Evaluating the Effectiveness of Layered Antivirus Protection through Mathematical Modelling and Sensitivity Analysis

Sunita Agarwal[1], Prasant Kumar Nayak[2], Gholam Mursalin Anasari[3]
[1,3]*School of Computer Science & IT, YBN University, Ranchi, Jharkhand, India*
[2]*Sri Sathya Sai University for Human Excellence, Kalaburagi, Karnataka, India*

***Abstract*—The rapid evolution of computer viruses poses a persistent threat to network security, demanding effective multi-layer defence strategies. This paper develops and analyses a compartmental mathematical model describing the dynamics of virus propagation in a computer network protected by three hierarchical antivirus layers: server-level, inbuilt, and user-installed systems. The model incorporates recruitment, deactivation, infection transmission, quarantine, and recovery processes to capture realistic network behaviour. Analytical investigation establishes the existence and stability of both disease-free and endemic equilibrium, with threshold dynamics governed by the basic reproduction number R_0. Sensitivity analysis both local (elasticity indices) and global (Latin Hypercube Sampling combined with Partial Rank Correlation Coefficients) is conducted to identify the most influential parameters affecting infection prevalence. Numerical simulations reveal that coordinated multi-layer protection effectively suppresses virus persistence, while deficiencies in server-level or inbuilt antivirus efficiency substantially increase infection peaks. The results demonstrate that enhancing quarantine and recovery rates, alongside robust server-level defence, significantly stabilizes network performance. This study provides a quantitative framework for evaluating and optimizing antivirus deployment strategies in complex computer networks.**

***Index Terms*—Computer virus propagation; Antivirus modelling; multi-layer defence systems; Stability analysis; Sensitivity analysis (elasticity and PRCC); Mathematical epidemiology; Network security dynamics.**

I. INTRODUCTION

The proliferation of computer viruses continues to challenge the security and stability of interconnected systems. Since the pioneering work of Cohen [2], which formally defined computer viruses and analysed their propagation mechanisms, mathematical modelling has emerged as a crucial tool for understanding and mitigating network-based infections. Analogous to biological epidemics, computer virus spread can be effectively studied through compartmental models that describe transitions among susceptible, infected, and recovered nodes [7, 9, and 11]. Such frameworks provide valuable insights into the conditions under which viruses persist or die out within complex communication environments.

Subsequent research extended these ideas to networked systems, addressing factors such as connectivity, resource limitations, and immunization strategies. Draief et al. [3] examined thresholds for virus spread on networks, while Huang and Sun [4] investigated the effects of resource constraints and protection costs on tipping points in infection dynamics. Similarly, Madar et al. [6] analysed immunization policies and their influence on epidemic thresholds in complex topologies. These contributions laid the foundation for modern cyber-epidemic modelling, where the dynamic interplay between infection and protection mechanisms determines the network's overall resilience.

Building on this theoretical basis, recent studies have introduced refined models that account for specific cyber security interventions. Mishra and Jha [7] proposed an SEIQRS framework to capture the transmission of malicious objects, incorporating quarantine and immunity effects. Mishra and Keshri [8] extended this to wireless sensor networks, emphasizing the role of node connectivity and defensive strategies. Moreover, Nayak et al. [11, 12]

and Mohanty et al. [13, 14] have advanced the understanding of antivirus interactions by developing dynamic models of infectious node behaviour and control strategies through isolation and optimal quarantine. These studies highlight that multi-layered protection is essential to prevent widespread infection in real-world computer networks.

Despite these advancements, most existing models consider antivirus protection as a single-layer mechanism, typically applied either at the node or network level. In practice, however, contemporary networks employ multiple protection layers, including server-level antivirus systems, inbuilt operating system defences, and user-installed security software. Understanding how these layers interact and contribute to overall network protection is crucial for optimizing cyber security design and policy.

Problem Statement and Research Objectives

This study aims to address the gap in existing literature by developing and analysing a multi-layer antivirus defence model that integrates the combined effects of server-level, inbuilt, and user-installed antivirus systems. The model examines how viruses bypass layered protection under varying conditions of antivirus efficiency and recovery mechanisms. The main objectives are to: (1) Formulate a dynamic model incorporating recruitment, infection, quarantine, and recovery processes in a multi-layer protected network; (2) Derive and analyse stability conditions for both disease-free and endemic equilibrium; (3) Perform local (elasticity-based) and global (PRCC–LHS-based) sensitivity analyses to identify the most influential parameters; and (4) Validate the model through numerical simulations illustrating the effectiveness of multi-layer antivirus strategies.

By integrating mathematical modelling with sensitivity analysis, the proposed framework provides a quantitative understanding of how layered antivirus systems can minimize infection persistence and enhance network robustness.

II. MODEL FORMULATION AND ASSUMPTIONS

In this section, we formulate a deterministic compartmental model to describe the dynamics of computer virus propagation within a network equipped with three layers of antivirus protection: (i) a server-level antivirus that monitors and filters traffic across the network, (ii) an inbuilt operating system antivirus providing internal protection to each node, and (iii) a user-installed antivirus package offering additional security.

The model divides the total number of computers in the network into five compartments according to their security status.

Let

$$N(t) = S_{b(t)} + S_{u(t)} + I(t) + Q(t) + R(t)$$

Represent the total number of computers in the network at time t, where:

- $S_b(t)$: Number of computers protected by the server and inbuilt antivirus layers,
- $S_u(t)$: Number of computers protected by all three layers (server, inbuilt, and user-installed antivirus),
- $I(t)$: Number of infected computers,
- $Q(t)$: Number of quarantined computers, and
- $R(t)$: Number of recovered (cleaned) computers.

The dynamics of the system are governed by the following assumptions:

1. New computers enter the network at a constant rate Λ, where π_b and π_u denote the proportions joining the S_b and S_u classes, respectively $(\pi_b + \pi_u = 1)$.
2. The server-level and inbuilt antivirus systems may fail to detect certain viruses with probabilities dependent on their efficiencies ε_1 and ε_2 while the user-installed antivirus has efficiency ε_3.
3. The infection rate depends on contact between infected and susceptible computers, governed by the transmission rate β.
4. Infected computers can be quarantined at a rate δ, recover at a rate γ, or be deactivated due to damage or removal at a natural rate μ.
5. Quarantined computers recover at a rate γ_q and return to the recovered class.
6. All compartments experience a natural removal or deactivation rate μ.

2.1. Model Equations

Based on the above assumptions, the model is formulated as the following system of nonlinear ordinary differential equations:

$$\frac{dS_b}{dt} = \Lambda\pi_b - \lambda_b S_b - \mu S_b \quad (1)$$

$$\frac{dS_u}{dt} = \Lambda\pi_u - \lambda_u S_u - \mu S_u \quad (2)$$

$$\frac{dI}{dt} = (\lambda_b S_b + \lambda_u S_u) - (\delta + \gamma + \mu)I \quad (3)$$

$$\frac{dQ}{dt} = \delta I - (\gamma_q + \mu)Q \quad (4)$$

$$\frac{dR}{dt} = \gamma I + \gamma_q Q - \mu R \quad (5)$$

Where the infection forces λ_b and λ_u represent the effective transmission rates for the partially and fully protected systems, respectively, defined as:

$$\lambda_b(t) = \beta(1-\varepsilon_2)(1-\varepsilon_1)\frac{I(t)}{N(t)} \quad (6)$$

$$\lambda_u(t) = \beta(1-\varepsilon_2)(1-\varepsilon_1)(1-\varepsilon_3)\frac{I(t)}{N(t)}. \quad (7)$$

2.2. Model Description

Equations $(1)-(5)$ describe the transition of systems among different protection states. The susceptible computers (S_b and S_u) decrease as they become infected through contact with infected systems. The infected systems (I) increase through new infections and decrease due to recovery, quarantine, or natural deactivation. The quarantined systems (Q) represent temporarily isolated computers that eventually recover (R) or are removed from the network. Recovered systems are assumed to be immune to reinfection for the duration of the study period. The model captures the interplay between infection dynamics and multi-layer antivirus protection, allowing exploration of how variations in antivirus efficiency or quarantine response affect the overall infection level within the network.

III. STABILITY ANALYSIS

Stability analysis provides insight into how the system behaves near equilibrium states and determines conditions under which the computer virus dies out or persists in the network. Two types of equilibrium points are considered: the disease-free equilibrium (DFE), corresponding to a completely secure network, and the endemic equilibrium (EE), representing persistent infection.

3.1. Disease-Free Equilibrium (DFE)

At the disease-free equilibrium, there are no infections or quarantined systems in the network; thus, $I = Q = 0$.

From equations $(1)-(5)$, setting all derivatives to zero, the DFE is given by:

$$E_0 = (S_b^0, S_u^0, I^0, Q^0, R^0) = \left(\frac{\Lambda\pi_b}{\mu}, \frac{\Lambda\pi_u}{\mu}, 0,0,0\right). \quad (8)$$

At this equilibrium, all systems remain in the protected compartments, and no infections occur.

3.2. Basic Reproduction Number (R_0)

The basic reproduction number,R_0, represents the expected number of secondary infections generated by a single infected computer in a fully protected network.

$$R_0 = \beta\frac{[\pi_b(1-\varepsilon_1)(1-\varepsilon_2)+\pi_u(1-\varepsilon_1)(1-\varepsilon_2)(1-\varepsilon_3)]}{\delta+\gamma+\mu} \quad (9)$$

This threshold parameter distinguishes between the elimination and persistence of the computer virus:

- If $R_0 < 1$, infection cannot sustain itself and will eventually die out.
- If $R_0 > 1$, the virus persists, leading to endemic equilibrium.

3.3. Local Stability of the Disease-Free Equilibrium

To examine local stability, the Jacobian matrix $J(E_0)$ of the system (1)–(5) is computed at the DFE. Linearizing of the model at around E_0 yields:

$$J_{E_0} = \begin{bmatrix} -\lambda_b - \mu & 0 & 0 & 0 & 0 \\ 0 & -\lambda_u - \mu & 0 & 0 & 0 \\ \lambda_b & \lambda_u & -(\delta + \gamma + \mu) & 0 & 0 \\ 0 & 0 & \delta & -(\gamma_q + \mu) & 0 \\ 0 & 0 & \gamma & \gamma_q & -\mu \end{bmatrix}$$

Since this is a triangular matrix and main diagonal entries are negative hence all the Eigen values are negative. Hence, the DFE is locally asymptotically stable

IV. SENSITIVITY ANALYSIS

Sensitivity analysis quantifies how uncertainty or changes in model parameters affect key model outputs. In this work we use two complementary approaches: (i) analytic elasticity of the basic reproduction number R_0 (local, dimensionless sensitivities) to provide mechanistic insight and (ii) global sensitivity via Latin Hypercube Sampling (LHS) with Partial Rank Correlation Coefficients (PRCC) (global, model-output based sensitivities) to capture effects across realistic parameter ranges. The two methods together enable robust identification and ranking of high-leverage parameters for control.

4.1 Baseline Parameter Values

All sensitivity computations were performed around a set of baseline parameter values shown in table 1 that represent typical operating conditions of a computer network with multiple antivirus protection layers.

Table 1. Baseline Parameters for Sensitivity Analysis

Parameter	Symbol	Description	Baseline Value
β	Transmission rate	Probability of infection spread per contact	0.99
ε_1	Inbuilt antivirus efficiency	Protection due to built-in system antivirus	0.15
ε_2	Server-level antivirus efficiency	Centralized antivirus protection at server	0.45
ε_3	User-installed antivirus efficiency	Efficiency of user-installed antivirus package	0.70
δ	Quarantine rate	Rate of infected nodes being isolated	0.08
γ	Recovery rate	Rate of recovery or repair of infected nodes	0.02
γ_q	Recovery rate from quarantine	Rate of restoration from quarantined nodes	0.06
μ	Natural deactivation rate	Rate of node loss or removal from network	0.02
Λ	Recruitment rate	Rate of new nodes joining the network	10
π_b	Fraction of server-protected systems	Proportion of computers protected at server level	0.55
π_u	Fraction of user-protected systems	Proportion of computers relying on user-level protection	0.45

4.2 Sensitivity Analysis (Elasticity Approach)

The normalized elasticity coefficients of R_0 were derived analytically as:

$$\Upsilon_{\beta}^{R_0} = 1$$

$$\Upsilon_{\epsilon_2}^{R_0} = -\frac{\epsilon_2}{1-\epsilon_2}$$

$$\Upsilon_{\epsilon_1}^{R_0} = -\frac{\epsilon_1}{1-\epsilon_1}$$

$$\Upsilon_{\epsilon_1}^{R_0} = -\frac{\epsilon_3(1-\epsilon_1)\pi_u}{\pi_b(1-\varepsilon_1)+\pi_u(1-\varepsilon_1)(1-\varepsilon_3)}$$

$$\Upsilon_{\delta}^{R_0} = -\frac{\delta}{\delta+\gamma+\mu}$$

$$\Upsilon_{\gamma}^{R_0} = -\frac{\gamma}{\delta+\gamma+\mu}$$

$$\Upsilon_{\mu}^{R_0} = -\frac{\mu}{\delta+\gamma+\mu}$$

The positive elasticity for β implies a direct proportional increase in R_0 with higher transmission intensity, whereas the negative elasticities for $\varepsilon_i, \delta, \gamma$, and μ show that strengthening antivirus mechanisms, recovery, or removal processes effectively suppress infection spread.

Among all parameters, ε_2 and δ (quarantine rate) exhibit the largest negative elasticities, confirming that these are the most effective control parameters to reduce virus persistence in the network.

4.3 Global Sensitivity (LHS–PRCC) Results

To verify and complement the local analysis, a global sensitivity scan was performed using 500 Latin Hypercube samples across realistic parameter ranges. The correlation between each parameter and the simulated infection peak was quantified using PRCC values which is shown in figure 3 and combined sensitivity result shown in table 2.

Table 2. Combined Elastic and Global Sensitivity Results

Parameter	Elasticity (Analytic)	PRCC (Global)	Influence Direction	Technical Meaning
β (Transmission rate)	+1.000	+0.222	Positive	Faster virus transmission increases infection prevalence.
ε_2 (Server antivirus efficiency)	−0.818	−0.349	Negative	Strongly reduces infection peaks; most effective antivirus layer.
δ (Quarantine rate)	−0.667	−0.355	Negative	Rapid isolation of infected nodes lowers outbreak magnitude.
γ (Recovery rate)	−0.444	−0.172	Negative	Increases recovery speed; moderate contribution.
ε_1 (Inbuilt antivirus)	−0.176	−0.110	Negative	Provides local protection; secondary importance.
ε_3 (User-installed antivirus)	−0.122	−0.077	Negative	Weak individual effect; complements other layers.
μ (Natural deactivation)	−0.111	+0.002	Neutral/ weak	Minimal influence on short-term infection dynamics.

4.4 Discussion

Both analyses consistently demonstrate that server-level antivirus efficiency (ε_2) and quarantine rate (δ) are the most critical parameters in suppressing virus propagation across the network. Their strong negative elasticities and PRCC values highlight that improving centralized antivirus functionality and rapid detection isolation protocols dramatically reduce infection peaks.

The transmission rate (β) remains the key risk factor; however, its effect can be mitigated by enhancing ε_2 and δ. The local elasticity and global PRCC results agree in ranking importance as:

Server antivirus (ε_2)>Quarantine rate (δ)>Transmission rate (β)>Recovery rate (γ)>Inbuilt (ε_1)>User installed(ε_3).

This combined analysis indicates that the server-managed antivirus system, coupled with a high quarantine response rate, forms the most effective defence architecture. Enhancements at these levels yield the greatest reduction in R_0 and infection peaks, validating the central hypothesis of this study that multi-layer antivirus coordination, dominated by strong server-level protection, ensures long-term cyber-epidemic stability in computer networks.

V. NUMERICAL SIMULATION OF THE MODEL

To investigate the dynamic behaviour of the proposed multi-layer antivirus model, numerical simulations were carried out using the Runge–Kutta method by using python. The system of nonlinear differential equations representing five compartments protected with server and inbuilt antivirus(S_b), fully protected nodes(S_u), infected nodes (I), quarantined nodes (Q), and recovered nodes(R).

The baseline parameter values used for this simulation are listed in Table 2, corresponding to the fully

protected configuration where all antivirus layers (server, inbuilt, and user-installed) are active.

Initial conditions were taken as $S_b(0) = 500, S_u(0) = 300, I(0) = 50, Q(0) = 20, R(0) = 10$

The numerical results (Figure 1) illustrate the temporal evolution of all five compartments under complete multi-layer antivirus protection. The infected population (I) exhibits an initial rise followed by a rapid decline toward zero, while quarantined nodes (Q) show a small transient peak before vanishing. The recovered nodes (R) increase monotonically and reach a steady value, indicating effective system recovery. Meanwhile, both protected compartments (S_b and S_u) stabilize at equilibrium, signifying that network protection levels remain steady under continuous recruitment and natural deactivation.

These outcomes verify the theoretical stability results, confirming that the system approaches a disease-free equilibrium (DFE) when all antivirus layers operate efficiently and that $R_0 < 1$ under the baseline configuration. Thus, the numerical simulations reinforce that the combined action of server-level, inbuilt, and user-installed antivirus mechanisms provides the most effective defence against network-wide virus propagation.

Infection dynamics under different antivirus protection configurations shown in figure 2

- The red curve (Scenario 1) represents the uncontrolled spread of infection in the absence of antivirus defence, showing a rapid rise in infected nodes.
- The orange curve (Scenario 2) demonstrates partial suppression when only the inbuilt antivirus is active, resulting in a lower but still persistent infection peak.
- The green curve (Scenario 3) shows the combined effect of server-level, inbuilt, and user-installed antivirus systems, where infection levels quickly decline and the network stabilizes to a virus-free equilibrium.

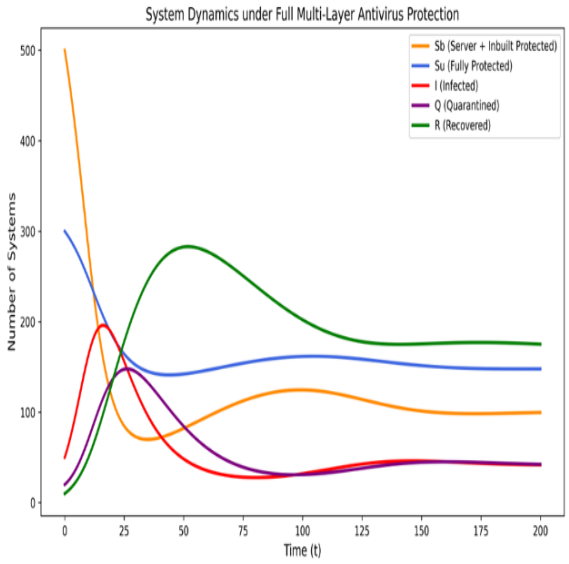

Figure:1 Temporal evolution of system compartments under complete multi-layer antivirus protection. The infected (I) and quarantined (Q) nodes decline over time, while recovered (R) nodes increase and the protected classes (S_b, S_u) stabilize, indicating long-term network stability.

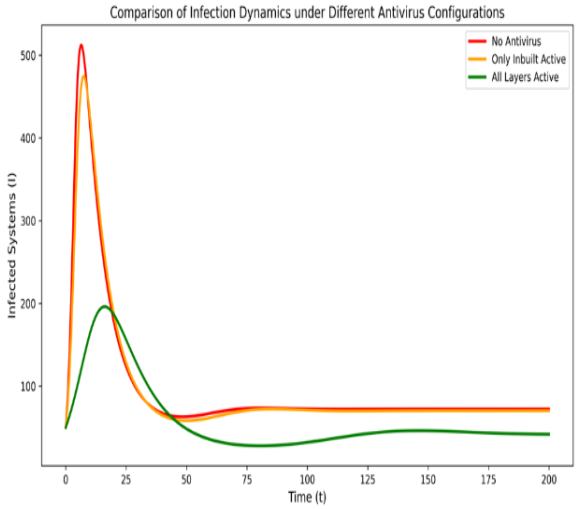

Figure 2: Temporal evolution of infected nodes under different antivirus protection scenarios.

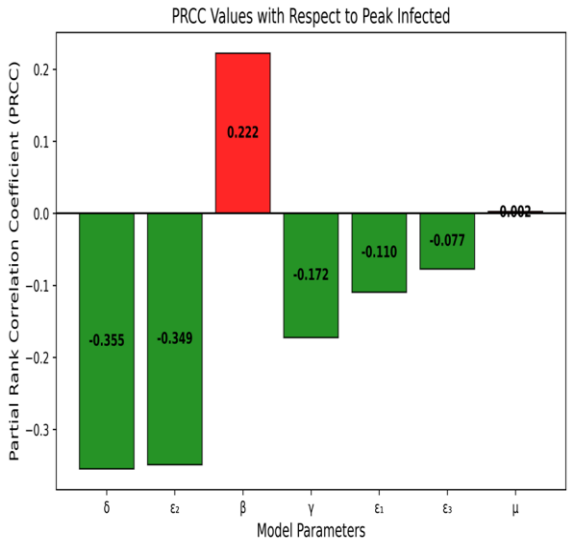

Figure 3: Global sensitivity of model parameters with respect to the infection peak using Partial Rank Correlation Coefficients (PRCCs)

REFERENCES

[1] H.W. Berhe, O.D. Makinde, D.M. Theuri, Parameter estimation and sensitivity analysis of dysentery diarrhea epidemic model, J. Appl. Math. 2019 (2019), 1–13.

[2] F. Cohen, Computer viruses, Comput. Secur. 6 (1) (1987) 22–35.

[3] M. Draief, A. Ganesh, L. Massoulié, Thresholds for virus spread on networks, Ann. Appl. Probab. 18 (2) (2008) 359–378.

[4] C. Huang, C. Sun, Effects of resource limitations and cost influences on computer virus epidemic dynamics and tipping points, Discrete Dyn. Nat. Soc. 2012 (2012), 1–15.

[5] S. Kondakci, D.D. Kondakci, Building epidemic models for living populations and computer networks, Science Progress 104 (2) (2021).

[6] N. Madar et al., Immunization and epidemic dynamics in complex networks, Eur. Phys. J. B 38 (2) (2004) 269–276.

[7] B.K. Mishra, N. Jha, SEIQRS model for the transmission of malicious objects in computer network, Appl. Math. Modell. 34 (3) (2010) 710–715.

[8] B.K. Mishra, N. Keshri, Mathematical model on the transmission of worms in wireless sensor network, Appl. Math. Modell. 37 (6) (2013) 4103–4111.

[9] M.E. Newman, S. Forrest, J. Balthrop, Email networks and the spread of computer viruses, Phys. Rev. E 66 (3) (2002).

[10] H. Yuan, G. Chen, Network virus-epidemic model with the point-to-group information propagation, Appl. Math. Comput. 206 (1) (2008) 357–367.

[11] P.K. Nayak, D. Mishra, S. Ram, Dynamic e-epidemic model for active infectious nodes in computer network, J. Stat. Manag. Syst. 19 (2) (2016) 247–257.

[12] S. Ram, P.K. Nayak, D. Mishra, Mathematical modelling, analysis involving behaviour of infectious nodes in a computer network, IEEE ICREISG (2020) 1–6.

[13] S. Mohanty, P.K. Nayak, S. Mohanty, Optimal control of malicious codes in a computer network by quarantine and isolation strategy, Lecture Notes in Electrical Engineering (2024) 333–344.

[14] S. Mohanty, P.K. Nayak, A.K. Paul, A. Basantia, Mathematical modeling for understanding computer virus behavior in a network and its stability analysis, IEEE OCIT (2023).