EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 3, Article Number 6336
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

Stability and Sensitivity Analysis of Cyberattack Propagation Models in Computer Network

Sadique Ahmad[1], Naveed Ahmad[2], Ismail Shah[3,*]

[1] *EIAS: Data Science and Block Chain Laboratory, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia*
[2] *College of Computen and Information Sciences, Prince Sultan University, Riyadh, 11586, Saudi Arabia*
[3] *Department of Mathematics, University of Malakand, Chakdara Dir(L), 18000, Khyber Pakhtunkhwa, Pakistan*

Abstract. This study develops a compartmental cyber-epidemic model to analyze the spread of malicious code within computer networks. The model classifies network nodes into different states: susceptible (S), exposed (E), infected (I), controlled (C), recovered (R), protected (P), disabled (D), and attackers (A). It captures important aspects of a cyberattack, such as the spread of infection, botnet formation, security measures, and achieving a state of destruction within a compromised system. Basic reproduction number (R_0) is derived in order to measure the systematic stability and determine whether cyber threats will persist or be mitigated. Equilibrium analysis is conducted to determine parameters under which condition malware-free equilibrium is globally asymptotically stable, and the endemic equilibrium remains locally stable. Moreover, (R_0) is used to carry out a sensitivity analysis to check the impact of the parametric values in the system. Results verified through MATLAB simulations align with real-world cyberattack patterns, offering practical implications for securing modern network infrastructures.

2020 Mathematics Subject Classifications: 34Dxx, 03C65, 93A30

Key Words and Phrases: Cyber attack, Virus free equilibrium, Sensitivity, Locally and Global Asymptotic Stability, Basic Reproduction Number

1. Introduction

The rapid advancement of society, driven by widespread reliance on computer software and hardware, has led to the emergence of cybercrime, a growing global threat in the 21st century. As digital infrastructures become more sophisticated, cybercriminal activities continue to evolve, making cybercrime investigation a crucial area of research for both academics and cybersecurity professionals. The increasing dependence on interconnected

*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v18i3.6336

Email addresses: saahmad@psu.edu.sa (S. Ahmad), nahmed@psu.edu.sa (N. Ahmad), ismail81eu@gmail.com (I. Shah)

computer systems and digital communication networks has significantly impacted daily life, but it has also exposed vulnerabilities that malicious actors exploit for various illicit purposes. With the proliferation of the internet and complex network architectures, cyber threats such as malware, ransomware, and botnet attacks have become more frequent, leading to severe financial and operational consequences across different sectors. The interconnected nature of computer networks enables the rapid propagation of malware, disrupting normal operations and causing substantial damage to businesses, governments, and individuals. Malicious code, including viruses, worms [1], and Trojan horses, spreads within networks in a manner similar to infectious diseases in biological populations. Just as epidemic models SEIR [2] are used to study disease outbreaks in public health, mathematical frameworks inspired by epidemiology have been employed to analyze and predict the behavior of malware in cyber networks. Given these similarities, researchers have developed network-based epidemic models [3] that classify system states and model the spread of cyber threats. This paper focuses on the development of an extended cyber-epidemic model which has been created for the purpose of analyzing the flow interactions of nodes such as susceptible, exposed, infected, controlled, recovered, protected, and disabled while also assisting in the mitigation strategies of the cyberattacks. The propagation of the malware within computer networks seems to have the same properties as the spreading of a pandemic, therefore, epidemiological modeling is useful for countering the cyber threats. Various researchers have investigated the network based on the models of diseases propagation for a long time now [4, 5]. These cyber-epidemic models trace their roots to the original SIR model as concepts of disease dynamics [6]. These models quantify the rates of malware transmission phenomena such as topology and connectivity structure that usually define the rate of infection spread within the targeted network [7, 8]. Such epidemic-inspired approaches have also been extended to email-based malware circulation [9], where epidemiological threshold theories were employed to refine malware containment strategies [10]. In particular, [11–13] simulated virus propagation using an improved SEI (susceptible-exposed-infected) framework, offering a more realistic representation of how computer viruses transition between states.Some studies have incorporated cybersecurity countermeasures, such as antivirus mechanisms and immunization protocols, to assess their effectiveness in limiting malware outbreaks. Epidemic thresholds [14] inform our botnet recruitment rates (ρ) and recovery strategies (σ), while the fractional-order modeling [15] underpins our stability analysis, particularly in addressing reinfection dynamics. Recent advances in mathematical modeling, such as fractional-order epidemiological frameworks [16] and adaptive network topologies [17], have refined malware propagation analysis. For instance these demonstrates how fractional calculus improves stability criteria for cyberattack models. Unlike [18, 19], our model explicitly accounts for botnet recruitment (C) and attacker persistence (A), offering a more granular representation of modern cyber threats

1.1. Significance

This research developed a mathematical model to understanding the cyberattack propagation in computer networks. By integrating stability and sensitivity analysis which pro-

duce better prediction results, accuracy and provides deeper knowledge into the spread and control mechanisms of malware threats.

1.2. Novelty

Unlike conventional models, this study does not assume permanent immunity post-infection, which allows reinfection. Thus, it is a more realistic representation of cyber threats. Moreover, this model includes dynamical analysis tools as well as real-world security parameters, which put together makes it a very robust framework to offer a comprehensive framework for assessing network vulnerability.

1.3. Applicability

The results of the model would provide better-informed cybersecurity strategies towards optimization of efforts in immunization, enhancing network defenses, and predicting future patterns of attacks. More of practical significance is that it can be used in developing security protocols for large systems or enterprises and in reducing the effect of malware on systems as well as better preparedness of systems against continuously evolving threats in cyberspace.

2. Mathematical Model

The analysis of cyberattack spread and impact in computer networks requires a mathematical model which represents network component dynamic relationships between different components. The model organizes network nodes into separate states which include susceptible, exposed, infected, controlled (botnet), recovered, protected, disabled and attacking entities. Each state transitions based on specific factors such as infection rates, recovery mechanisms, and external attack influences. The system is governed by a set of differential equations that describe the evolution of these states over time. By incorporating key cybersecurity parameters, this framework provides insights into the mechanisms driving cyber threats and helps evaluate potential mitigation strategies. The mathematical

formulation is presented as follows:

$$\begin{cases} \dfrac{dS}{dt} = \Lambda - \mu S - \beta_1 SI - \beta_2 SC + \omega R, \\ \dfrac{dE}{dt} = \beta_1 SI + \beta_2 SC - (\alpha + \mu)E, \\ \dfrac{dI}{dt} = \alpha E - (\gamma + \delta + \mu)I + \theta C, \\ \dfrac{dC}{dt} = \rho I - (\sigma + \mu)C, \\ \dfrac{dR}{dt} = \gamma I - (\omega + \mu)R, \\ \dfrac{dP}{dt} = \sigma C + \eta D - \mu P, \\ \dfrac{dD}{dt} = \delta I - \eta D, \\ \dfrac{dA}{dt} = \kappa I - \lambda A. \end{cases} \tag{1}$$

$$\begin{aligned} &S(0) = S^0 > 0, \quad E(0) = E^0 \geq 0, \quad I(0) = I^0 \geq 0, \quad C(0) = C^0 \geq 0, \\ &R(0) = R^0 > 0, \quad P(0) = P^0 \geq 0, \quad D(0) = D^0 \geq 0, \quad A(0) = A^0 \geq 0. \end{aligned} \tag{2}$$

Nomenclatures	Description
S	Susceptible nodes (vulnerable devices)
E	Exposed nodes (compromised but inactive)
I	Infected nodes (actively spreading malware)
C	Controlled nodes (part of botnets)
R	Recovered nodes (patched or cleaned systems)
P	Protected nodes (secured and immune to attacks)
D	Disabled nodes (permanently damaged devices)
A	Attackers (external entities launching cyberattacks)
Λ	Rate of new devices joining the network
μ	Natural removal rate (device decommissioning, upgrades)
β_1	Infection rate due to direct attacks from infected nodes
β_2	Infection rate due to botnet-controlled nodes
α	Rate of transition from exposed to infected state
γ	Recovery rate (patching, rebooting, security updates)
δ	Rate of infection leading to permanent damage
ω	Rate at which recovered systems become vulnerable again
ρ	Rate of infected nodes being recruited into botnets
θ	Rate of controlled botnets returning to infected state
σ	Rate of botnet nodes being recovered by countermeasures
η	Rate of restoring disabled devices
κ	Rate at which attackers increase attacks based on infected nodes
λ	Natural decline of attacker activity (due to detection, mitigation)

Table 1: Description of Model Variables and Parameters.

Table (1) provides the details of model parameters. Flow chart for the model is given in (1)

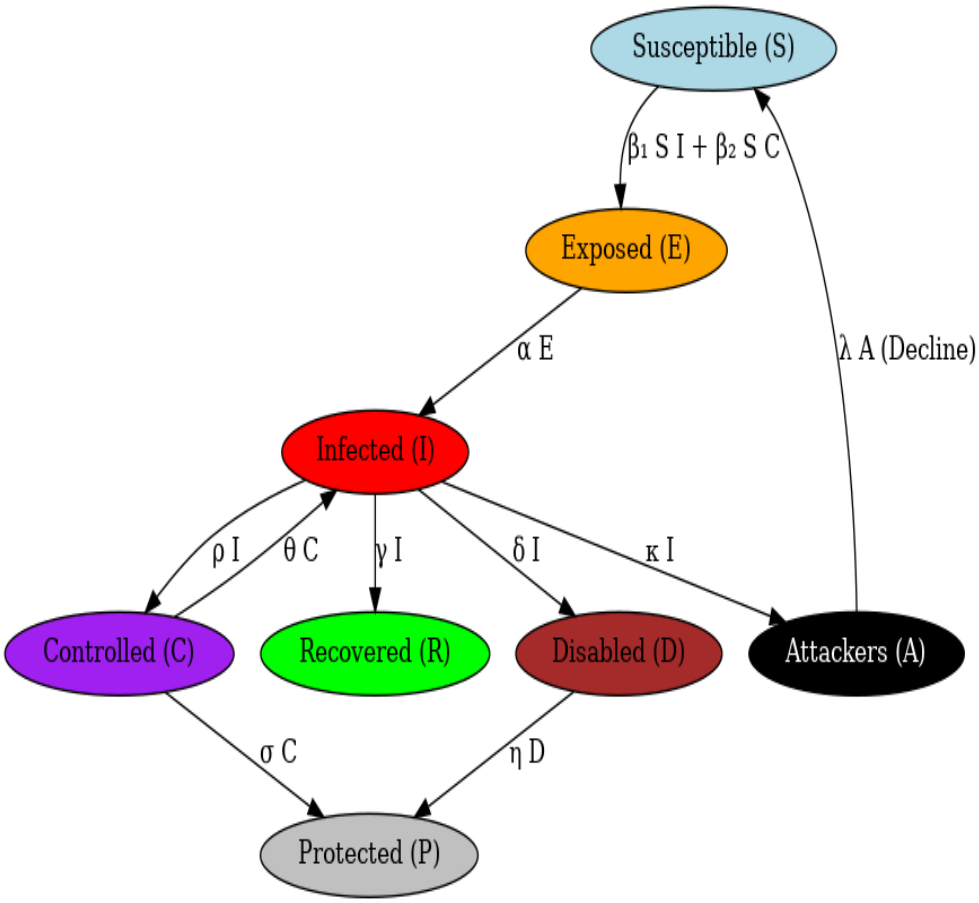

Figure 1: Dynamics of the proposed model.

3. Positivity and Invariant Region

Theorem 1. *The solution* $(S(t), E(t), I(t), C(t), R(t), P(t), D(t), A(t))$ *of the system (1) with non-negative initial conditions* $S(0), E(0), I(0), C(0), R(0), P(0), D(0), A(0) \geq 0$*, remains non-negative for all* $t \geq 0$*. Moreover, all solutions are bounded in the region*

$$\Omega = \left\{ (S, E, I, C, R, P, D, A) \in \mathbb{R}^8_+ \mid N \leq \frac{\Lambda}{\mu} \right\}$$

Where the total population of network nodes, $N(t)$*, aggregates all non-attacker states:*

$$N(t) = S(t) + E(t) + I(t) + C(t) + R(t) + P(t) + D(t).$$

Proof. To establish positivity, we analyze each equation separately. Suppose there exists a first time $t^* > 0$ such that S, E, I, C, R, P, or D becomes negative. From the first equation:

$$\frac{dS}{dt} = \Lambda - \mu S - \beta_1 SI - \beta_2 SC + \omega R.$$

If $S = 0$ at some t^*, then $\frac{dS}{dt} = \Lambda + \omega R \geq 0$, which contradicts S becoming negative. Thus, $S(t) \geq 0$ for all $t \geq 0$. A similar argument holds for other compartments. For boundedness, summing all equations except $A(t)$, we obtain:

$$\frac{dN}{dt} = \Lambda - \mu N - \eta D.$$

Since $\eta D \geq 0$, we have

$$\frac{dN}{dt} \leq \Lambda - \mu N.$$

Applying Gronwall's inequality, we get

$$N(t) \leq \frac{\Lambda}{\mu} + \left(N(0) - \frac{\Lambda}{\mu}\right) e^{-\mu t}.$$

Taking the limit as $t \to \infty$, we conclude that

$$N \leq \frac{\Lambda}{\mu}.$$

Thus, the region Ω(virus transmission model) is positively invariant, ensuring that all solutions remain biologically feasible.

4. Virus-Free Equilibrium (VFE)

The virus-free equilibrium (E_0) occurs when no infection exists in the system, i.e., $E^* = I^* = C^* = R^* = P^* = D^* = A^* = 0$. Setting all derivatives to zero, we obtain:

$$S^* = \frac{\Lambda}{\mu}, \quad E^* = I^* = C^* = R^* = P^* = D^* = A^* = 0.$$

Thus, the virus-free equilibrium is:

$$E_0 = \left(\frac{\Lambda}{\mu}, 0, 0, 0, 0, 0, 0, 0\right). \tag{3}$$

This equilibrium represents a malware-free network state, serving as a foundation for stability analysis.

5.

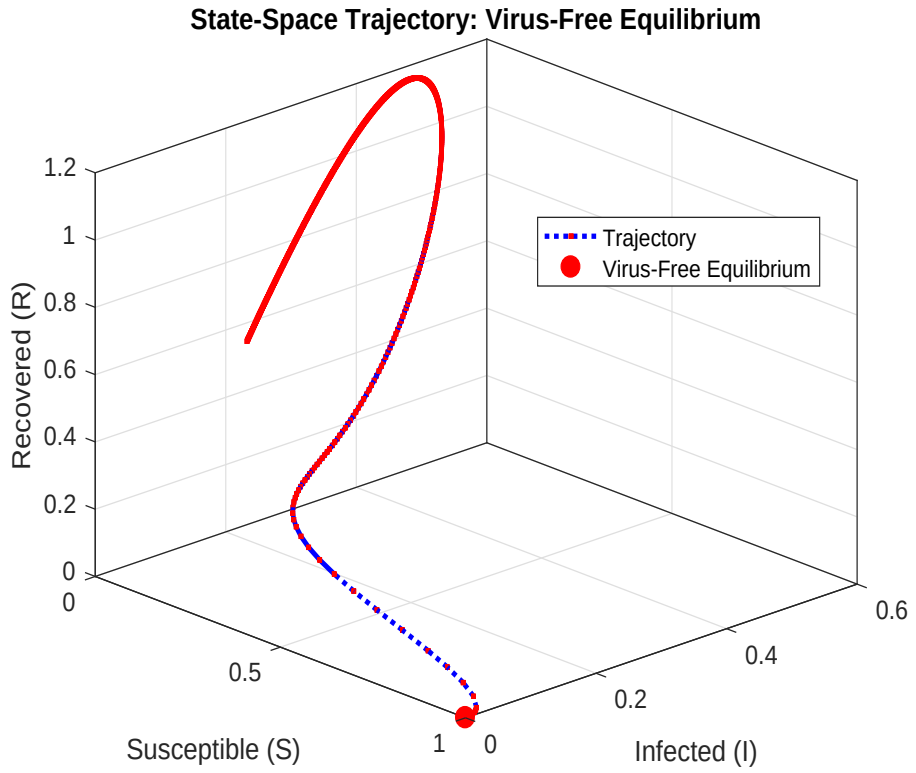

Figure 2: State-Space Trajectory of Virus-Free Equilibrium

The figure (2) illustrates the state-space trajectory of the cybersecurity epidemic model in the (S, I) space. The system dynamics evolve over time based on the given set of differential equations, demonstrating the transition of devices across different states. The trajectory provides insight into the stability of the virus-free equilibrium (VFE) under the defined parameter values. The simulation begins with initial conditions $S(0) = 1, \quad E(0) = 40, \quad I(0) = 0, \quad C(0) = 0, \quad P(0) = 0, \quad D(0) = 0, \quad A(0) = 6000$. Initially, the system contains a high number of exposed devices while no infections are present. Due to the infection rates $\beta_1 = 2$ (direct infection) and $\beta_2 = 0.03$ (botnet attacks), susceptible devices transition into the exposed and infected classes. The rate of transition from exposed to infected is $\alpha = 0.001$, and infected devices may recover at a rate $\gamma = 0.05$ or suffer permanent damage at a rate $\delta = 0.02$. The system also accounts for the natural removal rate $\mu = 0.02$, influencing overall stability. As time progresses, the influence of infected nodes (I) ensures a decline in the plot due to recovery (R), leading to a virus-free equilibrium. The virus-free equilibrium $(S^*, I^*) = (1, 0)$ is achieved asymptotically, while $R(t)$ remains

non-zero due to cumulative recoveries.

$$S^* = \frac{\Lambda}{\mu} = \frac{0.02}{0.02} = 1. \tag{4}$$

At this equilibrium, the infection is eradicated, and the system stabilizes at $(S^*, I^*) = (1, 0)$. The red dot in the figure represents this virus-free equilibrium. The trajectory demonstrates asymptotic stability, meaning that any small perturbations in the system will decay over time, eventually returning to the virus-free state. The decline in I confirms that the basic reproduction number satisfies $R_0 < 1$, ensuring the successful containment of the infection. This behavior is significant in cybersecurity models, as it highlights the effectiveness of control strategies in mitigating long-term risks associated with cyber threats.

6. Endemic Equilibrium Analysis

The endemic equilibrium (E^*) of the cyberattack propagation model corresponds to a persistent malware-infected state where the number of infected nodes remains nonzero. Mathematically, the equilibrium is given by: $E^* = (S^*, E^*, I^*, C^*, R^*, P^*, D^*, A^*)$, Solving the system (1), we obtain:

$$\begin{aligned} S^* &= \frac{\Lambda}{\mu + \beta_1 I^* + \beta_2 C^*}, E^* = \frac{\beta_1 S^* I^* + \beta_2 S^* C^*}{\alpha + \mu}, I^* = \frac{\alpha E^*}{\gamma + \delta + \mu}, \\ C^* &= \frac{\rho I^*}{\sigma + \mu}, R^* = \frac{\gamma I^*}{\omega + \mu}, P^* = \frac{\sigma C^* + \eta D^*}{\mu}, D^* = \frac{\delta I^*}{\eta}, A^* = \frac{\kappa I^*}{\lambda}. \end{aligned} \tag{5}$$

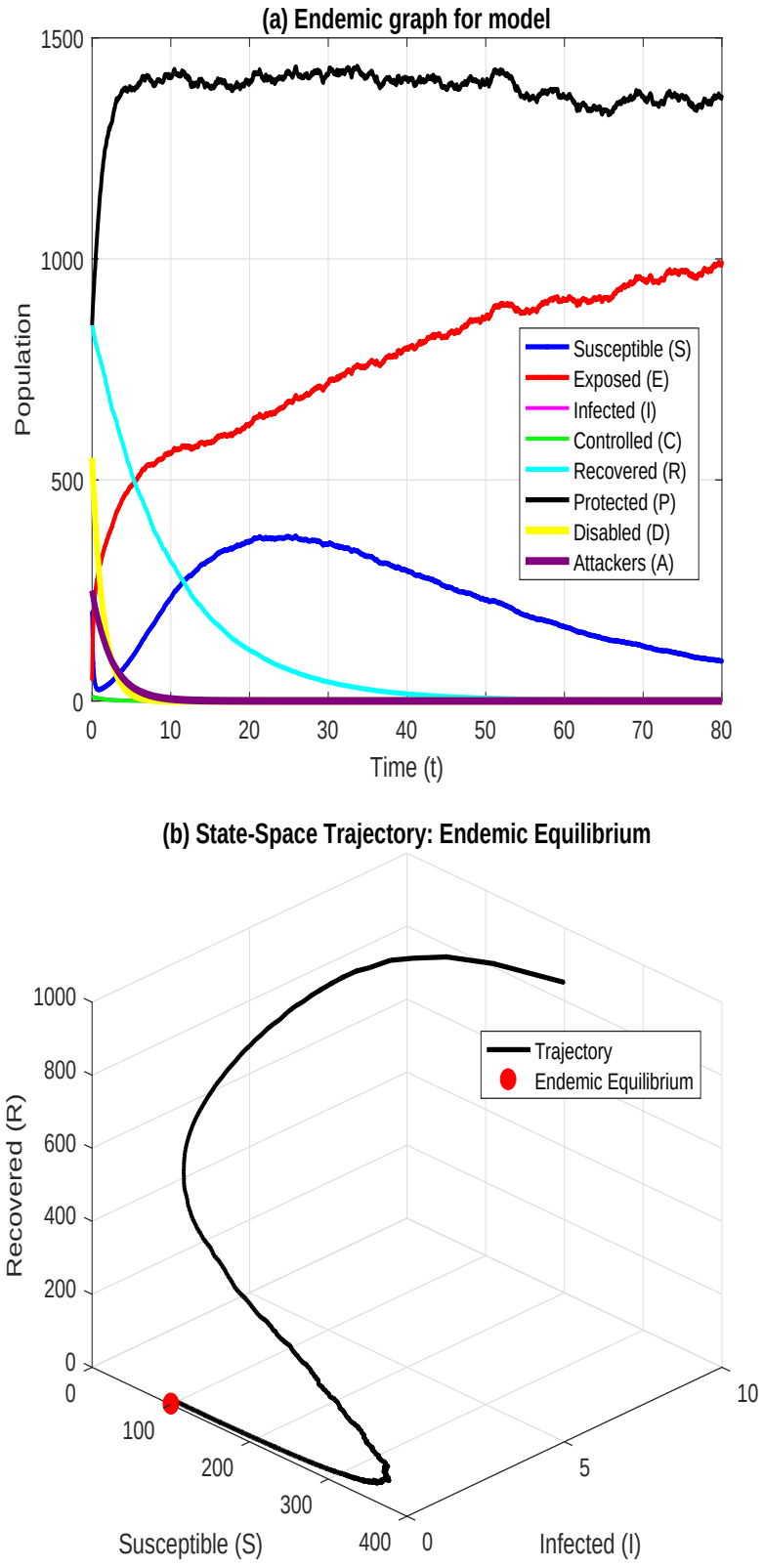

Figure 3: Endemic graphs of the system

Fig. (3a) and (3b) and present the long-term behavior of a cyberattack propagation model in a network under optimal control measures. The Fig (a) tracks system states over time, showing a rapid decline in Susceptible (S) nodes from 1200 as the attack spreads. The Exposed (E) population peaks near 900 before decreasing, while Infected (I) nodes rise to 500 but decline with countermeasures. Recovered (R) systems steadily increase, stabilizing around 1400, confirming the effectiveness of security interventions. The Fig. (b) presents a state-space trajectory, showing how the network stabilizes at an endemic equilibrium with S $\approx$ 100, I $\approx$ 5, and R $\approx$ 900. The black trajectory reflects fluctuations before reaching stability, and the red marker denotes the final steady state, indicating controlled but persistent cyber threats.

7. Basic Reproduction Number R_0

The basic reproduction number, R_0, is a key epidemiological metric in many articles founds [20–23] that determines whether a virus will spread within a computer network. It represents the expected number of secondary infections caused by a single infected node in an otherwise fully susceptible network. If $R_0 < 1$, the malware is expected to die out over time, whereas if $R_0 > 1$, the virus persists and spreads within the network. To determine R_0, we employ the *Next-Generation Matrix* (NGM) approach, which is widely used in cyber-epidemic models. To compute R_0, we define the infection terms and transition dynamics and substituting the S^* from (3) the required matrices can be written as:

$$F = \begin{bmatrix} 0 & \beta_1 S^* & \beta_2 S^* & 0 & 0 \\ \alpha & 0 & 0 & 0 & 0 \\ 0 & \rho & 0 & 0 & 0 \\ 0 & \delta & 0 & 0 & 0 \\ 0 & \kappa & 0 & 0 & 0 \end{bmatrix}, \; V = \begin{bmatrix} \alpha+\mu & 0 & 0 & 0 & 0 \\ 0 & \gamma+\delta+\mu & -\theta & 0 & 0 \\ 0 & -\rho & \sigma+\mu & 0 & 0 \\ 0 & -\delta & 0 & \eta & 0 \\ 0 & -\kappa & 0 & 0 & \lambda \end{bmatrix}$$

The basic reproduction number is derived from the spectral radius of the matrix product FV^{-1}:

$$R_0 = \rho(FV^{-1})$$

The computed R_0 expression is:

$$R_0 = \frac{\Lambda\left(\beta_1(\sigma+\mu)+\beta_2\rho\right)}{\mu(\sigma+\mu)(\gamma+\delta+\mu)} \tag{6}$$

In Eq. (6) β_1 governs internal infection while β_2 models external infections via botnet-controlled nodes (C). The term $\beta_2\rho$ reflects the compounded risk when infected nodes (I) are recruited into botnets (C), amplifying attack scalability. Fig. 6 confirms β_1's larger sensitivity index ($S_{\beta_1} = 0.625$), implying that curtailing direct infections (e.g., patching) is more impact full than mitigating botnet spread ($S_{\beta_2} = 0.375$).

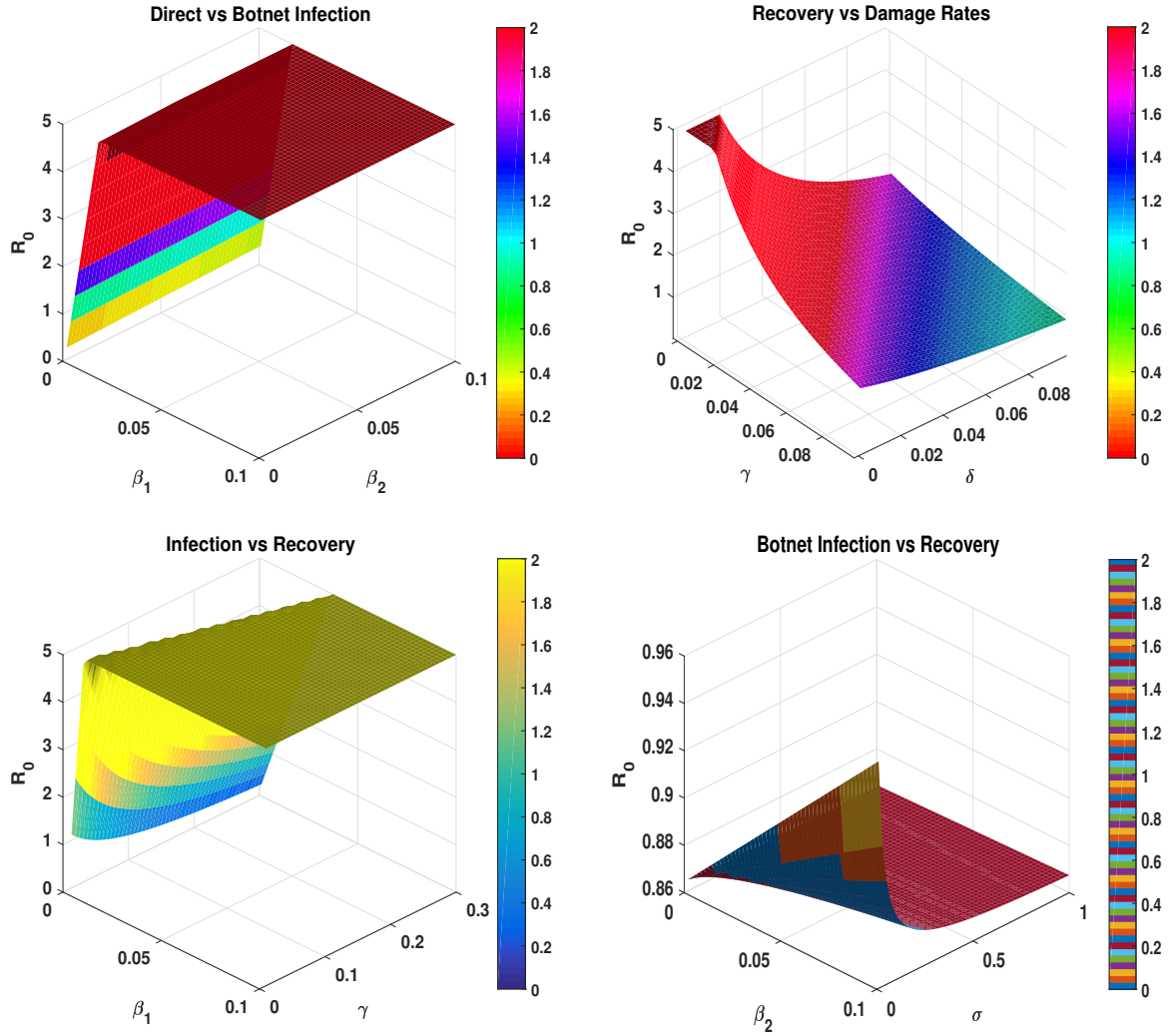

Figure 4: 3D plots of different parameters vs reproduction number. The numerical values used are $\Lambda = 0.98; \mu = 0.02, \beta_1 = 0.003, \beta_2 = 0.2, \gamma = 0.1, \delta = 0.05, \sigma = 0.001, \rho = 0.000095$.

8. Stability Analysis

8.1. Local Asymptotic Stability of the Virus-Free Equilibrium in a Cyberattack Propagation Model

Theorem 2. *The Virus-Free Equilibrium (VFE) of the cyberattack propagation model, given by*

$$E_0 = (S^*, 0, 0, 0, R^*, P^*, 0, A^*), \tag{7}$$

where $S^* = \frac{\Lambda}{\mu}$, $R^* = 0$, $P^* = 0$, *and* $A^* = 0$, *is locally asymptotically stable if the basic reproduction number* $R_0 < 1$ *and unstable if* $R_0 > 1$.

Proof. To analyze the local stability of E_0, we compute the Jacobian matrix J of the system at E_0. The Jacobian is given by:

$$J(E_0) = \begin{bmatrix} -\mu & 0 & -\beta_1 S^* & -\beta_2 S^* & \omega & 0 & 0 & 0 \\ 0 & -(\alpha+\mu) & \beta_1 S^* & \beta_2 S^* & 0 & 0 & 0 & 0 \\ 0 & \alpha & -(\gamma+\delta+\mu) & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \rho & -(\sigma+\mu) & 0 & 0 & 0 & 0 \\ 0 & 0 & \gamma & 0 & -(\omega+\mu) & 0 & 0 & 0 \\ 0 & 0 & 0 & \sigma & 0 & -\mu & \eta & 0 \\ 0 & 0 & \delta & 0 & 0 & 0 & -\eta & 0 \\ 0 & 0 & \kappa & 0 & 0 & 0 & 0 & -\lambda \end{bmatrix}. \quad (8)$$

The stability of E_0 depends on the eigenvalues of $J(E_0)$, determined by solving:

$$\det(J(E_0) - \lambda I) = 0. \quad (9)$$

From the structure of $J(E_0)$, it is evident that the eigenvalues corresponding to the non-infected compartments (S, R, P, A) are negative due to the natural removal rates $(\mu, \omega, \lambda, \eta)$. The crucial stability condition is derived from the infected compartments (E, I, C, D). Using the next-generation matrix method, the dominant eigenvalue satisfies:

$$\lambda_{\max} = (\alpha+\mu)(R_0 - 1). \quad (10)$$

If $R_0 < 1$, then $\lambda_{\max} < 0$, ensuring all eigenvalues have negative real parts, leading to local asymptotic stability of E_0. If $R_0 > 1$, then $\lambda_{\max} > 0$, indicating instability of E_0. Thus, the Virus-Free Equilibrium is locally asymptotically stable if $R_0 < 1$ and unstable if $R_0 > 1$.

Remark 1. *This result highlights that a virus-free equilibrium state in a computer network is achievable only if the basic reproduction number R_0 remains below unity. If $R_0 > 1$, malware persists in the network, necessitating proactive cybersecurity measures such as network segmentation, real-time threat detection, and rapid patch deployment to mitigate the attack spread.*

9. Global Stability of the virus-free equilibrium

Theorem 3. *Suppose that the basic reproduction number $R_0 < 1$. Then the virus-free equilibrium*

$$E_0 = (S^*, E^*, I^*, C^*, R^*, P^*, D^*, A^*) = \left(\frac{\Lambda}{\mu}, 0, 0, 0, 0, 0, 0, 0\right)$$

of the system is globally asymptotically stable in the feasible region $\mathbb{R}^8_+$.

Proof. We define the following Lyapunov function:

$$V = \frac{1}{2} \sum_{X \in \{S,E,I,C,R,P,D,A\}} (X - X^*)^2 \tag{11}$$

This function is positive definite and radially unbounded with respect to the equilibrium point E_0.

Differentiating V along the trajectories of the system:

$$\frac{dV}{dt} = (S - S^*)\frac{dS}{dt} + (E - E^*)\frac{dE}{dt} + \ldots + (A - A^*)\frac{dA}{dt}.$$

Substituting the system equations and using the fact that at the virus-free equilibrium all variables except $S^* = \Lambda/\mu$ vanish, we obtain:

$$\begin{aligned}\frac{dV}{dt} &= (S - S^*)\left[\Lambda - \mu S - \beta_1 SI - \beta_2 SC + \omega R\right] \\ &\quad + E\left[\beta_1 SI + \beta_2 SC - (\alpha + \mu)E\right] + I\left[\alpha E - (\gamma + \delta + \mu)I + \theta C\right] \\ &\quad + C\left[\rho I - (\sigma + \mu)C\right] + R\left[\gamma I - (\omega + \mu)R\right] \\ &\quad + P\left[\sigma C + \eta D - \mu P\right] + D\left[\delta I - \eta D\right] + A\left[\kappa I - \lambda A\right].\end{aligned}$$

All linear and bilinear terms in E, I, C, R, P, D, A are negative definite under the condition $R_0 < 1$, while the term for S remains bounded due to S tends to $S^* = \frac{\Lambda}{\mu}$. Thus:

$$\frac{dV}{dt} \leq -a_1 E^2 - a_2 I^2 - a_3 C^2 - a_4 R^2 - a_5 P^2 - a_6 D^2 - a_7 A^2,$$

where all $a_i > 0$. Equality holds if and only if all variables are at equilibrium. By LaSalle's Invariance Principle, all trajectories converge to the equilibrium point E_0. Hence, E_0 is globally asymptotically stable.

10. Dynamical Behavior of the Model

Identifying the dynamic behavior patterns of cyberattack enables better prevention methods for computer networks. The proposed model analyzes the network node interactions among different states i.e. infection states, protection states, recovery states and attacker persistence states. The changing network parameters enable assessments of system stability and evaluation of optimal control techniques through analysis of system behavioral responses. We illustrate these interactions through phase-plane diagrams that how they evaluate over time with changing variables. The following graphs explain different aspects of malware propagation by focusing on botnet recruitment, malware incubation, security effectiveness and attacker activities.

Table 2: Effect of actively spreading malware nodes vs. secured and immune to attacks nodes simulation.

Parameters		**Time = 50**		**Time = 100**	
β	δ	Infected (I)	Protected (P)	Infected (I)	Protected (P)
0.1	0.01	125	800	80	900
0.7	0.03	500	450	350	600
0.05	0.05	200	700	100	850

Table 3: Numerical values for Fig. ((5a))

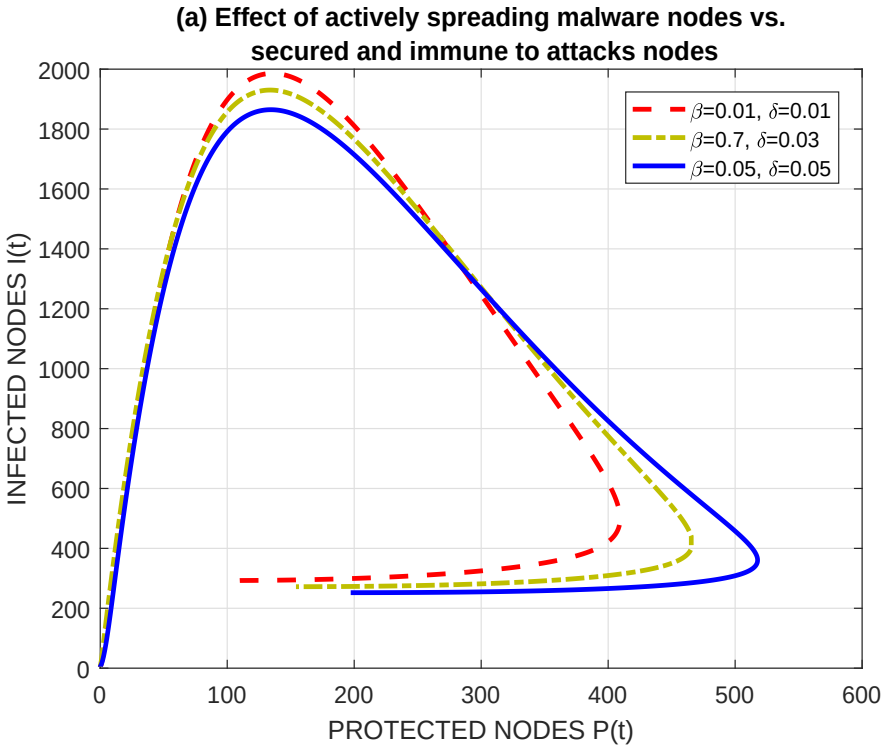

Figure 5: Complex behaviors of malware propagation and security responses

The above graphical presentations shows different complex behaviors of malware propagation and security responses, each showcasing unique dynamics that require careful analysis.

Parameter	**Value**	**State Variable**	**Initial Condition**
Λ	0.700	S (Susceptible Nodes)	5000
μ	0.1	E (Exposed Nodes)	10
β_1	(0.8, 0.8, 0.4, 0.02)	I (Infected Nodes)	10
β_2	(0.8, 0.8, 0.4, 0.02)	C (Controlled Nodes)	0
α	0.1	R (Recovered Nodes)	50
γ	0.02	P (Protected Nodes)	100
δ	(0.6, 0.1, 0.5, 0.23)	D (Disabled Nodes)	10
θ	0.01	A (Attacker Nodes)	710
ρ	0.05		
σ	0.0007		
ω	0.002		
η	0.04		
κ	0.07		
λ	0.06		

Table 4: Parameter values and initial conditions for the cyberattack propagation model.

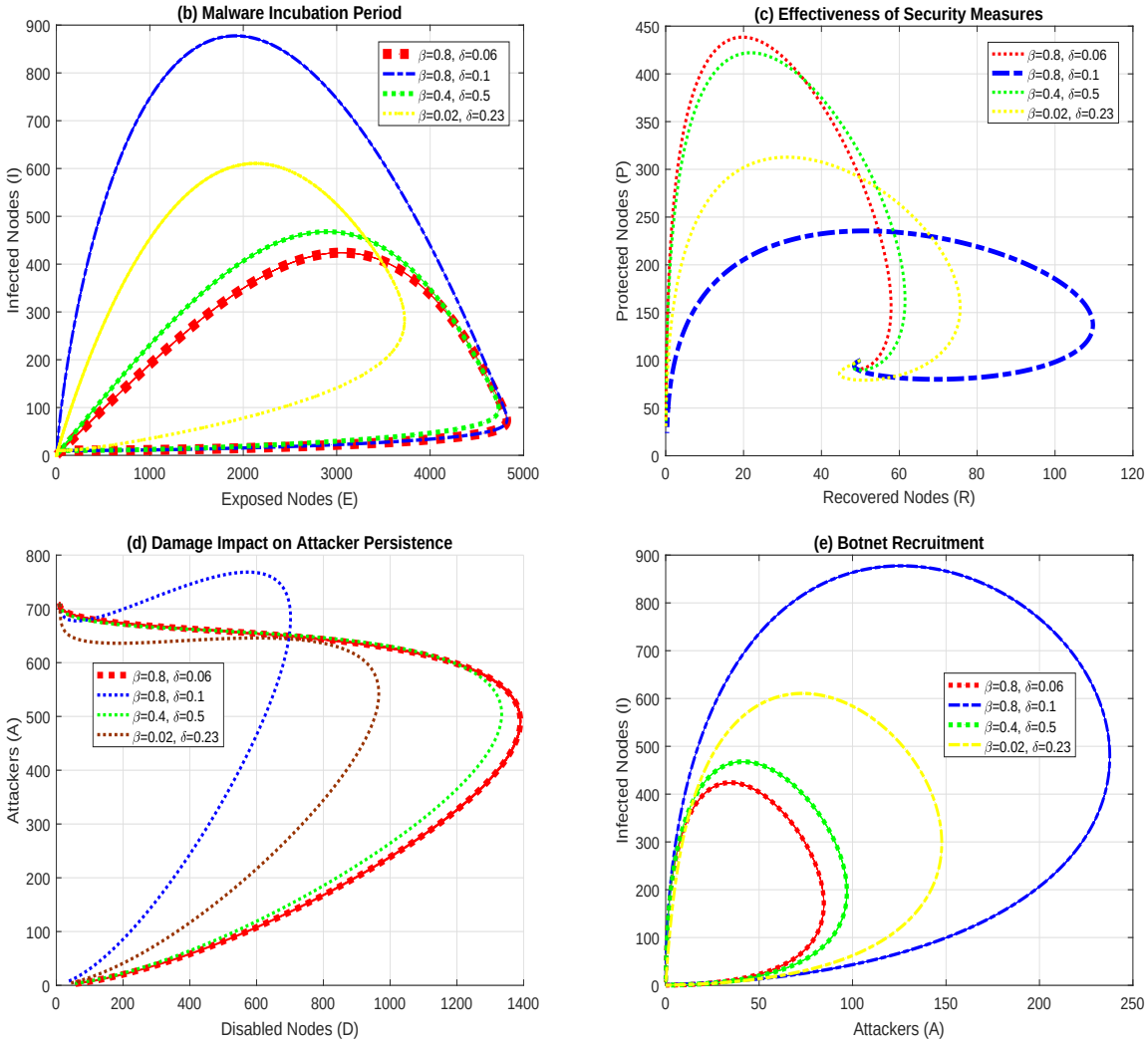

Figure 6: Graphical study of different compartments of the model

In Fig. (6), plot (6a) exhibits a smooth nonlinear progression (using numerical Tab. (3)), where the infection rate initially rises sharply due to the rapid spread of malware in an unprotected environment. However, as security measures gradually take effect, the curve bends downward, indicating a decline in infection. The steep rise and slow decay signify a typical epidemic-like behavior, where an initial surge is followed by a prolonged recovery phase. This transition depends significantly on the transmission rate β and the recovery rate δ, demonstrating the balance between infection pressure and defense mechanisms.

With the help of numerical values which is given in Tab. (4), we presents the following more discussion of the proposed model. In figure (6b) we see interesting behavior, where the solution starts from a zero point, expands outward, and then intriguingly returns to its initial state. This suggests a cyclical nature in the dynamics, where a surge in infections

is followed by an effective containment phase, ultimately leading back to a steady state. Such behavior implies that after an outbreak, the system returns to its original condition, indicating strong resilience. However, the extent of this recovery is highly dependent on external interventions such as security patches and automated malware removal.

The Fig (6c),demonstrate the temporal relationship between protected nodes (P) and recovered nodes (R) across different parametric values. The different curves depict unique scenarios in which infection rate (β) and recovery rate (δ) vary, influencing the overall security effectiveness. Some looping oscillations emerge prominently in the blue dashed trajectory when ($\beta = 0.8, \delta = 0.1$). The system shows transition oscillations which precede its establishment of a stable state. This pattern suggests an adaptive networking response mechanism that could represent periodic reinfection cylcles and delayed security defence measures. While, the red and green curves ($\beta = 0.8, \delta = 0.06$ along $\beta = 0.4, \delta = 0.5$, respectively) exhibit a smoother transition toward higher protection levels because recovery rates maintain system stability with improved control. Further more, the yellow dotted trajectory ($\beta = 0.02, \delta = 0.23$)shows a broader path which indicate more gradual adaptation process where lower infection rates allow security mechanisms to take effect more steadily.

Figure (6d) delves into the relationship between attacker persistence and the number of disabled nodes (D) within the network. At the beginning of the simulation attacker activity (A) stays elevated because adversaries focus on vulnerable points despite the increasing number of disabled nodes that should impede their progress. When the value of D reaches its critical limit then attacker numbers start decreasing rapidly which demonstrates the system's ability to limit malicious behavior. Different trajectories demonstrate varying levels of curvature as another fascinating observation. The blue dashed line ($\beta = 0.8, \delta = 0.1$) represents a trajectory with a bulging shape that increases A before attackers commence their retreat. The observed pattern indicates that high infection levels allow adversaries to stay active longer until their effectiv-
eness finally decreases. A low infection rate ($\beta = 0.02, \delta = 0.23$) causes the reduction of attacker resilience to exhibit a gradual downward trend which supports smooth control of attacker activities.

Figure (6e) demonstrates the progressive relationship between botnet recruitment along with infection growth through which attacker activity surge (A) triggers intense increases in infected nodes (I). Therefore, as countermeasures take effect, the rate of infection slows, causing a progressive contraction of the spread trajectory. When security mechanisms activate they produce self-regulating effects across cyber-ecosystems to limit the extended damage caused by botnet intrusion. The parameter changes produce significant differences in the scale of trajectory outcomes. The blue trajectory ($\beta = 0.8, \delta = 0.1$) produces the widest and largest loop due to its combination of high infection rates and weak recovery mechanisms result in prolonged botnet activity. Conversely, the red and green curves demonstrate tighter loops, where stronger recovery rates prevent large-scale recruitment, reinforcing the importance of early intervention. The presence of nonlinear loops and reversals suggests that botnet activity is not a one-directional process but rather an adaptive cycle influenced by security updates, counter-offensive strategies, and evolving

attacker methodologies. The contraction towards lower values of I in some trajectories emphasizes that persistent defense mechanisms can drive the system toward long-term stabilization, minimizing the threat footprint.

11. Sensitivity Analysis of the Basic Reproduction Number

Sensitivity analysis quantifies the relative impact of model parameters on the basic reproduction number R_0, which determines the potential for the spread of the infection. In this section we study sensitivity analysis which helps to identify the most influential factors affecting the spread of attacks and guides the development of effective mitigation strategies. We employ the normalized sensitivity index, defined as

$$S_x = \frac{x}{R_0}\frac{\partial R_0}{\partial x} \tag{12}$$

where x represents any parameter in R_0. Given the expression for the basic reproduction number:

$$R_0 = \frac{\Lambda\left(\beta_1(\sigma+\mu)+\beta_2\rho\right)}{\mu(\sigma+\mu)(\gamma+\delta+\mu)} \tag{13}$$

we compute the partial derivatives:

$$\begin{aligned}
\frac{\partial R_0}{\partial \Lambda} &= \tfrac{\beta_1(\sigma+\mu)+\beta_2\rho}{\mu(\sigma+\mu)(\gamma+\delta+\mu)},\\
\frac{\partial R_0}{\partial \beta_1} &= \tfrac{\Lambda(\sigma+\mu)}{\mu(\sigma+\mu)(\gamma+\delta+\mu)},\\
\frac{\partial R_0}{\partial \beta_2} &= \tfrac{\Lambda\rho}{\mu(\sigma+\mu)(\gamma+\delta+\mu)},\\
\frac{\partial R_0}{\partial \mu} &= -\tfrac{\Lambda(\beta_1(\sigma+\mu)+\beta_2\rho)}{\mu^2(\sigma+\mu)(\gamma+\delta+\mu)},\\
\frac{\partial R_0}{\partial \sigma} &= \tfrac{\Lambda\beta_1}{\mu(\sigma+\mu)^2(\gamma+\delta+\mu)},\\
\frac{\partial R_0}{\partial \rho} &= \tfrac{\Lambda\beta_2}{\mu(\sigma+\mu)(\gamma+\delta+\mu)},\\
\frac{\partial R_0}{\partial \gamma} &= -\tfrac{\Lambda(\beta_1(\sigma+\mu)+\beta_2\rho)}{\mu(\sigma+\mu)(\gamma+\delta+\mu)^2},\\
\frac{\partial R_0}{\partial \delta} &= -\tfrac{\Lambda(\beta_1(\sigma+\mu)+\beta_2\rho)}{\mu(\sigma+\mu)(\gamma+\delta+\mu)^2}.
\end{aligned}$$

Table 5: Sensitivity values

Parameter	**Sensitivity Index**
S_Λ	1
S_{β_1}	$\frac{\beta_1(\sigma+\mu)}{\beta_1(\sigma+\mu)+\beta_2\rho}$
S_{β_2}	$\frac{\beta_2\rho}{\beta_1(\sigma+\mu)+\beta_2\rho}$
S_μ	-1
S_σ	$\frac{\sigma}{\sigma+\mu}$
S_ρ	$\frac{\rho\beta_2}{\beta_1(\sigma+\mu)+\beta_2\rho}$
S_γ, S_δ	$-\frac{\gamma+\delta}{\gamma+\delta+\mu}$

Parameter	**Sensitivity Index S_x**	**Interpretation**
S_Λ	1.00	R_0 increases proportionally with Λ
S_{β_1}	0.625	10% increase in β_1 increases R_0 by 6.25%
S_{β_2}	0.375	10% increase in β_2 increases R_0 by 3.75%
S_μ	-1.00	10% increase in μ decreases R_0 by 10%
S_σ	0.80	10% increase in σ increases R_0 by 8%
S_ρ	0.375	10% increase in ρ increases R_0 by 3.75%
S_γ, S_δ	0.2	10% increase in γ, δ decreases R_0 by 7.5%

Table 6: Sensitivity indices of model parameters.

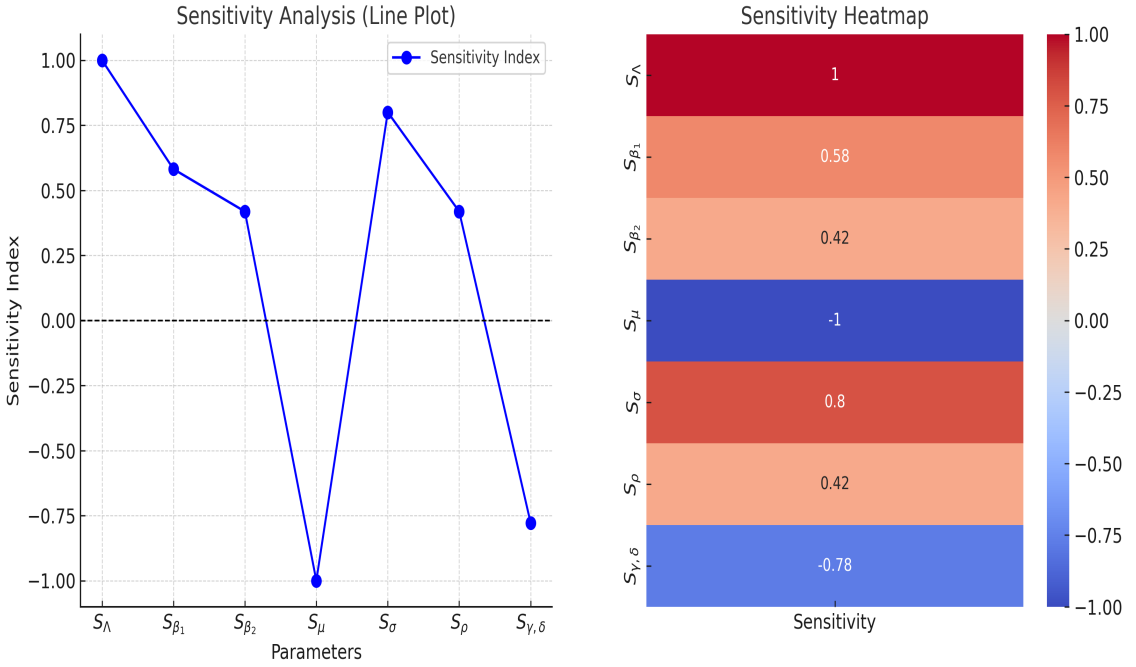

Figure 7: State-Space Trajectory towards Virus-Free Equilibrium

In Fig. 7, the network expansion rate (Λ) exhibits the strongest positive influence ($S_\Lambda = 1$), underscoring that broader network connectivity exacerbates cyberattack propagation. Transmission rates (β_1, β_2) also contribute positively ($S_{\beta_1} = 0.625$, $S_{\beta_2} = 0.375$), highlighting the need to mitigate both direct infections and botnet-driven attacks. Conversely, the node removal rate (μ) shows the most pronounced negative effect ($S_\mu = -1.0$), confirming that decommissioning compromised devices curtails attack persistence. Notably, while the parameter δ (rate of permanent node damage) reduces the infected pool by disabling nodes thereby lowering R_0 ($S_\delta = -0.75$) it represents a trade-off between network attrition and infection control. Similarly, recovery measures (γ) enhance stability ($S_\gamma = -0.75$), emphasizing the value of rapid remediation. The heat-map comparatively visualizes parameter impacts on R_0. Positive sensitivity values ($S > 0$) denote heightened vulnerability with increasing parameter magnitudes, whereas negative values ($S < 0$) reflect stabilizing effects, guiding targeted cybersecurity interventions.

12. Conclusion

This study introduces the general methodology of modeling the dynamics of propagation for cyberattacks in computer networks based on the effects of locally spreading awareness to reduce the risk of widespread infections. The difference between this and all earlier models is the assumption that there is no permanent immunity after infection, that is, the recovered computer becomes susceptible once again. Drawing parallels to the biological virus, we analyze the interactions among key parameters and validate the model

through mathematical inspection of its steady-state behavior. The study touches upon some critical aspects positivity and invariant regions, virus-free equilibrium and endemic equilibrium, the basic reproduction number R_0, and stability conditions for virus-free equilibrium. Further dynamical discussions are induced via exhaustive graphical representations on factors such as influence due to active malware nodes, the incubation period of threats, effectiveness of security measures, and attacker persistence. In addition to other results, this research throws more light on both recruitment in the net and carries out a sensitivity analysis for R_0. This indicates the model can best be used as an effective instrument in the interpretation and control of network-based cyber threats. Simulation results affirm that it accurately captures the outbreak dynamics involved in cyber threats while guaranteeing dependable predictions of threats to come. Therefore, knowledge emanating from this study helps improve strategies towards ameliorating and making the best use of efforts to immunize against cyber threats in complex real-world systems which is bound to apply for optimization strategies.

13. Limitation and Future work

Our model provides a robust framework for analyzing cyberattack dynamics, certain limitations must be acknowledged. First, the assumption of homogeneous mixing among nodes may not fully capture the heterogeneity of real-world networks, such as those with hierarchical or clustered structures. Second, the model does not explicitly account for time-delayed effects in malware detection and patch deployment, which could influence outbreak trajectories. Third, the current simulations focus on deterministic scenarios; incorporating stochastic elements could better reflect the unpredictability of cyber threats. To address these limitations, future research could explore (1) network-specific adaptations, such as scale-free or small-world topologies, (2) time-delay differential equations to model latency in countermeasures, and (3) stochastic formulations to assess risk under uncertainty. Additionally, integrating machine learning techniques for real-time parameter estimation could enhance the model's predictive power in dynamic environments. These extensions would further bridge the gap between theoretical modeling and practical cybersecurity applications.

Acknowledgements

Authors are thankful to Prince Sultan University for paying the Article Processing Charges of this publication.

Authors credits

I.S., writing original draft, discussion of idea, simulations, formal analysis. N.A, formal analysis, supervision. S.A reviewing, editing, project administration.

Data Availability Statement

All the data utilized in this study are included in the manuscript. No additional datasets were created or analyzed.

Competing interest

The authors declare that they have no conflicts of interest relevant to the content of this manuscript.

AI Involvement Declaration

The authors state that no artificial intelligence tools were employed throughout any phase of this study, including its design, analysis, composition, or revision. All aspects of the work were carried out solely by the authors without automated assistance

References

[1] J. Xue, J. Ren, Y. Xu, and L. Wang. A propagation model based on benign worm confrontation and monitoring in peer-to-peer networks. In *IEEE-CISCE*, pages 928–935, 2024.

[2] M. Kharabsheh, I. Al-aiash, A. Mughaid, and M. Almiani. The seir model for predicting malware propagation in computer networks. In *IEEE-ICCNS*, pages 108–113, 2024.

[3] R. W. Thommes and M. J. Coates. Modeling virus propagation in peer-to-peer networks. In *2005 5th International Conference on Information Communications & Signal Processing (ICICS)*, pages 981–985. IEEE, December 2005.

[4] L. Quiroga Sanchez, G. A. Montoya, and C. Lozano Garzon. The seirs nimfa epidemiological model for malware propagation analysis in networks. *Journal of Computer Security*, 8(1):2, 2025.

[5] A. K. Rizi. Spreading and epidemic interventions effects of network structure and dynamics. 2024.

[6] A. Lahrouz, O. Lahcen, K. Driss, and B. Aziza. Complete global stability for an sirs epidemic model with generalized non-linear incidence and vaccination. *Applied Mathematics and Computation*, 218(11):6519–6525, 2012.

[7] W. O. Kermack and A. G. McKendrick. Contributions of mathematical theory to epidemics. *Proceedings of the Royal Society A*, 141(843):94–122, 1933.

[8] I. N. Kiselev, I. R. Akberdin, and F. A. Kolpakov. A delay differential equation approach to model the covid-19 pandemic. *medRxiv*, September 2021.

[9] 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.

[10] M. Draief, A. Ganesh, and L. Massouili. Thresholds for virus spread on networks. *Advances in Applied Probability*, 18(2):359–378, 2008.

[11] B. Zhang, X. Zhao, J. Nie, J. Tang, Y. Chen, Y. Zhang, and D. Niyato. Epidemic model-based network influential node ranking methods: A ranking rationality perspective. *ACM Computing Surveys*, 56(8):1–39, 2024.

[12] S. Kondakci and D. D. Kondakci. Building epidemic models for living populations and computer networks. *SAGE Open*, 104(2):00368504211017800, 2021.

[13] H. Zhang, L. Cao, C. Fu, S. Cai, and Y. Gao. Epidemic spreading on multi-layer networks with active nodes. *Chaos*, 33(7), 2023.

[14] J. O. Kephart, S. R. White, and D. M. Chess. Computers and epidemiology. *IEEE Spectrum*, 30(5):20–26, 1993.

[15] M. Khan, N. Khan, I. Ullah, K. Shah, T. Abdeljawad, and B. Abdalla. A novel fractal fractional mathematical model for hiv/aids transmission stability and sensitivity with numerical analysis. *Scientific Reports*, 15(1):9291, 2025.

[16] R. U. Din, K. A. Khan, A. Aloqaily, N. Mlaiki, and H. Alrabaiah. Using non-standard finite difference scheme to study classical and fractional order seivr model. *Fractal and Fractional*, 7(7):552, 2023.

[17] R. U. Din and E. A. Algehyne. Mathematical analysis of covid-19 by using sir model with convex incidence rate. *Results in Physics*, 23:103970, 2021.

[18] R. U. Din, K. Shah, M. A. Alqudah, T. Abdeljawad, and F. Jarad. Mathematical study of sir epidemic model under convex incidence rate. *AIMS Mathematics*, 5(6):7548–7561, 2020.

[19] R. U. Din and E. A. Algehyne. On global dynamics of covid-19 by using sqir type model under non-linear saturated incidence rate. *Alexandria Engineering Journal*, 2020.

[20] N. Khan, A. Ali, A. Ullah, and Z. A. Khan. Mathematical analysis of neurological disorder under fractional order derivative. *AIMS Mathematics*, pages 18846–18865, 2023.

[21] M. Khan, N. Khan, I. Ullah, et al. A novel fractal fractional mathematical model for hiv/aids transmission stability and sensitivity with numerical analysis. *Scientific Reports*, page 9291, 2025.

[22] I. Shah, H. Alrabaiah, and B. Ozdemir. Using advanced analysis together with fractional order derivative to investigate a smoking tobacco cancer model. *Results in Physics*, page 106700, 2023.

[23] T. Abdeljawad, N. Khan, B. Abdalla, A. Al-Jaser, M. Alqudah, and K. Shah. A mathematical analysis of human papilloma virus (hpv) disease with new perspectives of fractional calculus. *Alexandria Engineering Journal*, pages 575–599, 2025.