

[11] S. Geethamalini, S. Balamuralitharan, M. Radha, V. Geetha, and A. Rathinasamy, *Stability analysis of deterministic SEIA worm model by reproductive number*, *AIP Conference Proceedings*, **38**, 1–10, (2019).

[12] A. Alkhazzan et al., *Lyapunov-based analysis and worm extinction in wireless networks using stochastic SVEIR model*, *Alexandria Engineering Journal*, **118**, 337–353, (2025).

[13] M. S. Arif, *A novel explicit scheme for stochastic diffusive SIS models with treatment effects*, *Partial Differential Equations in Applied Mathematics*, **14**, 101215, (2025).

[14] L.-X. Yang and X. Yang, *The spread of computer viruses over a reduced scale-free network*, *Physica A Statistical Mechanics and Its Applications*, **396**,173–184, (2013).

[15] J. D. H. Guillén, Á. M. Del Rey and R. C. Vara, *On the Optimal Control of a Malware Propagation Model*, *Mathematics*, **8(9)**,1518, (2020).

[16] Y. Zhou, Y. Wang, K. Zhou, S.-F. Shen, and W.-X. Ma, *Dynamical behaviors of an epidemic model for malware propagation in wireless sensor networks*, *Frontiers in Physics*, **11**, (2023).

[17] C. R. Lucatero, *Analysis of epidemic models in complex networks and node isolation Strategie proposal for reducing virus propagation*, *Axioms*, **13(2)**,79, (2024).

[18] Y. S. Rao, A. K. Rauta, S. N. Kund, B. Sethi, and J. Behera, *Mathematical Model on Distributed Denial of Service Attack in the Computer Network*, *WSEAS TRANSACTIONS ON COMMUNICATIONS*, **22**, 183–191, (2023).

[19] N. Anwar, S. Naz, M. A. Z. Raja, I. Ahmad, M. Shoaib, and A. K. Kiani, *Machine learning solutions with supervised adaptive neural networks for countermeasure competing strategy of computer virus models*,*Simulation Modelling Practice and Theory*, **142**,103141, (2025).

[20] S. Muthukumar, A. Balakumar, and V. Chinnadurai, *The dynamics of the fractional SEIQR malware spread model on wireless sensor networks*,*The Journal of Analysis*, **32**,2349–2370, (2024).

[21] U. U. Rehman and T. Mahmood, *A study and performance evaluation of computer network under the environment of bipolar complex fuzzy partition Heronian mean operators*,*Advances in Engineering Software*, **180**,103443, (2023).

[22] Fikru S Tessema, Boka K. Bole, Purnachandra R Koya, *Dynamics of a Stochastic and Deterministic SVIQRS Cholera Epidemic model*,*Applied Mathematics & Information Sciences*, **16(6)**,961–971, (2022).

[23] Y. S. Rao, B. Dihudi, S. Biswas, D. K. Sahu, J. K. Dash, and D. K. Singh, *Stability analysis of malware propagation in the computer network for fractional-order differential equations*,*Elsevier eBooks*, **16(6)**,147–158, (2025).

[24] Özdemir, N., Uçar, S., & Billur İskender Eroğlu, B. (2020). Dynamical analysis of fractional order model for computer virus propagation with kill signals. International Journal of Nonlinear Sciences & Numerical Simulation, 21.

[25] Joshi, H., & Yavuz, M, *A novel fractional-order model and analysis of cancer-immune system interaction in an avascular environment with an efficient control mechanism*, *Journal of Computational and Applied Mathematics,*, **473**,116888, (2026).

[26] Enver, A.,& Ayaz, F, *Melatonin and breast cancer: a mathematical modeling approach in blind women*, *Bulletin of Biomathematics*, **3(2)**,164-191, (2025).

[27] Neamah, R. A., Nassar, A. A., Alansari, L. S., Njim, E. K., Hadji, L., & Madan, R. *Static deflection analysis of functionally graded beams using various beam theories*, *Mathematical Modelling and Numerical Simulation with Applications*, **5(2)**, 396-420, (2025).

[28] Ebrahimzadeh, A., Jajarmi, A., & Yavuz, M *Fractional Optimal Control of Anthroponotic Cutaneous Leishmaniasis with Behavioral and Epidemiological Extensions*, *Mathematical and Computational Applications*, **30(6)**,122, (2025).

[29] Ahmad, A., Kumam, P., & Seangwattana, T. *Strong convergence multi-step inertial golden ratio-based algorithms for split feasibility problems with applications* ,*Mathematical Modelling and Numerical Simulation with Applications*, **5(2)**,307-347, (2025).

[30] Geetha, R., Muthurathinam Sivabalan, M. Y., Megala, T.,& Pradeep, M. S., *Biodiversity and ecosystem stability in a four-species prey-predator food chain with meta-communities* , *AIMS Bioengineering*, **12(4)**, 530-555, (2025).

[31] Hassaballa, A. A., Yavuz, M., Farah, G. A., Almulhim, F. A., Abdel-Khalek, S., & Abdel-Salam, E. A. B., *Mathematical modeling of influence of multiplicative white noise on dynamical soliton solutions in the KdV equation*, *Mathematics Open*, **4**,2550013, (2025).

[32] Nkeki, C., & Mbarie, I., *On a mathematical model and the efficacy of control measures on the transmission dynamics of chickenpox*, *Bulletin of Biomathematics*, **3(1)**,37-61, (2025).

[33] Boulaasair, L., Bouzahir, H.,& Yavuz, M., *Analysis and simulation of a stochastic epidemic model with general incidence function and vaccination process*, *Palestine Journal of Mathematics*, **14 (2)**,540-550, (2025).

[34] Naik, P. A., Yeolekar, B. M., Qureshi, S., Yavuz, M., Huang, Z., & Yeolekar, M., *Fractional insights in tumor modeling: an interactive study between tumor carcinogenesis and macrophage activation*,*Advanced Theory and Simulations*, **8(7)**, 2401477, (2025).

[35] O. A. Adepoju, T. M. Olatunji, S. O. Olanrewaju, and H. O. Ibrahim, *Stability Analysis of HIV/AIDS Epidemic Model with Vertical Transmission*, *Advances in Mathematics Scientific Journal*, **13(3)**,433–451, (2024).

[36] Lasalle J. P., *The stability of dynamical system*, *Philadelphia, PA, SIAM*,1-76, (1976).

## Author information

Yerra Shankar Rao, Department of Mathematics, NIST University, Berhampur, Odisha, India.
E-mail: sankar.math1@gmail.com

Dhirendra Kumar Sahu, Department of Mathematics, Research Scholar, BPUT Rourkela, Odisha, India.
E-mail: dhirendra.kumar107@gmail.com

Binayak Dihudi, Department of Mathematics, KIST, Jatni, Bhubaneswar, Odisha, India.
E-mail: bdihudi@gmail.com

Mehmet Yavuz, Department of Mathematics and Computer Sciences, Necmettin Erbakan University, Konya, Department of Applied Mathematics and Informatics, Kyrgyz-Turkish Manas University, Bishkek, Kyrgyzstan, Türkiye, Kyrgyzstan.
E-mail: mehmetyavuz@erbakan.edu.tr

Jayanta Kumar Dash, Department of Mathematics, IMIT, Cuttack, Odisha, India.
E-mail: jkdash@gmail.com

Anasuya Nath, Department of Mathematics, Utkal University, Bhubaneswar, Odisha, India.
E-mail: anasuya_nath@yahoo.comnewline

Received: 2025-06-22.
Accepted: 2025-12-28.