Available online at http://scik.org

Commun. Math. Biol. Neurosci. 2026, 2026:34

https://doi.org/10.28919/cmbn/9775

ISSN: 2052-2541

MATHEMATICAL ANALYSIS OF MALWARE PROPAGATION IN COMPUTER NETWORKS USING AN SPIQR EPIDEMIC MODEL

MD MRIDUL HAQUE CHOUDHURY[1,2,*], HEMEN BHARALI[1], DIBAKAR DUTTA[2]

[1]Department of Mathematics, Assam Don Bosco University, Tapesia, Sonapur, Guwahati-782402, Assam, India

[2]Department of Mathematics, Barkhetri College, Narayanpur, Mukalmua-781126, Nalbari, Assam, India

Abstract: In modern times, malware poses a significant threat to information security. Consequently, numerous mathematical models have been developed to describe the dissemination of malware. This study presents the SPIQR (susceptible-protected-infectious-quarantined-recovered) model to analyze how malware spreads through computer networks. We initiate our analysis by formulating a nonlinear dynamic equation that delineates the dissemination of malware. Subsequently, we compute the basic reproduction number (BRN), denoted by R_0 for the proposed model. The network's stability is contingent upon the magnitude of R_0. Particularly, if $R_0 < 1$, the system remains free from malware, while if $R_0 > 1$, the network enters an endemic state. We determine the system's equilibrium points and perform numerical simulations to investigate malware spread within the network, aiming to confirm our theoretical results. In addition, we examine the nodes' communication range to provide more comprehensive data. We also examine the networks' susceptible, protected, infected, quarantined, and recovered node dynamics.

Keywords: malware propagation; stability analysis; mathematical model; malicious objects; basic reproduction number.

2020 AMS Subject Classification: 92D30.

*Corresponding author

E-mail address: mridulchoudhury.bcm@gmail.com

Received January 13, 2026

1. INTRODUCTION

The use of electronic mail and its associated technologies continues to be a primary means for the dissemination of malicious software, commonly referred to as malware, within contemporary computer networks [1]. Malware penetration poses a considerable risk to the security and stability of increasingly complex computer networks. There exists a wide variety of malicious software, including worms, viruses, Trojan horses, adware, ransomware, and spyware, each employing distinct mechanisms to compromise systems and cause damage [2]. A key challenge lies in accurately simulating and understanding the spread of malware.

Consequently, it is imperative to not only identify malware within a network but also to adeptly model its dissemination. Although a substantial segment of scholarly inquiry in this domain has predominantly focused on methodologies for malware identification, the development of mathematical models to replicate its propagation has been given relatively reduced focus [3]. The models are crucial, as they provide fundamental insights into malware dynamics and facilitate the evaluation of the effectiveness of counteractive measures. Typically, the mathematical methodologies employed to model malware transmission are divided into global and deterministic frameworks, which are often grounded in ordinary differential equation systems.

The dynamics of malware spread within computer networks can be likened to the transmission of epidemics in human populations. In this analogy, malware's spread within a network of interconnected computers is similar to how diseases are transmitted through vectors in public health. In the context of vector-borne illnesses, it is crucial to acknowledge that the pathogens inhabit a portion of the vector's life cycle, facilitating a cyclical process of transmission between the host and the vector. Anderson and May [4, 5] conducted an in-depth examination of the dynamics of biological viruses, parasites, and various infectious agents that influence human populations, employing a range of epidemic modeling methodologies.

2. RELATED WORKS

In recent decades, numerous scholars have focused their efforts on the SIR (Susceptible-Infectious-Recovered) pandemic model to obtain greater clarity and comprehension of malware

spreading dynamics, as demonstrated by the research conducted by Youssef et al. [6], Feng et al. [7], Rey et al. [8], and Kermack and McKendrick [9-11]. In their studies, nodes are classified into three categories: susceptible, infectious, and recovered.

Recent investigations have culminated in the formulation of diverse malware dissemination models that draw inspiration from the SIR model. For example, Xiao et al. [12] proposed the SIRS model for malware transmission, incorporating dispersion processes and delays in time. They predicted tipping points and explored the dynamics of these tipping events, influenced by Hopf bifurcation and Turing instability. Dong et al. [13] introduced the SIRS epidemic model in a fractional network that is characterized by dynamics of a saturated treatment function and fuzzy transmission. Carnier et al. [14] enhanced the methods for deriving an accurate Markov chain applicable to any malware model grounded in the fundamental SIR framework. Among these frameworks, the SEIR model assumes a crucial role in elucidating malware dissemination. Furthermore, a substantial portion of mathematical epidemiology is dedicated to ascertaining the BRN alongside the stability of both endemic equilibrium and non-trivial equilibrium states. For instance, Prajapati et al. [15] created apandemic model to characterize the transmission of malware across networks subject to removable devices. They developed a reproduction number and determined points of equilibrium for both malware-free and endemic circumstances. Liu et al. [16] formulated a SEIRS model for a delayed e-epidemic for malware dissemination, incorporating a rate of non-monotone incidence that is generalized. Shakya et al. [17] introduced theSIR model based on correlation that considers the features of spatial correlation of Wireless Sensor Networks (WSNs). In their investigation, they computed the BRNand examined local stability as well as Hopf bifurcation. Furthermore, Liu et al. [18] addressed the uniqueness of equilibrium and global stability by proposing a distributed continuous-time model to investigate the spread of two competing viruses within a network. Zhang et al. [19] conducted nonlinear stability analysis and Hopf bifurcation evaluations, as well as stability evaluations utilizing an e-epidemic time-delay model to study delayed dynamics.

Mishra and Keshri [20] introduced theSEIR-V model, which assumes that sensor nodes can either be exposed to a disease that slows transmission or be inoculated against future infections.

Their work led to the development of a reproductive ratio that quantifies the incidence of secondary infections resulting from the integration of an infected sensor into a susceptible cohort.

Mishra, Srivastava, and Mishra [21] suggested the SIQRS model, which significantly excluded the latent (or exposed) phase of infections, where sensors may exhibit symptoms like diminished transmission rates. Additionally, the vaccination section was omitted from this particular model.

Mishra and Tyagi [22] introduced the SEIQR-V epidemic model to enhance comprehension of infection dynamics within Wireless Sensor Networks (WSN). With the addition of a quarantining (isolation) compartment, this model improved Mishra and Keshri's SEIR-V model [20].

Nwokoye and Umeh [23] refined theSEIQR-V model originally proposed by Mishra and Tyagi [22]. Their research concentrated on modifying the model by utilizing mathematical expressions to delineate distribution density and range within Wireless Sensor Networks (WSNs).

Zhang and Si [24] employed delay as a bifurcation parameter to explore the emergence of Hopf bifurcation in the SEIR-V epidemic model formulated by Mishra and Keshri [20]. Their investigation utilized the normal form approach and the center manifold theorem to scrutinize the properties of Hopf bifurcation, revealing an adverse state within WSNs, wherein the incidence of infections transitions from a stable equilibrium to a limit cycle.

Biswal and Swain [25] introduced theSIQVD (Susceptible-Infectious-Quarantine-Vaccination-Dead) model to examine the propagation dynamics of malware in WSNs. This model functions as a strategic framework for alleviating malware threats in these networks. They established the mathematical prerequisites for the existence of WSNs under malware incursions and assessed the dynamic behavior of malware dissemination within these systems.

Mohanty et al. [26] created the SEIAQR (Susceptible-Exposed-Infectious-Antidotal-Quarantine-Recovered) model beneath conventional antivirus defense to stop malware from spreading.They established the model's stability at equilibrium points, where it is demonstrated that the endemic and virus-free equilibria are globally asymptotically stable provided the BRN is less than one; otherwise, the model is unstable.

Previous investigations have predominantly concentrated on the modeling of malware dissemination, frequently neglecting the intrinsic properties of computer networks. There exists a deficiency in the development of robust control mechanisms aimed at mitigating malware proliferation. For instance, the velocity of malware transmission is influenced by variables such as the communication range and the regularity of node interactions, whereas the recovery velocity of nodes can be enhanced through systematic updates. Consequently, the integration of node attributes could augment computer networks by diminishing the transmission range and amplifying update frequencies. To remedy these deficiencies, this manuscript presents an enhanced model for malware propagation. The principal contribution of this study is the meticulous derivation of the BRN. The novelty of this study resides in its investigation of the dynamics of malware transmission within networks via the proposed SPIQR model and the identification of optimal tactics to constrain malware spread based on the reproduction number.

3. FORMULATION OF THE SPIQR MODEL

A novel differential equation malware propagation epidemic model in computer networks is constructed in this section. The subclasses of nodes that make up the population size N(t) are susceptible, protected, infected, quarantined, and recovered; their relative sizes are indicated by S(t), P(t), I(t), Q(t), and R(t). This suggests that at any moment $t \geq 0$, $N(t) = S(t) + P(t) + I(t) + Q(t) + R(t)$ satisfies this condition. To establish the model, certain assumptions have been made.At the start of a computer network, every node is susceptible. The following assumptions may cause a node's position to change once malware enters computer networks:

- Once the system's infected nodes are functioning, they establish connections with susceptible nodes and spread the infection. At the rate of β, or a function βSI, the susceptible nodes move into infected nodes.At rateα, some of the susceptible nodes become protected.
- At the rate of γ, some protected nodes return to the susceptible state as a result of protection failure.

- At a rate of η, the system enters a quarantine state after its infectious nodes have been found. At a rate of ϕ, the periodic system updates will cause some nodes in class I to move into class R.
- At a rate of θ, during periodic system updates, a few nodes from class Q will move to class R.
- At a rate of λ, the system's recovered nodes return to the susceptible state once more.
- Some of the susceptible nodes, protected nodes, infectious nodes, quarantine nodes and recovered nodes become dead due to software or hardware failure at a rate σ.

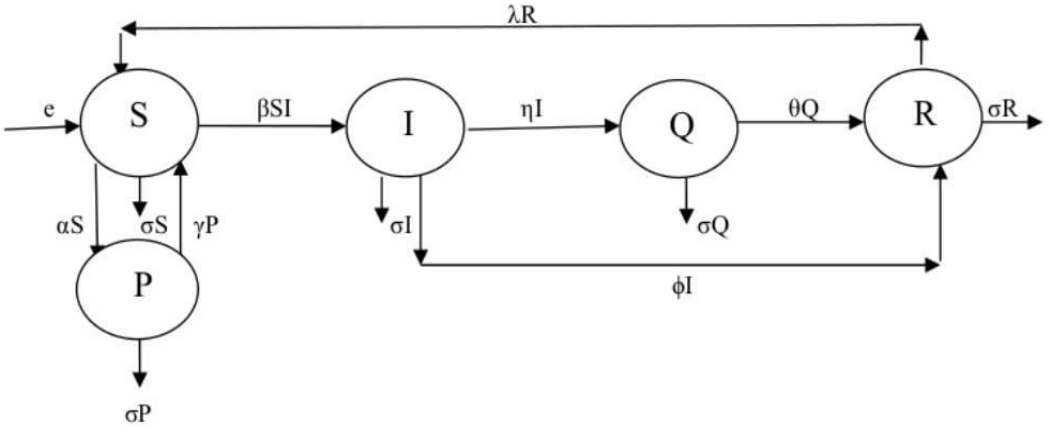

Figure 1: Malware propagation's flow diagram in Computer Networks.

Consequently, the SPIQR model is represented by the differential equation system below:

$$\frac{dS}{dt} = e - \beta SI - \alpha S - \sigma S + \gamma P + \lambda R$$

$$\frac{dP}{dt} = \alpha S - \gamma P - \sigma P$$

$$\frac{dI}{dt} = \beta SI - \eta I - \phi I - \sigma I \quad (1)$$

$$\frac{dQ}{dt} = \eta I - \theta Q - \sigma Q$$

$$\frac{dR}{dt} = \phi I + \theta Q - \lambda R - \sigma R$$

The parameters and their meaning are as follows:

e: Rate at which new computer network nodes are added

β: Rate of Infectivity Contact

α: The rate of susceptible nodes moving to the protected category (by means of security updates)

γ: The rate at which, as a result of protection failure, protected nodes once more move intothe susceptiblestate

η: Quarantine rate from the infectious segment to the quarantined segment

ϕ: The rate at which infectious nodes move intothe recovered state due to system updates

θ: Transmission rate from the quarantined segment to the recovered segment

λ: Conversion rate of recovered nodes to susceptible states

σ: Node death rate as a result of software or hardware failures

4. POINTS OF EQUILIBRIUM IN THE SYSTEM

We shall examine the two categories of the system's equilibrium points. In one case, $I \neq 0$ indicates the endemic equilibrium points, and in the other, I=0 indicates the malware-free equilibrium points.

Thus, the equation (1) system will be shown as

$$\frac{dS}{dt} = e - \beta SI - \alpha S - \sigma S + \gamma P + \lambda R = 0$$

$$\frac{dP}{dt} = \alpha S - \gamma P - \sigma P = 0$$

$$\frac{dI}{dt} = \beta SI - \eta I - \phi I - \sigma I = 0 \qquad (2)$$

$$\frac{dQ}{dt} = \eta I - \theta Q - \sigma Q = 0$$

$$\frac{dR}{dt} = \phi I + \theta Q - \lambda R - \sigma R = 0$$

4.1 Malware-free Equilibrium Point

Once equation (2)'s system was solved, we discovered malware-free equilibrium points.

The system's malware-free points are given as $D_0 = (S_0, P_0, I_0, Q_0, R_0)$ i.e.

$$S_0 = \frac{e(\gamma + \sigma)}{\sigma(\alpha + \gamma + \sigma)}, \quad P_0 = \frac{e\alpha}{\sigma(\alpha + \gamma + \sigma)}, \quad I_0 = 0, \quad Q_0 = 0, \quad R_0 = 0.$$

4.2 The Basic Reproduction Number (R_0)

Since the model contains two infected compartments, namely I and Q, the next-generation matrix method (NGM) is applied to compute the basic reproduction number R_0[27]. The main

advantage of the NGM is that it allows the analysis to focus exclusively on infected compartments, while ignoring uninfected ones.

Let $X= (I, Q)^T$.

Then, model (1) can be written in the following form:

$$\frac{dX}{dt}= F - V \tag{3}$$

Where $F = \begin{pmatrix} \beta SI \\ 0 \end{pmatrix}$ and $V = \begin{pmatrix} \eta I + \phi I + \sigma I \\ -\eta I + \theta Q + \sigma Q \end{pmatrix}$

We define f and v as the Jacobian matrices of F and V, evaluated at the malware-free equilibrium point D_0:

$$f= \left(\frac{\partial F}{\partial X}\right)|D_0 = \begin{pmatrix} \beta So & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \beta \frac{e\,(\gamma+\sigma)}{\sigma(\alpha+\gamma+\sigma)} & 0 \\ 0 & 0 \end{pmatrix} \tag{4}$$

$$v = \left(\frac{\partial V}{\partial X}\right)|D_0 = \begin{pmatrix} \eta + \phi + \sigma & 0 \\ -\eta & \theta + \sigma \end{pmatrix} \tag{5}$$

The basic reproduction number R_0 is the largest matrix eigenvalue of the matrix fv^{-1}given by Equation (6):

$$f\,v^{-1}= \begin{pmatrix} \frac{e\beta\,(\gamma+\sigma)}{\sigma(\alpha+\gamma+\sigma)(\eta+\phi+\sigma)} & 0 \\ 0 & 0 \end{pmatrix} \tag{6}$$

Then, the BRN R_0 can be obtained as

$$R_0= \rho\,(fv^{-1}) = \frac{e\beta\,(\gamma+\sigma)}{\sigma(\alpha+\gamma+\sigma)(\eta+\phi+\sigma)}, \text{ where } \rho \text{ is the spectral radius.} \tag{7}$$

4.3 Endemic Equilibrium Point

For the endemic equilibrium $I \neq 0$. The system's endemic equilibrium points are given as $D^* = (S^*, P^*, I^*, Q^*, R^*)$ as

$$S^* = \frac{\eta + \sigma + \phi}{\beta}$$

$$P^* = \frac{\alpha\,(\eta + \sigma + \phi)}{\beta\,(\gamma + \sigma)}$$

$$I^* = -\frac{(\theta+\sigma)(\lambda+\sigma)\{-e\,\beta(\gamma+\sigma)+\sigma(\alpha+\gamma+\sigma)\,(\eta+\sigma+\phi)\}}{\beta\sigma\,(\gamma+\sigma)\,\{\eta(\theta+\lambda+\sigma)+(\theta+\sigma)(\lambda+\sigma+\phi)\}} = \frac{e\,\beta(\theta+\sigma)(\lambda+\sigma)(\gamma+\sigma)}{L}\left(1-\frac{1}{Ro}\right)$$

$$Q^* = -\frac{\eta\,(\lambda+\sigma)\,\{-e\,\beta(\gamma+\sigma)+\sigma(\alpha+\gamma+\sigma)(\eta+\sigma+\phi)\}}{\beta\sigma\,(\gamma+\sigma)\,\{\eta(\theta+\lambda+\sigma)+(\theta+\sigma)(\lambda+\sigma+\phi)\}} = \frac{e\,\beta\eta(\lambda+\sigma)(\gamma+\sigma)}{L}\left(1-\frac{1}{Ro}\right)$$

$$R^{*}= -\frac{\{\eta\theta + (\theta + \sigma)\phi\}\{-e\,\beta(\gamma + \sigma)+ \sigma(\alpha + \gamma + \sigma)(\eta + \sigma + \phi)\}}{\beta\sigma\,(\gamma + \sigma)\,\{\eta(\theta + \lambda + \sigma)+ (\theta + \sigma)(\lambda + \sigma + \phi)\}} = \frac{e\,\beta\{\eta\theta + (\theta + \sigma)\phi\}(\gamma+ \sigma)}{L}\left(1 - \frac{1}{Ro}\right)$$

where $L = \beta\sigma(\gamma + \sigma)\{\eta(\theta + \lambda + \sigma) + (\theta + \sigma)(\lambda + \sigma + \phi)\}$

If $R_0 > 1$, it is clear that D* will exist uniquely.

5. STABILITY ANALYSIS OF THE SPIQR MODEL

Theorem 1: *When $R_0 < 1$, the system's malware-free equilibrium is locally stable,whereas it becomes unstable when $R_0 > 1$.*

Proof:

Using the Jacobian method, we show the local stability at the malware-free equilibrium.

By using system (2), the Jacobian can be taken as,

$$J(D_0) = \begin{bmatrix} -\alpha - Io\beta - \sigma & \gamma & -So\beta & 0 & \lambda \\ \alpha & -\gamma - \sigma & 0 & 0 & 0 \\ Io\,\beta & 0 & So\beta - \eta - \sigma - \phi & 0 & 0 \\ 0 & 0 & \eta & -\theta - \sigma & 0 \\ 0 & 0 & \phi & \theta & -\lambda - \sigma \end{bmatrix}$$

At the equilibrium point $D_0 = (S_0,P_0,I_0,Q_0,R_0) = \left(\frac{e\,(\gamma+ \sigma)}{\sigma(\alpha+ \gamma+ \sigma)}, \frac{e\,\alpha}{\sigma\,(\alpha + \gamma + \sigma)},0,0,0\right)$ the Jacobian matrix becomes

$$J(D_0) = \begin{bmatrix} -\alpha - \sigma & \gamma & -\frac{e\,\beta(\gamma+ \sigma)}{\sigma\,(\alpha + \gamma + \sigma)} & 0 & \lambda \\ \alpha & -\gamma - \sigma & 0 & 0 & 0 \\ 0 & 0 & \frac{e\,\beta(\gamma+ \sigma)}{\sigma\,(\alpha + \gamma + \sigma)} - \eta - \sigma - \phi & 0 & 0 \\ 0 & 0 & \eta & -\theta - \sigma & 0 \\ 0 & 0 & \phi & \theta & -\lambda - \sigma \end{bmatrix} \quad (8)$$

The eigen values of equation (8) are : -σ, -(α + γ + σ), -(θ + σ), -(λ + σ) and $-\eta - \sigma - \phi + \frac{e\,\beta(\gamma+ \sigma)}{\sigma(\alpha + \gamma + \sigma)}$ $i.e$ $\frac{e\,\beta(\gamma+ \sigma)}{\sigma\,(\alpha + \gamma + \sigma)}\left(1 - \frac{1}{Ro}\right)$.When $R_0 < 1$, all five eigenvalues have negative values.

Hence, the system will be locally stable if $R_0<1$ inthe malware-free equilibrium and unstable if $R_0> 1$.

Theorem 2: *The endemic equilibrium of the system is locally stable whenever $R_0 > 1$,*

Proof:

At the point of endemic equilibrium$D^* = (S^*, P^*, I^*, Q^*, R^*)$

$$J(D^*) = \begin{bmatrix} -\alpha - I*\beta - \sigma & \gamma & -S*\beta & 0 & \lambda \\ \alpha & -\gamma - \sigma & 0 & 0 & 0 \\ I*\beta & 0 & S*\beta - \eta - \sigma - \phi & 0 & 0 \\ 0 & 0 & \eta & -\theta - \sigma & 0 \\ 0 & 0 & \phi & \theta & -\lambda - \sigma \end{bmatrix} \quad (9)$$

The characteristic equation of the given 5 × 5 matrix J(D*) is:

$\mu^5 + c_4\mu^4 + c_3\mu^3 + c_2\mu^2 + c_1\mu + c_0 = 0$

where the coefficients are:

$c_4 = I * \beta - S * \beta + \alpha + \lambda + 5\sigma + \eta + \varphi + \theta + \gamma$

$c_3 = I^*\beta\lambda + 4I^*\beta\sigma + I^*\beta\eta + I^*\beta\phi + I^*\beta\theta + I^*\beta\gamma - S^*\beta\alpha - S^*\beta\lambda - 4S^*\beta\sigma - S^*\beta\theta - S^*\beta\gamma + \alpha\lambda + 4\alpha\sigma + \alpha\eta + \alpha\phi + \alpha\theta + 4\lambda\sigma + \lambda\eta + \lambda\phi + \lambda\theta + \lambda\gamma + 10\sigma^2 + 4\sigma\eta + 4\sigma\phi + 4\sigma\theta + 4\sigma\gamma + \eta\theta + \mu\eta + \phi\theta + \phi\gamma + \theta\gamma$

$c_2 = 3I^*\beta\lambda\sigma + I^*\beta\lambda\gamma + I^*\beta\lambda\theta + I^*\beta\lambda\gamma + 6I^*\beta\sigma^2 + 3I^*\beta\sigma\eta + 3I^*\beta\sigma\phi + 3I^*\beta\sigma\theta + 3I^*\beta\sigma\gamma + I^*\beta\eta\theta + I^*\beta\eta\gamma + I^*\beta\phi\theta + I^*\beta\phi\gamma + I^*\beta\theta\gamma - S^*\beta\alpha\lambda - 3S^*\beta\alpha\sigma - S^*\beta\alpha\lambda - 3S^*\beta\alpha\sigma - 3S^*\beta\sigma^2 - 3S^*\beta\sigma\gamma - S^*\beta\theta\gamma + 3\alpha\lambda\sigma + \alpha\lambda\mu + 3\alpha\sigma\eta + 6\sigma\alpha^2 + 3\alpha\sigma\phi + 3\alpha\sigma\theta + 3\alpha\sigma\gamma + \lambda\sigma\phi + \lambda\sigma\theta + \lambda\sigma\gamma + \lambda\eta\theta + \lambda\eta\gamma + \lambda\phi\theta + \lambda\phi\gamma + \lambda\theta\gamma + 10\sigma^3 + 6\sigma\eta^2 + 6\sigma\phi^2 + 6\sigma\theta^2 + 6\sigma\gamma^2 + 3\sigma\eta\theta + 3\sigma\eta\gamma + 3\sigma\phi\theta + 3\sigma\phi\gamma + 3\sigma\theta\gamma + \eta\theta\gamma + \phi\theta\gamma$

$c_1 = 3I^*\beta\lambda\sigma^2 + 2I^*\beta\lambda\sigma\eta + 2I^*\beta\lambda\sigma\phi + 2I^*\beta\lambda\sigma\theta + 2I^*\beta\lambda\sigma\gamma + I^*\beta\lambda\gamma\eta + 4I^*\beta\sigma^3 + 3I^*\beta\sigma^2\eta + 3I^*\beta\sigma^2\phi + 3I^*\beta\sigma^2\theta + 3I^*\beta\sigma^2\gamma + 2I^*\beta\sigma\eta\phi + 2I^*\beta\sigma\eta\gamma + 2I^*\beta\sigma\phi\gamma + 2I^*\beta\sigma\theta\gamma + I^*\beta\eta\theta\eta + I^*\beta\eta\theta\phi + I^*\beta\eta\theta\gamma - 2S^*\beta\alpha\lambda\sigma - 3S^*\beta\alpha\sigma^2 - 2S^*\beta\alpha\sigma\eta - 3S^*\beta\alpha\sigma\gamma - 2S^*\beta\alpha\sigma\theta - 2S^*\beta\alpha\sigma\phi - 4S^*\beta\sigma^3 - 3S^*\beta\sigma^2\eta - 3S^*\beta\sigma^2\phi - 3S^*\beta\sigma^2\theta - 3S^*\beta\sigma^2\gamma - 2S^*\beta\sigma\eta\phi - 2S^*\beta\sigma\eta\gamma - 2S^*\beta\sigma\phi\gamma - 2S^*\beta\sigma\theta\gamma + 2\sigma\alpha\lambda\sigma + 2\sigma\alpha\sigma^2 + 2\sigma\alpha\sigma\eta + 2\sigma\alpha\sigma\phi + 2\sigma\alpha\sigma\theta + 2\sigma\alpha\sigma\gamma + 2\lambda\alpha\sigma^2 + 3\lambda\alpha\sigma\eta + 3\lambda\alpha\sigma\phi + 3\lambda\alpha\sigma\theta + 3\lambda\alpha\sigma\gamma + 2\lambda\alpha\sigma\phi + 2\lambda\alpha\sigma\theta + 2\lambda\alpha\sigma\gamma + 4\lambda\sigma^3 + 3\lambda\sigma\eta^2 + 3\lambda\sigma\phi^2 + 3\lambda\sigma\theta^2 + 3\lambda\sigma\gamma^2 + 4\sigma^3\eta + 4\sigma^3\phi + 4\sigma^3\theta + 4\sigma^3\gamma + 3\sigma^2\eta\theta + 3\sigma^2\eta\gamma + 3\sigma^2\phi\theta + 3\sigma^2\phi\gamma + 3\sigma^2\theta\gamma + 2\sigma\eta\theta\gamma + 2\sigma\phi\theta\gamma$

$c_0 = I^*\beta\lambda\sigma^3 + I^*\beta\lambda\sigma^2\eta + I^*\beta\lambda\sigma^2\theta + I^*\beta\lambda\sigma^2\gamma + I^*\beta\lambda\sigma\eta\gamma + I^*\beta\lambda\sigma\theta\eta + I^*\beta\sigma^4 + I^*\beta\sigma^3\eta + I^*\beta\sigma^3\phi + I^*\beta\sigma^3\theta + I^*\beta\sigma^3\gamma + I^*\beta\sigma^2\eta\theta + I^*\beta\sigma^2\phi\eta + I^*\beta\sigma^2\phi\gamma + I^*\beta\sigma\eta\phi\gamma + I^*\beta\sigma\phi\theta\gamma - S^*\beta\alpha\lambda\sigma^2 - S^*\beta\alpha\sigma^3 - S^*\beta\alpha\sigma^2\theta - S^*\beta\alpha\lambda\sigma\theta - S^*\beta\alpha\sigma^3 - S^*\beta\alpha\sigma^2\theta - S^*\beta\sigma^3 - S^*\beta\sigma^2\gamma - S^*\beta\sigma^2\theta\eta - S^*\beta\sigma^4 - S^*\beta\sigma^3\theta - S^*\beta\sigma^3\gamma - S^*\beta\sigma^2\theta\gamma + \alpha\lambda\sigma^3 + \alpha\lambda\sigma^2\eta + \alpha\lambda\sigma^2\phi + \alpha\lambda\sigma^2\theta + \alpha\lambda\sigma\gamma\theta + \alpha\lambda\sigma\phi\theta + \alpha\lambda\sigma^3\phi + \alpha\lambda\sigma^3\theta + \alpha\lambda\sigma^2\eta\theta +$

$\alpha\lambda\sigma^2\phi\theta + \lambda\sigma^4 + \lambda\sigma^3\eta + \lambda\sigma^3\phi + \lambda\sigma^3\theta + \lambda\sigma^3\gamma + \lambda\sigma^2\phi\eta + \lambda\sigma^2\phi\theta + \lambda\sigma^2\phi\gamma + \lambda\sigma\eta\phi\gamma + \lambda\sigma\phi\theta\gamma + \sigma^5 + \sigma^4\eta + \sigma^4\phi + \sigma^4\theta + \sigma^4\gamma + \sigma^3\eta\theta + \sigma^3\phi\theta + \sigma^3\phi\gamma + \sigma^3\theta\eta + \sigma^2\eta\theta\gamma + \sigma^2\phi\theta\gamma$

When $R_0 > 1$, the endemic equilibrium (S*, P*, I*, Q*, R*) is asymptoticallystable, according to the Routh-Hurwitz criterion [28].

Theorem 3: *If $R_0 < 1$, the system's malware-free equilibrium is globally asymptotically stable (GAS).*

Proof:

Consider a Lyapunov function,

$V = I + \frac{\eta}{\theta+\sigma} Q$

Compute the time derivative

$\frac{dV}{dt} = \frac{dI}{dt} + \frac{\eta}{\theta+\sigma}\frac{dQ}{dt}$

Substitution from the model equations

$\frac{dV}{dt} = [\ \beta SI - (\eta + \phi + \sigma)I] + \frac{\eta}{\theta+\sigma}[\ \eta I - (\theta + \sigma)\ Q\ ]$

$= I[\ \beta S - (\eta + \phi + \sigma) + \frac{\eta 2}{\theta+\sigma}\ ] - \frac{\eta}{\theta+\sigma}(\theta + \sigma)\ Q$

$= I[\ \beta S - (\eta + \phi + \sigma - \frac{\eta 2}{\theta+\sigma}\ )] - \eta Q$

Since all parameters are positive and $Q \geq 0$, the second term is non-positive.

At the disease-free equilibrium (DFE), $S \leq S_0$

Thus, $\frac{dV}{dt} \leq I[\beta S_0 - (\eta + \phi + \sigma)] = I[\ \beta \frac{e\ (\gamma+\sigma)}{\sigma(\alpha+\gamma+\sigma)} - (\eta + \phi + \sigma)] = I\ (\eta + \phi + \sigma)\ (R_0 - 1)$

If $R_0 < 1$, $\frac{dV}{dt} < 0$

Therefore, the malware-free equilibrium is GAS, if $R_0 < 1$.

Theorem 4: *The system's endemic equilibrium is GAS whenever $R_0 > 1$.*

Proof:

We consider the following non-linear Lyapunov function,

$Z = (\ S\text{-}S^*\text{-}S^*\ \log\frac{S}{S^*}) + (\ P\text{-}P^*\text{-}P^*\ \log\frac{P}{P^*}) + (\ I\text{-}I^*\text{-}I^*\ \log\frac{I}{I^*}) + (\ Q\text{-}Q^*\text{-}Q^*\ \log\frac{Q}{Q^*}) + (\ R\text{-}R^*\text{-}R^*\ \log\frac{R}{R^*})$

Differentiating Z along trajectories of system (1), we obtain

$$\dot{Z} = (1- \frac{S*}{S})\, \dot{S} + (1- \frac{P*}{P})\, \dot{P} +(1- \frac{I*}{I})\, \dot{I}+ (1- \frac{Q*}{Q})\, \dot{Q}+ (1- \frac{R*}{R})\, \dot{R}$$

Putting the value of $\dot{S}, \dot{P}, \dot{I}, \dot{Q}$ and $\dot{R}$ from the system (1), we get

$$\dot{Z} = (1- \frac{S*}{S})\, (e - \beta SI - \alpha S - \sigma S + \gamma P + \lambda R) + (1- \frac{P*}{P})\, (\alpha S - \gamma P - \sigma P) +(1- \frac{I*}{I})\, (\beta SI - \eta I - \phi I - \sigma I)+ (1- \frac{Q*}{Q})\, (\eta I - \theta Q - \sigma Q) + (1- \frac{R*}{R})\, (\phi I + \theta Q - \lambda R - \sigma R)$$

Now we use the equilibrium relations (for each component at D* we have the corresponding balance equality, e.g., $0 = e - \beta S^*I^* - \alpha S^* - \sigma S^* + \gamma P^* + \lambda R^*$, etc.). After straightforward but routine rearrangement and grouping of terms (collecting coefficients of differences and using the equilibrium identities to cancel constant parts), $\dot{Z}$ can be written in the following convenient form:

$$\dot{Z} = -\alpha S^* \psi (\frac{S}{S*}) - \gamma P^* \psi (\frac{P}{P*}) -(\eta+\phi+\sigma)\, I^* \psi (\frac{I}{I*}) - (\theta+\sigma) Q^* \psi (\frac{Q}{Q*}) - (\lambda+\sigma) R^* \psi(\frac{R}{R*})$$

where for $u > 0$ we define $\psi(u) = u - 1 - \log u$. Recall the elementary inequality $\psi(u) \geq 0$ for all $u > 0$ with equality only at $u = 1$. Because all equilibrium components S^*, P^*, I^*, Q^*, R^* and all coefficients $\alpha, \gamma, \eta, \phi, \sigma, \theta, \lambda, \beta$ are nonnegative (and the bracketed coefficients' sums are strictly positive), every term on the right-hand side is nonpositive. Hence, $\dot{Z} \leq 0$ for all $S,P,I,Q,R > 0$.

Moreover, $\dot{Z} = 0$ if and only if every ψ (.) term is zero, i.e., if and only if

$$\frac{S}{S*} = \frac{P}{P*} = \frac{I}{I*} = \frac{Q}{Q*} = \frac{R}{R*} = 1$$

(and $\frac{SI}{S*I*} = 1$ follows automatically), which is exactly $(S,P,I,Q,R) = D^*$. Thus the largest invariant set $\dot{Z} = 0$ is the singleton$\{D^*\}$.

By LaSalle's invariance principle [29], every positive solution of system (1) approaches D* as $t \to \infty$. Therefore, the endemic equilibrium D* is GAS whenever it exists in particular when $R_0 > 1$.

6. NUMERICAL METHODS AND SIMULATIONS

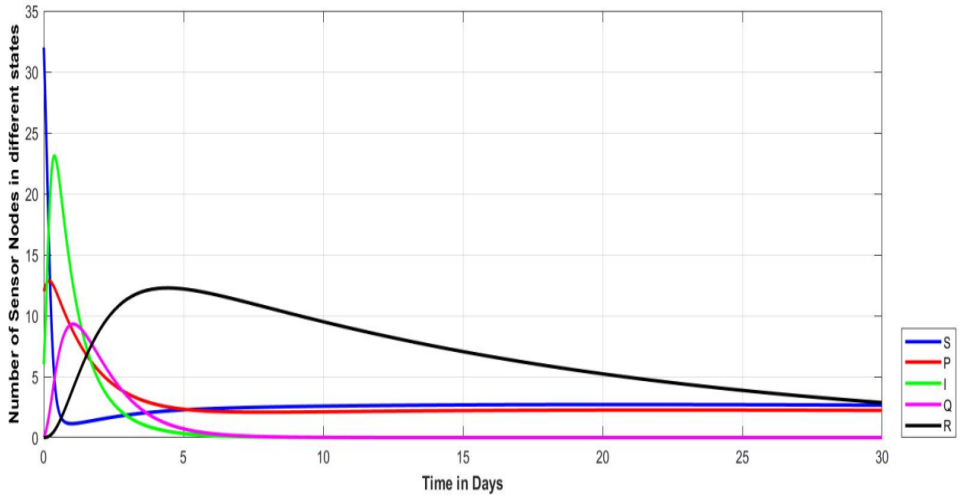

Figure 2: Dynamics of malware propagation with time when $R_0 < 1$.

In this section to validate theoretical results, we will use MATLAB to run numerical simulations for the two parameter sets that show how the model behaves based on the BRN.It is assumed that $0 \leq t \leq 30$ in both cases, and there are N=50 devices in total with S(0) = 32, P(0) = 12, I(0)=6, Q(0) = 0,R(0)=0. Additionally, the coefficients' numerical values are as follows: e=0.2, β=0.3, α=0.5, σ=0.05, γ=0.55, λ=0.01, η= 0.9, ϕ=0.01 and θ=0.65. The value of BRN $R_0 = 0.68 < 1$ and a disease-free stable state was obtained (see Figure 2). It is concluded that malware dies out from the computer networks. By Theorem 1, it is also verified.

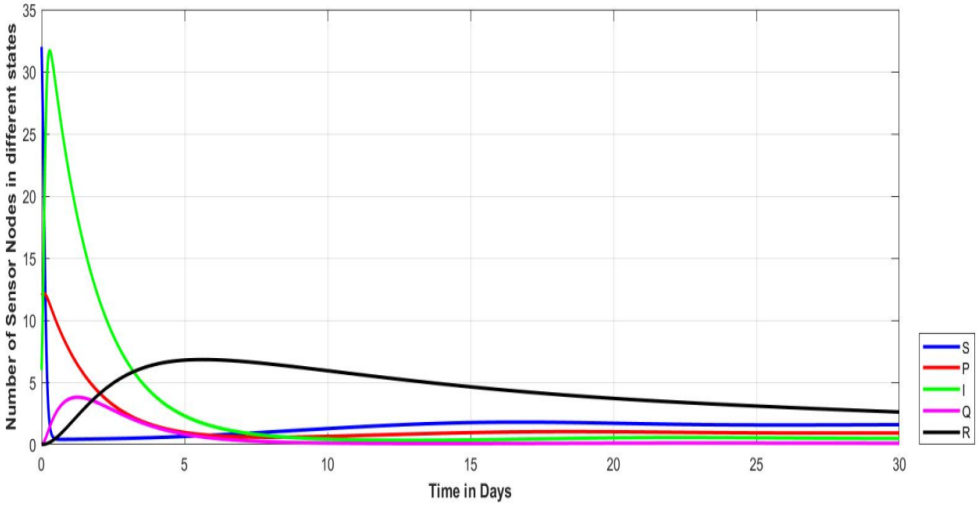

Figure 3: Dynamics of malware propagation with time when $R_0 > 1$.

Conversely, the second simulation takes into consideration e=0.5, β=0.5, α=0.35, σ=0.05 , γ=0.55, λ=0.01, η=0.25 ,ϕ=0.01 and θ=0.65 and consequently R_0=10.19 > 1. The system consequently reaches the endemic stable state (see Figure 3). Under these circumstances, malware continues to exist on computer networks. By Theorem 2, it is also verified.

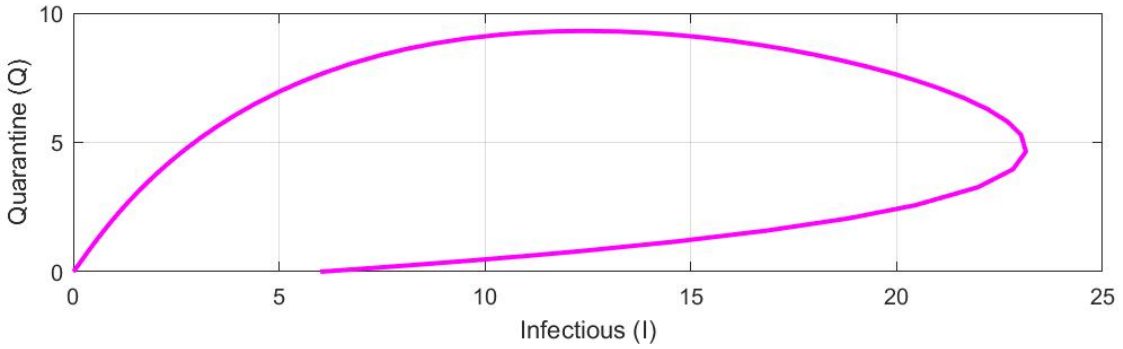

Figure 4: The classes I and Q's dynamic behavior with e=0.2, β=0.3, α=0.5, σ=0.05, γ=0.55, λ=0.01, η= 0.9, ϕ=0.01, and θ=0.65.

Figure 4 illustrates that, under the given parameter values, the infected I(t) and quarantined Q(t) populations initially vary but after all decline to zero. This corroborates that the system converges to the disease-free equilibrium, implying effective control and elimination of malware spread in the network.

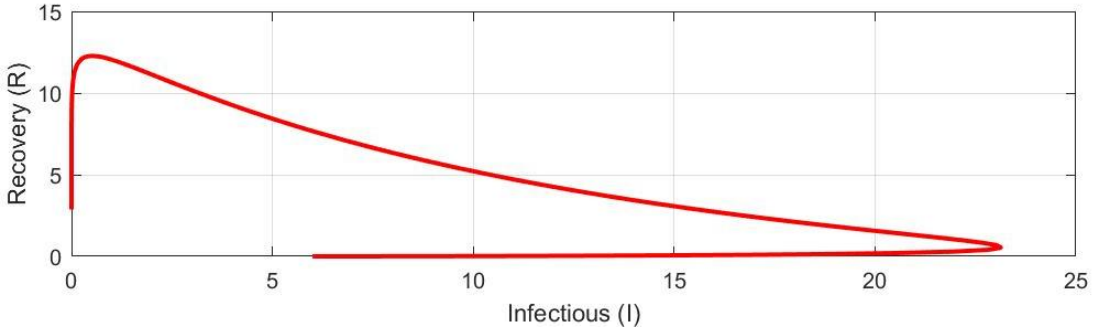

Figure 5: The classes I and R's dynamic behavior with e=0.2, β=0.3, α=0.5, σ=0.05, γ=0.55, λ=0.01, η= 0.9, ϕ=0.01, and θ=0.65.

Figure 5 shows that, under the given parameter values, the infected population I(t)disintegrates to zero as time increases. At the same time, the recovered population R(t) increases due to recovery from both infected and quarantined classes and eventually approaches its steady-state level, confirming effective malware control in the network.

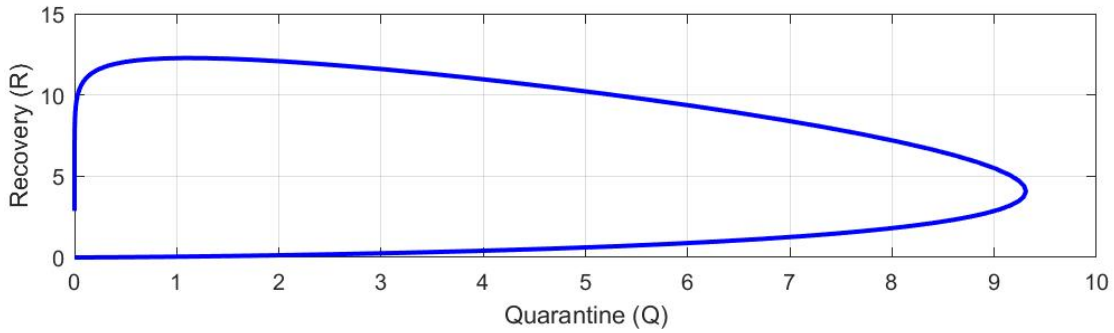

Figure 6: The classes Q and R's dynamic behavior with e=0.2, β=0.3, α=0.5, σ=0.05, γ=0.55, λ=0.01, η= 0.9, ϕ=0.01, and θ=0.65.

Figure 6 demonstrates that, for the given parameter values, the quarantined population Q(t) initially increases and then decreases to zero due to the high recovery rate θ, while the recovered population R(t) increases over time. This suggests that quarantined nodes are successfully treated and moved to the recovered class, leading the system toward the disease-free equilibrium.

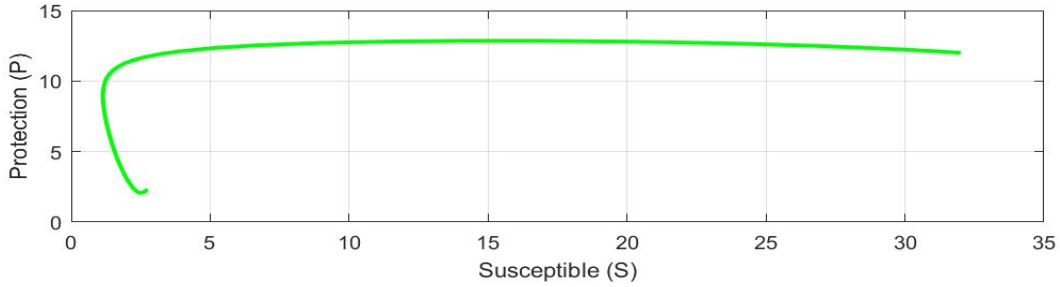

Figure 7: The classes S and P's dynamic behavior with e=0.2, β=0.3, α=0.5, σ=0.05, γ=0.55, λ=0.01, η= 0.9, ϕ=0.01, and θ=0.65.

Figure 7 shows that the susceptible population S(t) decreases over time due to protection and infection effects, while the protected population P(t) initially increases as susceptible nodes are moved into the protected class. At last, both S(t) and P(t) approach their respective equilibrium levels, indicating stabilization of the network under the applied protection mechanism.

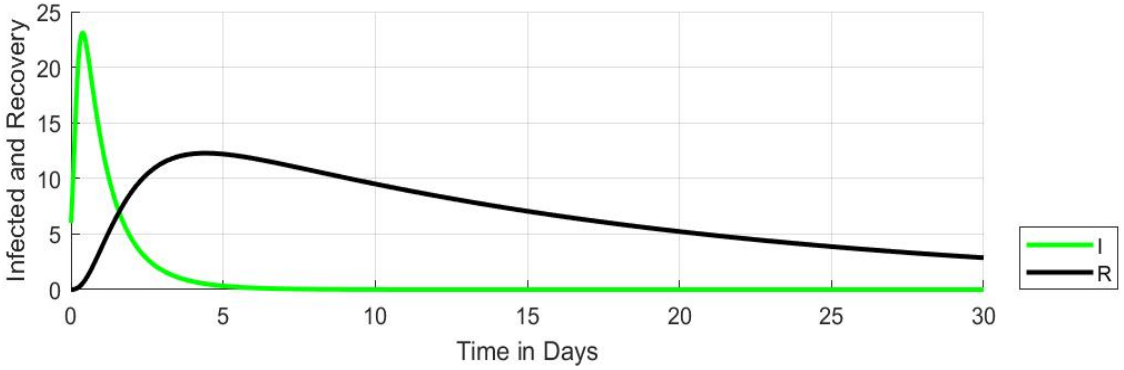

Figure 8: The classes I and R's dynamic behavior with η= 0.9, ϕ=0.01, σ=0.05, θ=0.65.

Figure 8 illustrates that, for the given parameter values, the infected population I(t) decreases over time due to the combined effects of quarantine, recovery, and natural removal. Simultaneously, the recovered population R(t) increases as infected nodes move into the recovered class and eventually approaches a stable equilibrium level.

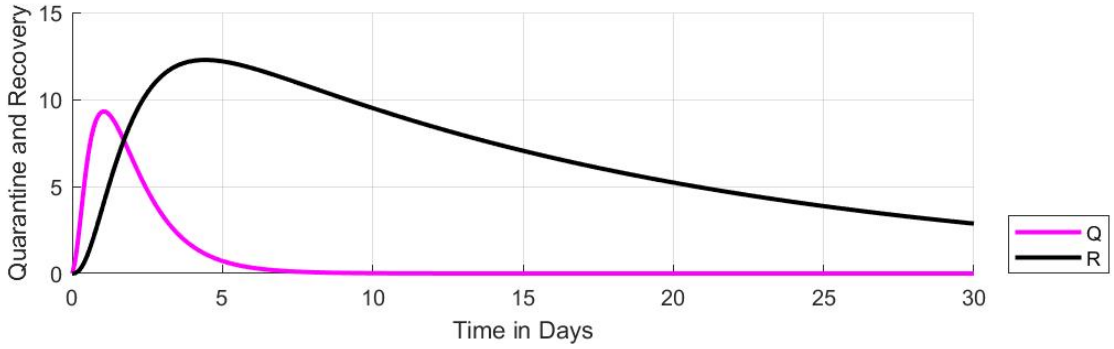

Figure 9: The classes Q and R's dynamic behavior with λ=0.01,σ=0.05, θ=0.65.

Figure 9 shows that the quarantined population Q(t) initially increases due to the isolation of infected nodes and then gradually decreases as individuals recover or are removed at rate θ and σ. Concurrently, the recovered population R(t) increases correspondingly and eventually reaches a steady-state level, indicating an effective transition from quarantine to recovery.

7. CONCLUSION

The principal objective of the suggested model is to mitigate the dissemination of malware throughout networks and extend the operational longevity of computer networks. To achieve this, an epidemic-based SPIQR model has been developed to analyze malware transmission within these networks. We investigated the intricate dynamics of malware dissemination and discerned two separate equilibrium states: one denotes a malware-free condition, and the other indicates an endemic condition. The BRN (R_0) for the theoretical framework was calculated, and its impact on the behavioral dynamics of the system was analyzed. Our findings show that when $R_0<1$, the system stabilizes and remains free of malware, whereas if $R_0> 1$, malware persists in the system in an endemic state. We also observed that increasing the rate of quarantine or protective measures leads to a decrease in infectious nodes. The synergistic application of isolation measures and protective protocols has enhanced the resilience and durability of computer

networks. In our future research, we will carry out relevant investigations and compare the results with those of other infectious disease models in order to confirm the method's feasibility.

CONFLICT OF INTERESTS

The authors declare that there is no conflict of interests.

REFERENCES

[1] M.E.J. Newman, S. Forrest, J. Balthrop, Email Networks and the Spread of Computer Viruses, Phys. Rev. E 66 (2002), 035101. https://doi.org/10.1103/physreve.66.035101.

[2] B.K. Mishra, N. Jha, SEIQRS Model for the Transmission of Malicious Objects in Computer Network, Appl. Math. Model. 34 (2010), 710-715. https://doi.org/10.1016/j.apm.2009.06.011.

[3] J. Hernández Guillén, A. Martín del Rey, L. Hernández Encinas, Study of the Stability of a SEIRS Model for Computer Worm Propagation, Physica: Stat. Mech. Appl. 479 (2017), 411-421. https://doi.org/10.1016/j.physa.2017.03.023.

[4] R.M. Anderson, R.M. May, Infectious Diseases of Humans, Oxford University Press, Oxford, 1991. https://doi.org/10.1093/oso/9780198545996.001.0001.

[5] R.M. Anderson, R.M. May, Population Biology of Infectious Diseases: Part I, Nature 280 (1979), 361-367. https://doi.org/10.1038/280361a0.

[6] M. Youssef, C. Scoglio, An Individual-Based Approach to SIR Epidemics in Contact Networks, J. Theor. Biol. 283 (2011), 136-144. https://doi.org/10.1016/j.jtbi.2011.05.029.

[7] L. Feng, X. Liao, Q. Han, H. Li, Dynamical Analysis and Control Strategies on Malware Propagation Model, Appl. Math. Model. 37 (2013), 8225-8236. https://doi.org/10.1016/j.apm.2013.03.051.

[8] A.M. del Rey, R.C. Vara, S.R. González, A Computational Propagation Model for Malware Based on the SIR Classic Model, Neurocomputing 484 (2022), 161-171. https://doi.org/10.1016/j.neucom.2021.08.149.

[9] W.O. Kermack, A.G. McKendrick, A Contribution to the Mathematical Theory of Epidemics, Proc. R. Soc. Lond. Ser. A 115 (1927), 700-721. https://doi.org/10.1098/rspa.1927.0118.

[10] W.O. Kermack, A.G. McKendrick, Contributions to the Mathematical Theory of Epidemics. II. —The Problem of Endemicity, Proc. R. Soc. Lond. Ser. A. 138 (1932), 55-83. https://doi.org/10.1098/rspa.1932.0171.

[11] W.O. Kermack, A.G. McKendrick, Contributions to the Mathematical Theory of Epidemics. III.—Further Studies of the Problem of Endemicity, Proc. R. Soc. Lond. Ser. A. 141 (1933), 94-122. https://doi.org/10.1098/rspa.1933.0106.

[12] M. Xiao, S. Chen, W.X. Zheng, Z. Wang, Y. Lu, Tipping Point Prediction and Mechanism Analysis of Malware Spreading in Cyber–Physical Systems, Commun. Nonlinear Sci. Numer. Simul. 122 (2023), 107247. https://doi.org/10.1016/j.cnsns.2023.107247.

[13] N.P. Dong, H.V. Long, N.T.K. Son, The Analysis of a Fractional Network-Based Epidemic Model with Saturated Treatment Function and Fuzzy Transmission, Iran. J. Fuzzy Syst. 20 (2023), 1-18.

[14] R.M. Carnier, Y. Li, Y. Fujimoto, J. Shikata, Modeling Exact Markov Chains for Malware Based on Random Propagation, Preprint, (2023). https://doi.org/10.36227/techrxiv.22047527.v1.

[15] A. Prajapati, A Propagation Model of Malicious Objects via Removable Devices and Sensitivity Analysis of the Parameters, in: A.A. Abd El-Latif, Y. Maleh, W. Mazurczyk, et al. (eds) Advances in Cybersecurity, Cybercrimes, and Smart Emerging Technologies. CCSET 2022. Engineering Cyber-Physical Systems and Critical Infrastructures, vol 4. Springer, Cham, (2023). https://doi.org/10.1007/978-3-031-21101-0_6

[16] J. Liu, T. Saeed, A. Zeb, Delay Effect of an E-Epidemic SEIRS Malware Propagation Model with a Generalized Non-Monotone Incidence Rate, Results Phys. 39 (2022), 105672. https://doi.org/10.1016/j.rinp.2022.105672.

[17] R.K. Shakya, K. Rana, A. Gaurav, P. Mamoria, P.K. Srivastava, Stability Analysis of Epidemic Modeling Based on Spatial Correlation for Wireless Sensor Networks, Wirel. Pers. Commun. 108 (2019), 1363-1377. https://doi.org/10.1007/s11277-019-06473-0.

[18] J. Liu, P.E. Pare, A. Nedic, C.Y. Tang, C.L. Beck, et al., Analysis and Control of a Continuous-Time Bi-Virus Model, IEEE Trans. Autom. Control. 64 (2019), 4891-4906. https://doi.org/10.1109/tac.2019.2898515.

[19] Z. Zhang, S. Kumari, R.K. Upadhyay, A Delayed E-Epidemic SLBS Model for Computer Virus, Adv. Differ. Equ. 2019 (2019), 414. https://doi.org/10.1186/s13662-019-2341-8.

[20] B.K. Mishra, N. Keshri, Mathematical Model on the Transmission of Worms in Wireless Sensor Network, Appl. Math. Model. 37 (2013), 4103-4111. https://doi.org/10.1016/j.apm.2012.09.025.

[21] B.K. Mishra, S.K. Srivastava, B.K. Mishra, A Quarantine Model on the Spreading Behavior of Worms in Wireless Sensor Network, Trans. IoT Cloud Comput. 2 (2014), 1-13.

[22] B.K. Mishra, I. Tyagi, Defending Against Malicious Threats in Wireless Sensor Network: A Mathematical Model, Int. J. Inf. Technol. Comput. Sci. 6 (2014), 12-19. https://doi.org/10.5815/ijitcs.2014.03.02.

[23] Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria, C.H. Nwokoye, I.I. Umeh, The Seiqr–V Model: On a More Accurate Analytical Characterization of Malicious Threat Defense, Int. J. Inf. Technol. Comput. Sci. 9 (2017), 28-37. https://doi.org/10.5815/ijitcs.2017.12.04.

[24] Z. Zhang, F. Si, Dynamics of a Delayed Seirs-V Model on the Transmission of Worms in a Wireless Sensor Network, Adv. Differ. Equ. 2014 (2014), 295. https://doi.org/10.1186/1687-1847-2014-295.

[25] S.R. Biswal, S.K. Swain, Analyze the Effects of Quarantine and Vaccination on Malware Propagation in Wireless Sensor Network, Int. J. Innov. Technol. Explor. Eng. 8 (2019), 3537-3543. https://doi.org/10.35940/ijitee.j9761.0881019.

[26] S. Mohanty, P.K. Nayak, S. Mohanty, Quarantine Approach to Defend Against Malicious Codes in a Traditional Antivirus Computer Network, in: A. Sikander, M. Zurek-Mortka, C.K. Chanda, P.K. Mondal, (eds) Advances in Energy and Control Systems. ESDA 2022. Lecture Notes in Electrical Engineering, vol 1148. Springer, Singapore, 2024. https://doi.org/10.1007/978-981-97-0154-4_27.

[27] P. van den Driessche, J. Watmough, Reproduction Numbers and Sub-Threshold Endemic Equilibria for Compartmental Models of Disease Transmission, Math. Biosci. 180 (2002), 29-48. https://doi.org/10.1016/s0025-5564(02)00108-6.

[28] H. Zhang, R.K. Upadhyay, G. Liu, Z. Zhang, Hopf Bifurcation and Optimal Control of a Delayed Malware Propagation Model on Mobile Wireless Sensor Networks, Results Phys. 41 (2022), 105926. https://doi.org/10.1016/j.rinp.2022.105926.

[29] M.A. Safi, S.M. Garba, Global Stability Analysis of SEIR Model with Holling Type II Incidence Function, Comput. Math. Methods Med. 2012 (2012), 826052. https://doi.org/10.1155/2012/826052.