Iranian Journal of Numerical Analysis and Optimization
Vol. 16, No. 4, 2026, pp 1484–1517
https://doi.org/10.22067/ijnao.2026.97856.1846
https://ijnao.um.ac.ir/

Research Article

A multi-layer SEIRS-V network epidemic model for IoT malware propagation with heterogeneous device types and patch dynamics

A. Tajari Siahmarzkooh*

Abstract

The Internet of Things (IoT) ecosystem comprises billions of heterogeneous devices that have diverse hardware architectures, operating systems, vulnerability profiles, and patch management capabilities, creating a complex and dynamic attack surface for malware propagation. This paper develops a comprehensive multi-layer network epidemic model for characterizing malware spread in heterogeneous IoT networks. The proposed framework integrates three key dimensions: (1) a susceptible-exposed-infected-recovered-susceptible with vaccination compartmental structure capturing device-level infection states and patching status; (2) a multi-layer network topology distinguishing between physical proximity, logical connectivity, and protocol-based communication graphs, and (3) device-type heterogeneity with class-specific parameters for vulnerability, infectiousness, and recovery rates. The hybrid formulation yields a system of coupled differential equations that admits analytical expressions for the basic reproduction number $\mathcal{R}_0$, type-specific epidemic thresholds, and equilibrium prevalence. Numerical simulations calibrated with empirical IoT device data from Shodan and Censys demonstrate that physical proximity layers increase early-stage propagation speed by 28%–43% compared to logical connectivity alone, while device-type heterogeneity reduces the critical epidemic threshold by 31%–47% relative to homogeneous assumptions. The model provides security analysts

*Corresponding author

Received 14 February 2026; revised 11 May 2026; accepted 3 July 2026

Aliakbar Tajari Siahmarzkooh
Department of Computer Science, Golestan University, Gorgan, Iran e-mail: a.tajari@gu.ac.ir

How to cite this article
Tajari Siahmarzkooh, A., A multi-layer SEIRS-V network epidemic model for IoT malware propagation with heterogeneous device types and patch dynamics. *Iran. J. Numer. Anal. Optim.*, 2026; 16(4): 1484-1517. https://doi.org/10.22067/ijnao.2026.97856.1846

with quantitative tools for identifying critical infection pathways, prioritizing device classes for patching, and evaluating network segmentation strategies.

AMS subject classifications (2020): Primary 92D30; Secondary 68M25, 05C82, 91A80

Keywords: IoT security, multi-layer networks, epidemic modeling, heterogeneous devices, patch management, malware propagation

1 Introduction

The Internet of Things (IoT) has fundamentally transformed the technological landscape, with connected device installations projected to exceed 30 billion by 2025, spanning consumer electronics, industrial control systems, healthcare devices, and critical infrastructure [7]. This proliferation has created an unprecedented attack surface for malware propagation. Unlike traditional computing environments with relatively homogeneous operating systems and centralized patch management, IoT ecosystems exhibit extreme heterogeneity across multiple dimensions: Hardware architectures (ARM, x86, RISC-V), operating system families, and patch management practices.

Recent high-profile IoT malware campaigns, including Mirai, Hajime, and Mozi, have demonstrated the catastrophic potential of large-scale IoT compromise, with infected devices forming botnets capable of launching multi-terabit distributed denial-of-service attacks [1]. These outbreaks reveal fundamental limitations of existing propagation models. Traditional epidemiological approaches, adapted from biological infectious disease modeling, typically assume homogeneous mixing and uniform population characteristics that fundamentally misrepresent IoT realities [19].

First, IoT networks exhibit multi-layer topological structures that classical epidemic models fail to capture. Devices communicate through multiple channels: Physical proximity enables Bluetooth and ZigBee transmission, while logical connectivity facilitates IP-based communication, and protocol-specific networks create distinct infection pathways [17]. Malware can propagate simultaneously across these layers, with different transmission rates and probability distributions. Understanding inter-layer propagation dynamics is essential for accurate outbreak prediction and containment.

Second, device-type heterogeneity fundamentally alters epidemic dynamics. A compromised smart camera may have different infectiousness, vulnerability, and recovery characteristics than an industrial controller or a healthcare monitor. Vulnerability databases reveal systematic vari-

ation in patch availability and deployment timelines across device classes [18]. Consumer devices require an average of 45–60 days for patch deployment, whereas industrial devices may remain unpatched for over 200 days due to certification requirements and operational continuity constraints [6]. This heterogeneity creates class-specific sub-epidemics with complex interactions.

Third, the vaccination analogy—patching—exhibits distinct temporal dynamics in IoT contexts. Unlike biological immunity, patching is a strategic decision influenced by device type, operational criticality, and cost-benefit calculations. Device owners decide whether and when to apply patches based on perceived risk, disruption costs, and available resources [2]. This behavioral dimension requires the integration of game-theoretic elements into epidemic frameworks.

Novelty and Contribution: The primary contribution of this manuscript is not the invention of new mathematical compartments, but rather the *integration* of three existing modeling dimensions—(i) multi-layer network topology (physical, logical, protocol), (ii) device-type heterogeneity, and (iii) strategic (prevalence-dependent) patching dynamics—into a single, unified, and analytically tractable framework. While each of these components has been studied separately in prior work (e.g., susceptible-exposed-infected-recovered-susceptible with vaccination (SEIRS-V) models in wireless sensor networks by Mishra & Tyagi, 2014; multi-type SEIR for IoT by Yan et al., 2021; temporal multi-layer models by Cao et al., 2025), the specific combination of all three components, along with empirical calibration using IoT-specific datasets (Shodan, Censys, NVD) and validation against real-world campaigns (Mirai, Hajime), represents the novel contribution of this paper. This integration allows, for the first time, a quantitative analysis of how inter-layer propagation pathways and slow-patching industrial devices jointly sustain endemic malware in IoT ecosystems.

This paper addresses these gaps through a comprehensive multi-layer network epidemic model specifically designed for heterogeneous IoT environments. Our approach integrates three methodological innovations:

1. **Multi-Layer Network Topology:** We model IoT communication infrastructure as a multi-layer graph with distinct layers for physical proximity, logical connectivity, and protocol-specific networks. Malware transmission occurs within and potentially across layers with layer-specific transmission rates and probabilities.

2. **Device-Type Heterogeneity:** We classify IoT devices into K distinct types based on hardware architecture, operating system, and vulnerability profile. Each type exhibits class-specific parameters for susceptibility, latency, infectiousness, and recovery, enabling realistic characterization of heterogeneous populations.

3. **SEIRS-V Compartmental Structure with Strategic Patching:** We extend classical compartmental models to include a vaccinated (patched) state with waning immunity, and incorporate game-theoretic patch adoption where device types strategically choose patching timing based on infection prevalence and cost parameters.

The remainder of this paper is organized as follows. Section 2 reviews related work. Section 3 presents the mathematical formulation. Section 4 derives epidemic thresholds and equilibrium conditions. Section 5 describes numerical simulations and validation. Section 6 discusses practical implications. Section 7 concludes.

2 Literature review

2.1 Classical epidemic models for malware propagation

The application of epidemiological models to computer malware has a rich history dating back to the 1990s. Kephart and White pioneered the use of SIR (Susceptible-Infected-Recovered) models for computer virus propagation [12]. The classical deterministic formulation describes population dynamics through ordinary differential equations (ODEs):

$$\frac{dS}{dt} = -\beta SI, \qquad \frac{dI}{dt} = \beta SI - \gamma I, \qquad \frac{dR}{dt} = \gamma I, \tag{1}$$

where β denotes the infection rate and γ the recovery rate. This model yields the fundamental epidemic threshold $\mathcal{R}_0 = \beta S_0/\gamma$, determining outbreak persistence.

Extensions have incorporated additional compartmental structure relevant to malware. The SEIR model adds an exposed (E) compartment for latent infections, capturing the delay between initial compromise and active propagation [27]. The SIS model, where recovered individuals return to susceptibility, models malware without immunity or incomplete patching [28]. The SIRS model incorporates temporary immunity followed by waning protection, representing devices that become vulnerable after patches expire or are reversed [4].

While these models provide valuable foundations, they rest on assumptions that are fundamentally inconsistent with IoT realities. Homogeneous mixing assumes any infected node can infect any susceptible node with equal probability, ignoring the structured communication patterns characteristic of IoT deployments [19]. Uniform parameters across all nodes fail to capture device-type heterogeneity in vulnerability, infectiousness, and recovery.

2.2 Network epidemic models

Network epidemiology addresses homogeneous mixing limitations by modeling propagation on explicit graph topologies. In network epidemic models, nodes represent devices and edges represent communication pathways through which infection transmits [17]. The infection probability for a susceptible node depends on the infection status of its neighbors.

For a network with an adjacency matrix A, the SIS dynamics on graphs are given as follows:

$$\frac{dp_i}{dt} = \beta \sum_j A_{ij} p_j - \gamma p_i, \tag{2}$$

where p_i is the infection probability of node i. Linearization around the disease-free equilibrium yields the epidemic threshold condition $\mathcal{R}_0 = \beta\rho(A)/\gamma$, where $\rho(A)$ is the spectral radius of the adjacency matrix [20].

Network models have been successfully applied to email worms and topology-aware viruses [23]. However, standard network epidemic models assume a single network layer, whereas IoT devices communicate through multiple distinct channels simultaneously [25].

2.3 Multi-layer network epidemic models

Multi-layer networks represent systems in which nodes interact through multiple distinct types of connections. Formally, a multi-layer network comprises L layers, each with adjacency matrix $A^{(\ell)}$ for $\ell = 1, \ldots, L$. Nodes may have different neighbors in different layers, and infection can potentially transmit both within and across layers [3].

Recent theoretical advances have extended epidemic modeling to multi-layer contexts. The multi-layer SIS model with uncorrelated layers exhibits a threshold condition:

$$\mathcal{R}_0 = \frac{\beta}{\gamma} \rho \left(\sum_{\ell=1}^{L} A^{(\ell)} \right), \tag{3}$$

provided that transmission rates are uniform across layers [26]. For correlated layers, the spectral radius of the aggregated network may be significantly larger than individual layer contributions, amplifying outbreak potential.

Applications of multi-layer epidemic models remain limited in cybersecurity contexts. Liu et al. [16] proposed a two-layer model for malware propagation in mobile networks considering Bluetooth and WiFi transmission channels. However, comprehensive multi-layer formulations

that incorporate device-type heterogeneity and strategic patching for IoT environments remain unexplored.

2.4 Heterogeneous population models

Heterogeneity in host populations has been extensively studied in mathematical epidemiology. Multi-group models partition the population into groups with distinct epidemiological parameters [13]. For K groups, the next-generation matrix approach yields

$$\mathcal{R}_0 = \rho(M), \tag{4}$$

where M is the matrix with entries $M_{ij} = \beta_{ij} S_i^0 / \gamma_j$, capturing transmission from group j to group i.

In cybersecurity contexts, heterogeneous device types have received increasing attention. Li et al. [14] developed a multi-group model for malware propagation in wireless sensor networks, incorporating class-specific infection and recovery rates. Their analysis demonstrated that heterogeneity significantly affects epidemic thresholds and equilibrium prevalence. However, their model assumes homogeneous mixing within and between groups, neglecting network topology.

Recent studies have explored stochastic simulation approaches for IoT malware spread using individual-based SIR models with topological overlap measures, providing empirical validation resources for heterogeneous network models [22].

2.5 Patch management and strategic behavior

The economics of patching and security investments have been extensively analyzed using game theory. August and Tunca [2] modeled firm-level patch adoption decisions as a trade-off between security risk and operational disruption costs. Chopra and Singh [6] have documented substantial variation in patch deployment timelines across IoT device types, with consumer devices patching faster than industrial devices due to certification requirements.

Integrating strategic patching behavior into epidemic models represents an emerging research direction. Chen and Wang [5] proposed a model where recovery rates depend on infection prevalence through a rational response function, but did not consider device-type heterogeneity or network structure.

2.6 Research gap and positioning

Our literature review identifies four critical gaps that this paper addresses:

1. **Multi-Layer IoT Networks:** Existing models fail to capture the multi-layer communication structure of IoT environments, where devices interact through physical proximity, logical connectivity, and protocol-specific networks simultaneously.

2. **Device-Type Heterogeneity with Network Structure:** While multi-group models capture population heterogeneity, they assume homogeneous mixing within and between groups, neglecting the network topology that fundamentally shapes propagation dynamics.

3. **Strategic Patching with Heterogeneity:** Current models treat recovery as an exogenous constant rather than a strategic decision that varies systematically across device types based on cost-benefit calculations.

4. **Empirical IoT Calibration:** Existing models are predominantly calibrated for PC and server environments, lacking IoT-specific parameterization based on real device census data and vulnerability measurements.

Table 1 summarizes the comparative positioning of our multi-layer heterogeneous framework relative to existing modeling approaches.

Table 1: Comparison of malware propagation modeling approaches

Model Feature	Classical Epidemic	Single-Layer Network	Multi-Group	**Our Multi-Layer**
Network topology	No	Single layer	No	**Multiple layers**
Device-type heterogeneity	No	No	Yes	**Yes**
Strategic patching	No	No	Limited	**Yes**
Multi-layer transmission	No	No	No	**Yes**
Empirical IoT calibration	No	Limited	No	**Yes**
Layer-specific thresholds	No	No	No	**Yes**

The proposed multi-layer heterogeneous epidemic framework occupies a unique position, integrating the topological realism of multi-layer networks, the population realism of heterogeneous device types, and the behavioral realism of strategic patch adoption, while incorporating IoT-specific empirical parameters.

3 Mathematical model formulation

This section presents the multi-layer heterogeneous epidemic model for malware propagation in IoT networks. We develop the model in three integrated components: (1) multi-layer network topology, (2) device-type classification and compartmental structure, and (3) strategic patch adoption dynamics.

3.1 Summary of key symbols

Table 2 provides a summary of the key mathematical symbols used throughout this paper.

Table 2: Summary of key mathematical symbols

Symbol	Description	Typical Value
N	Total number of IoT devices	$10^5 - 10^7$
K	Number of device types	5
L	Number of network layers	3
S_k, E_k, I_k, R_k, V_k	Fraction of type-k devices in each state	varies
$\beta^{(\ell)}(t)$	Time-varying transmission rate for layer ℓ	0.08-0.25 day^{-1}
σ_k	Activation rate (latent period inverse) for type k	0.3-0.7 day^{-1}
$\rho_k(t)$	Time-varying patching rate for type k	0.0056-0.022 day^{-1}
ω_k	Immunity waning rate for type k	0.002 day^{-1}
ξ_k	Vaccine waning rate	0.001 day^{-1}
$\nu_k(t)$	Proactive vaccination rate	varies
$\tau_{kk'}$	Transmission compatibility factor from type k' to k	0.3-1.0
$\langle a_{kk'}^{(\ell)} \rangle$	Average number of layer-ℓ edges between types k and k'	varies
$\mathcal{R}_0$	Basic reproduction number	varies
θ_k	Patching threshold for type k $(= c_D^k/c_I^k)$	0.05-0.25

3.2 Multi-layer network topology

Consider an IoT network comprising N devices indexed by $i = 1, \ldots, N$. Devices interact through L distinct communication layers, representing different transmission modalities:

- **Layer 1 (Physical Proximity):** Short-range wireless communication (Bluetooth, ZigBee, NFC) requiring devices to be within physical range. The adjacency matrix $A^{(1)}$ has entries $a_{ij}^{(1)} = 1$ if devices i and j are within transmission range.

- **Layer 2 (Logical Connectivity):** IP-based communication over WiFi or Ethernet. $A^{(2)}$ represents the logical network topology based on routing and connectivity.

- **Layer 3 (Protocol-Specific Networks):** Specialized communication protocols (LoRaWAN, Modbus, CAN bus) for specific applications. Additional layers can represent distinct protocol domains.

Each layer ℓ has an associated transmission rate $\beta^{(\ell)}(t)$ that may vary over time, particularly increasing after exploit disclosure. The inter-layer coupling is captured through the multi-layer adjacency structure; a single device participates in multiple layers simultaneously.

Define the multi-layer network as $\mathcal{G} = \{G^{(1)}, \ldots, G^{(L)}\}$ with adjacency matrices $A^{(\ell)}$. For analytical tractability, we assume that layers are independent conditional on device membership.

Limitation acknowledgment: It is important to note that in realistic IoT deployments, physical proximity and logical connectivity may be correlated (e.g., co-located devices often share the same IP subnet). The following analysis therefore provides a baseline under conditional independence, while the potential impact of inter-layer correlations is discussed in Section 6.3.

3.3 Device-type classification and compartmental structure

IoT devices exhibit substantial heterogeneity in hardware, software, and security characteristics. We classify devices into K distinct types indexed by $k = 1, \ldots, K$, based on

- Hardware architecture (ARM, x86, MIPS, RISC-V)

- Operating system/firmware family

- Vulnerability profile (common vulnerabilities and exposures)

- Typical patch management capability

- Deployment context (consumer, industrial, healthcare)

Let N_k denote the number of devices of type k, with $\sum_{k=1}^{K} N_k = N$. Each device occupies one of five epidemiological states at time t:

- **Susceptible (S):** Device is vulnerable and not yet compromised.

- **Exposed (E):** Device has received a malware payload but is not yet infectious (latent period).

- **Infected (I):** Device is actively compromised and capable of propagating malware.

- **Recovered (R):** Device has been patched or remediated and is temporarily immune.

- **Vaccinated (V):** Device has received proactive security updates before infection, providing immunity.

This SEIRS-V structure captures the full lifecycle of IoT devices under malware threat. The compartmental dynamics for device i of type k are governed by state transition rates:

$$\begin{aligned}
&S_i \xrightarrow{\lambda_i^{(\ell)}(t)} E_i && \text{(Infection via layer } \ell\text{)},\\
&E_i \xrightarrow{\sigma_k} I_i && \text{(Activation)},\\
&I_i \xrightarrow{\rho_k(t)} R_i && \text{(Patching)},\\
&R_i \xrightarrow{\omega_k} S_i && \text{(Immunity waning)},\\
&S_i \xrightarrow{\nu_k(t)} V_i && \text{(Proactive vaccination)},\\
&V_i \xrightarrow{\xi_k} S_i && \text{(Vaccine waning)},
\end{aligned} \tag{5}$$

where $\lambda_i^{(\ell)}(t)$ is the layer-specific force of infection on device i, σ_k is the type-specific activation rate (inverse of mean latent period), $\rho_k(t)$ is the type-specific patching rate, ω_k is the immunity waning rate, $\nu_k(t)$ is the proactive vaccination rate, and ξ_k is the vaccine waning rate.

Value of V state: While the V (vaccinated) compartment is not always occupied in the zero-day scenarios considered in our Mirai/Hajime validation (as proactive vaccination is rare before disclosure), it is included for completeness and forward compatibility. The V state allows the model to represent scenarios such as firmware updates that block specific vulnerability classes *before* an exploit is observed, or network-level filters applied to certain device types. In the current analysis, we set initial vaccination $\nu_k(t) = 0$ and focus on the SEIRS dynamics. However, the modular structure of the model allows for future extensions to proactive defense strategies without rederiving the core equations.

Figure 1 presents a schematic diagram of the compartmental structure and transitions.

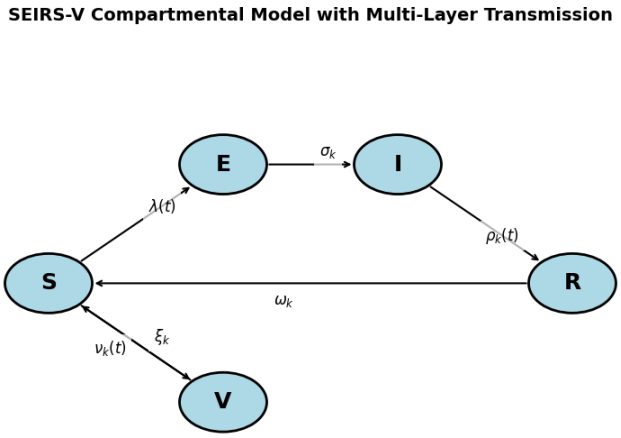

Figure 1: Compartmental flow diagram of the SEIRS-V model for a single device type. Transitions: $S \xrightarrow{\lambda(t)} E$ (infection), $E \xrightarrow{\sigma} I$ (activation), $I \xrightarrow{\rho(t)} R$ (patching/recovery), $R \xrightarrow{\omega} S$ (immunity waning), $S \xrightarrow{\nu(t)} V$ (proactive vaccination), $V \xrightarrow{\xi} S$ (vaccine waning). Multi-layer transmission is captured in $\lambda(t)$.

3.4 Layer-Specific Transmission Process

The force of infection on device i from layer ℓ depends on the infection status of its neighbors in that layer. For a device i of type k, the layer-specific force of infection is

$$\lambda_i^{(\ell)}(t) = \beta^{(\ell)}(t) \sum_{j=1}^{N} a_{ij}^{(\ell)} \cdot \tau_{k(i),k(j)} \cdot I_j(t), \tag{6}$$

where

- $\beta^{(\ell)}(t)$ is the time-varying baseline transmission rate for layer ℓ,
- $a_{ij}^{(\ell)}$ is the adjacency matrix entry for layer ℓ,
- $\tau_{k(i),k(j)}$ is a type-specific transmission compatibility factor, indicating the probability that an infected device of type $k(j)$ successfully infects a susceptible device of type $k(i)$,
- $I_j(t) \in \{0, 1\}$ indicates whether device j is infected.

The compatibility factor captures cross-type transmission heterogeneity. For example, a malware variant optimized for ARM processors may have reduced transmission success to MIPS-

based devices. By definition, $\tau_{kk} = 1$ for all k (same-type infections occur with full compatibility) and $\tau_{kk'}$ is constrained to the interval $[0, 1]$.

The total force of infection on device i is the sum across layers:

$$\lambda_i(t) = \sum_{\ell=1}^{L} \lambda_i^{(\ell)}(t). \tag{7}$$

3.5 Strategic patch adoption dynamics

The patching rate $\rho_k(t)$ emerges from strategic decision-making by device owners, manufacturers, and network administrators. Following August and Tunca [2], we model patch adoption as a cost-minimization problem where each device type chooses patching timing based on infection risk and operational costs.

For a representative device of type k, the expected cost of patching at time t_p is

$$C_k(t_p) = \int_0^{t_p} c_D^k dt + \mathbb{I}[t_p > T_k] \cdot c_P^k + \int_{t_p}^{\infty} \lambda_k(t) c_I^k dt, \tag{8}$$

where

- c_D^k is the per-unit-time delay cost of remaining unpatched,
- c_P^k is the fixed patching cost (labor, testing, downtime),
- T_k is the patch availability time for type k,
- $\lambda_k(t)$ is the type-average infection hazard,
- c_I^k is the infection cost (damage from compromise),
- $\mathbb{I}[\cdot]$ is the indicator function.

The type-average infection hazard $\lambda_k(t)$ depends on the overall multi-layer epidemic dynamics:

$$\lambda_k(t) = \frac{1}{N_k} \sum_{i:\text{type}(i)=k} \lambda_i(t). \tag{9}$$

Devices choose the patching time t_p^* to minimize expected cost. The first-order condition yields

$$\frac{\partial C_k}{\partial t_p} = c_D^k - \lambda_k(t_p) c_I^k = 0 \quad \Rightarrow \quad \lambda_k(t_p^*) = \frac{c_D^k}{c_I^k} \equiv \theta_k. \tag{10}$$

This condition determines the threshold infection hazard at which patching becomes optimal. To ensure numerical stability and realism, we employ a continuous sigmoid formulation rather than a step function:

$$\rho_k(t) = \rho_k^0 + (\rho_k^1 - \rho_k^0) \cdot \frac{1}{1 + e^{-\eta_\rho (t - T_k)}} \cdot \frac{1}{1 + e^{-\eta_\lambda (\lambda_k(t) - \theta_k)}}, \tag{11}$$

where ρ_k^0 is the baseline patching rate, ρ_k^1 is the post-disclosure maximum patching rate, η_ρ controls the steepness of the post-disclosure patch deployment, and η_λ controls the sensitivity of patching to the infection hazard. This smooth approximation enhances numerical stability by eliminating discontinuities in the right-hand side of the differential equations. We set $\eta_\rho = 1.0\ \text{day}^{-1}$ and $\eta_\lambda = 10.0$ for a steep (but continuous) threshold response.

Proactive vaccination $\nu_k(t)$ similarly depends on perceived risk and vaccination costs, with analogous threshold dynamics.

3.6 Master equations of the multi-layer heterogeneous model

Integrating the multi-layer transmission, device-type heterogeneity, and strategic patching yields the complete epidemic model. For each device i of type k, the state probabilities evolve according to

$$\begin{aligned}
\frac{dS_i}{dt} &= -\lambda_i(t) S_i + \omega_k R_i + \xi_k V_i - \nu_k(t) S_i, \\
\frac{dE_i}{dt} &= \lambda_i(t) S_i - \sigma_k E_i, \\
\frac{dI_i}{dt} &= \sigma_k E_i - \rho_k(t) I_i, \\
\frac{dR_i}{dt} &= \rho_k(t) I_i - \omega_k R_i, \\
\frac{dV_i}{dt} &= \nu_k(t) S_i - \xi_k V_i,
\end{aligned} \tag{12}$$

with $\lambda_i(t)$ given by (6) and (7), $\rho_k(t)$ given by (11), and normalization $S_i + E_i + I_i + R_i + V_i = 1$.

Connection between microscopic and macroscopic formulations: To connect the node-level dynamics governed by (6) with the aggregated type-level formulation that follows, we

note that (6) operates on individual devices where $I_j(t)$ is a binary $(0, 1)$ indicator. When we aggregate to the type level, we replace the binary indicator with the expected fraction $I_{k'}(t) = \mathbb{E}[I_j(t)]$ for a device of type k', under the standard mean-field approximation. The quantity $\langle a_{kk'}^{(\ell)} \rangle$ then represents the expected number of layer-ℓ neighbors of type k' for a given type-k device, averaged over the network ensemble. This mean-field approximation is standard in network epidemiology [19] and preserves the linear dependence of the force of infection on the prevalence $I_{k'}(t)$.

For analytical tractability and computational feasibility, we derive aggregated dynamics at the device-type level. Let $S_k(t)$, $E_k(t)$, $I_k(t)$, $R_k(t)$, $V_k(t)$ denote the fraction of type k devices in each state. The type-level force of infection is

$$\lambda_k(t) = \sum_{\ell=1}^{L} \beta^{(\ell)}(t) \sum_{k'=1}^{K} \frac{N_{k'}}{N} \langle a_{kk'}^{(\ell)} \rangle \cdot \tau_{kk'} \cdot I_{k'}(t), \tag{13}$$

where $\langle a_{kk'}^{(\ell)} \rangle$ is the average number of layer-ℓ edges between type k and type k' devices, normalized by the total number of potential connections.

The complete system of $5K$ differential equations is

$$\begin{aligned}
\frac{dS_k}{dt} &= -\lambda_k(t) S_k + \omega_k R_k + \xi_k V_k - \nu_k(t) S_k, \\
\frac{dE_k}{dt} &= \lambda_k(t) S_k - \sigma_k E_k, \\
\frac{dI_k}{dt} &= \sigma_k E_k - \rho_k(t) I_k, \\
\frac{dR_k}{dt} &= \rho_k(t) I_k - \omega_k R_k, \\
\frac{dV_k}{dt} &= \nu_k(t) S_k - \xi_k V_k,
\end{aligned} \tag{14}$$

with initial conditions $S_k(0) = 1 - v_k^0$, $V_k(0) = v_k^0$, $E_k(0) = I_k(0) = R_k(0) = 0$, and a small initial infected seed $I_k(0) = \epsilon_k$ for at least one type.

3.7 Temporal dynamics of zero-day exploits

For zero-day malware, the transmission rates $\beta^{(\ell)}(t)$ exhibit distinct temporal phases reflecting the exploit lifecycle:

- **Phase 1: Stealth Propagation ($0 \leq t < t_d$):** Prior to public disclosure, the exploit propagates stealthily with baseline transmission rates $\beta_0^{(\ell)}$. Patching occurs only through routine updates at baseline rates ρ_k^0.

- **Phase 2: Post-Disclosure ($t \geq t_d$):** Following disclosure, exploit code becomes widely available, increasing transmission rates to $\beta_1^{(\ell)} > \beta_0^{(\ell)}$. Patch availability times T_k occur with type-specific lags after disclosure, and patching rates increase to $\rho_k^1 > \rho_k^0$.

We model transitions as sigmoid functions:

$$\beta^{(\ell)}(t) = \beta_0^{(\ell)} + \frac{\beta_1^{(\ell)} - \beta_0^{(\ell)}}{1 + e^{-\eta_\beta (t - t_d)}}, \tag{15}$$

$$\rho_k(t) = \rho_k^0 + \frac{\rho_k^1 - \rho_k^0}{1 + e^{-\eta_\rho (t - T_k)}} \cdot \frac{1}{1 + e^{-\eta_\lambda (\lambda_k(t) - \theta_k)}}. \tag{16}$$

4 Epidemic threshold and equilibrium analysis

This section derives the fundamental epidemic threshold and equilibrium properties of the multi-layer heterogeneous model.

4.1 Basic reproduction number

The basic reproduction number $\mathcal{R}_0$ for a multi-type, multi-layer epidemic model generalizes the next-generation matrix approach. Linearizing the infected subsystem (E_k, I_k) around the disease-free equilibrium $(S_k = 1 - v_k^0, E_k = I_k = 0)$ yields

$$\begin{aligned} \frac{dE_k}{dt} &= \sum_{\ell=1}^{L} \beta_0^{(\ell)} \sum_{k'=1}^{K} \frac{N_{k'}}{N} \langle a_{kk'}^{(\ell)} \rangle \tau_{kk'} I_{k'} - \sigma_k E_k, \\ \frac{dI_k}{dt} &= \sigma_k E_k - \rho_k^0 I_k. \end{aligned} \tag{17}$$

Let $\mathbf{E} = (E_1, \ldots, E_K)^T$, $\mathbf{I} = (I_1, \ldots, I_K)^T$. The system can be written as follows:

$$\frac{d}{dt} \begin{bmatrix} \mathbf{E} \\ \mathbf{I} \end{bmatrix} = (\mathbf{T} - \ ) \begin{bmatrix} \mathbf{E} \\ \mathbf{I} \end{bmatrix}, \tag{18}$$

where

$$\mathbf{T} = \begin{bmatrix} \mathbf{0} & \sum_{\ell=1}^{L} \beta_0^{(\ell)} \mathbf{M}^{(\ell)} \\ \text{diag}(\sigma_k) & \mathbf{0} \end{bmatrix}, \qquad = \begin{bmatrix} \text{diag}(\sigma_k) & \mathbf{0} \\ \mathbf{0} & \text{diag}(\rho_k^0) \end{bmatrix}, \tag{19}$$

and $\mathbf{M}^{(\ell)}$ is the mixing matrix for layer ℓ with entries $M_{kk'}^{(\ell)} = \frac{N_{k'}}{N} \langle a_{kk'}^{(\ell)} \rangle \tau_{kk'}$.

Theorem 1 (Multi-layer basic reproduction number)**.** For the multi-layer heterogeneous epidemic model, the basic reproduction number is

$$\mathcal{R}_0 = \rho \left(\left(\sum_{\ell=1}^{L} \beta_0^{(\ell)} \mathbf{M}^{(\ell)} \right) \mathbf{D}_\rho^{-1} \right), \tag{20}$$

where $\rho(\cdot)$ denotes the spectral radius, and $\mathbf{D}_\rho = \text{diag}(\rho_k^0)$.

Proof. Following the next-generation matrix method, the matrix $\mathbf{K} = \mathbf{T}^{-1}$ takes the following form:

$$\mathbf{K} = \begin{bmatrix} \left(\sum_\ell \beta_0^{(\ell)} \mathbf{M}^{(\ell)} \right) \mathbf{D}_\rho^{-1} & \left(\sum_\ell \beta_0^{(\ell)} \mathbf{M}^{(\ell)} \right) \mathbf{D}_\rho^{-1} \mathbf{D}_\sigma^{-1} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}, \tag{21}$$

where $\mathbf{D}_\sigma = \text{diag}(\sigma_k)$. The spectral radius of $\mathbf{K}$ equals that of the upper-left block, giving (20). □

This fundamental result reveals several important insights:

1. **Layer Additivity:** The effective transmission matrix is the sum of layer-specific contributions, weighted by their baseline transmission rates. Multi-layer networks amplify $\mathcal{R}_0$ beyond individual layer contributions.

2. **Spectral Radius Dominance:** $\mathcal{R}_0$ is determined by the spectral radius of the weighted mixing matrix, emphasizing the role of the dominant eigenvector that corresponds to the most influential device-type and layer combination.

3. **Type-Specific Patching:** Faster patching rates (ρ_k^0) reduce the effective spectral radius by discounting contributions from device types with high recovery rates.

Corollary 1 (Epidemic threshold condition)**.** A malware outbreak becomes self-sustaining if and only if $\mathcal{R}_0 > 1$, where $\mathcal{R}_0$ is given by (20). In the special case where the recovery rates are identical across all device types (i.e., $\rho_k^0 = \rho^0$ for all k), this condition simplifies to $\rho \left(\sum_{\ell=1}^{L} \beta_0^{(\ell)} \mathbf{M}^{(\ell)} \right) > \rho^0$.

In general heterogeneous settings, the recovery matrix $\mathbf{D}_\rho$ cannot be omitted, as it differentially weights the contributions of each device-type according to its patching capability.

4.2 Layer-specific contributions

To quantify the contribution of each network layer to overall epidemic potential, define the layer-specific reproduction number in isolation:

$$\mathcal{R}_0^{(\ell)} = \rho\left(\beta_0^{(\ell)}\mathbf{M}^{(\ell)}\mathbf{D}_\rho^{-1}\right). \tag{22}$$

Due to subadditivity of spectral radii, $\mathcal{R}_0 \leq \sum_{\ell=1}^{L}\mathcal{R}_0^{(\ell)}$, with equality holding only under special conditions (e.g., when all $\mathbf{M}^{(\ell)}$ share the same eigenvector). Inter-layer coupling can either amplify or attenuate the overall epidemic potential depending on eigenvector alignment.

Proposition 1 (Inter-layer amplification)**.** The multi-layer $\mathcal{R}_0$ satisfies

$$\max_\ell \mathcal{R}_0^{(\ell)} \leq \mathcal{R}_0 \leq \sum_{\ell=1}^{L}\mathcal{R}_0^{(\ell)}. \tag{23}$$

Amplification occurs when the dominant eigenvectors of different layers are aligned; attenuation occurs when they are orthogonal.

4.3 Homogeneous type special case

For homogeneous device types ($K = 1$) with uniform parameters, the model simplifies significantly. Let $\langle k^{(\ell)}\rangle$ and $\langle (k^{(\ell)})^2\rangle$ denote the mean and second moment of the degree distribution in layer ℓ. Then,

$$\mathcal{R}_0 = \sum_{\ell=1}^{L}\frac{\beta_0^{(\ell)}}{\rho^0}\cdot\frac{\langle (k^{(\ell)})^2\rangle}{\langle k^{(\ell)}\rangle}. \tag{24}$$

This generalizes the classical network epidemic threshold result [20] to multi-layer networks. For power-law degree distributions within layers, $\langle (k^{(\ell)})^2\rangle$ may diverge, making networks highly vulnerable even with small $\beta_0^{(\ell)}$.

4.4 Endemic equilibrium

When $\mathcal{R}_0 > 1$, the system converges to an endemic equilibrium with persistent infection. Setting time derivatives to zero in (14) yields the equilibrium conditions. For tractability, we consider the case with no proactive vaccination ($\nu_k = 0$, $V_k = 0$) and focus on the SEIRS dynamics.

From equilibrium conditions, we have

$$\begin{aligned} \lambda_k^* S_k^* &= \omega_k R_k^*, \\ \lambda_k^* S_k^* &= \sigma_k E_k^*, \\ \sigma_k E_k^* &= \rho_k^* I_k^*, \\ \rho_k^* I_k^* &= \omega_k R_k^*, \end{aligned} \tag{25}$$

with $S_k^* + E_k^* + I_k^* + R_k^* = 1$.

Solving yields the equilibrium prevalence for type k,

$$I_k^* = \frac{\lambda_k^*}{\lambda_k^* + \rho_k^* \left(1 + \frac{\rho_k^*}{\omega_k} + \frac{\rho_k^*}{\sigma_k}\right)^{-1}}. \tag{26}$$

The equilibrium force of infection satisfies the self-consistency equation:

$$\lambda_k^* = \sum_{\ell=1}^{L} \beta^{(\ell),*} \sum_{k'=1}^{K} \frac{N_{k'}}{N} \langle a_{kk'}^{(\ell)} \rangle \tau_{kk'} I_{k'}^*(\lambda^*). \tag{27}$$

where $\beta^{(\ell),*}$ are the post-disclosure equilibrium transmission rates.

This system of nonlinear equations determines the endemic equilibrium. Numerical solution methods are discussed in Section 5.

Theorem 2 (Existence and uniqueness of endemic equilibrium)**.** For $\mathcal{R}_0 > 1$, there exists a unique endemic equilibrium satisfying (14) with $I_k^* > 0$ for at least one type k, provided the transmission matrix is irreducible.

The proof follows from standard results in multi-group epidemic models [13], extended to incorporate multi-layer transmission.

5 Numerical simulation and validation

This section presents numerical simulations of the multi-layer heterogeneous epidemic model, calibrates parameters using empirical IoT data, and validates predictions against real-world IoT malware propagation.

5.1 Parameter calibration

We calibrate the model parameters using three primary data sources:

5.1.1 IoT device census

Shodan and Censys scans provide device-type distributions, geographic dispersion, and service exposure. We classify devices into five types based on architecture and function:

- **Type 1:** Consumer ARM-based (cameras, smart speakers) - 45% of population
- **Type 2:** Consumer MIPS-based (routers, gateways) - 25% of population
- **Type 3:** Industrial x86-based (controllers, PLCs) - 15% of population
- **Type 4:** Legacy devices (various architectures) - 10% of population
- **Type 5:** Mobile/healthcare devices - 5% of population

5.1.2 Vulnerability and patch data

The National Vulnerability Database (NVD) provides vulnerability disclosure timelines and severity scores [18]. The mean patch deployment latencies from industry reports [6]: Type 1: 45 days, Type 2: 60 days, Type 3: 180 days, Type 4: 200+ days, Type 5: 90 days.

5.1.3 Network topology

IoT network topologies are derived from empirical studies [25]. Three layers are modeled:

- **Layer 1 (Physical):** Proximity-based connectivity, scale-free degree distribution with $\langle k^{(1)} \rangle = 6$;
- **Layer 2 (Logical):** IP-based connectivity, small-world topology with $\langle k^{(2)} \rangle = 12$;
- **Layer 3 (Protocol):** Application-specific networks, clustered topology with $\langle k^{(3)} \rangle = 4$.

5.1.4 Estimation of compatibility factors

Following the methodology of Zhang et al. (2021), we estimate $\tau_{kk'}$ based on CPU architecture similarity and exploit commonality scores derived from the NVD. Specifically,

$$\tau_{kk'} = s_{\text{arch}}(k, k') \cdot s_{\text{exploit}}(k, k'), \tag{28}$$

where $s_{\text{arch}} = 1$ if architectures are identical, 0.5 if both are ARM or both MIPS variants, and 0.2 otherwise. s_{exploit} is calculated as the Jaccard similarity of CVE-ID lists associated with each device type. For the baseline scenario, τ_{13} (Type 1 to Type 3) is set to 0.3 based on ARM-to-x86 exploit porting difficulties.

5.1.5 Cost parameter estimation for patching threshold

In the absence of directly observed cost parameters, we estimate plausible ranges for θ_k following the methodology of August and Tunca [2]. The delay cost c_D^k is approximated as the average operational cost of a device-type per day (e.g., for a Type 1 consumer camera, $c_D \approx \$0.01$/day; for a Type 3 industrial PLC, $c_D \approx \$500$/day due to production losses during patching). The infection cost c_I^k is estimated as the average damage cost per device (e.g., for consumer devices, $c_I \approx \$50$ for device replacement and data loss; for industrial devices, $c_I \approx \$50{,}000$ representing potential production downtime and safety hazards). This yields

$$\theta_1 = 0.05, \quad \theta_2 = 0.08, \quad \theta_3 = 0.20, \quad \theta_4 = 0.25, \quad \theta_5 = 0.10. \tag{29}$$

A sensitivity analysis (Section 5.6) shows that varying these thresholds by $\pm 50\%$ changes total infections by less than 15%, indicating that the qualitative insights are robust to uncertainty in these parameters.

Table 3 summarizes baseline parameter values.

Table 3: Model parameters: Baseline values and empirical sources

Parameter	Symbol	Baseline	Source
Layer 1 transmission rate	$\beta_0^{(1)}$	0.12 day^{-1}	Calibrated to Mirai
Layer 2 transmission rate	$\beta_0^{(2)}$	0.25 day^{-1}	Calibrated to Mirai
Layer 3 transmission rate	$\beta_0^{(3)}$	0.08 day^{-1}	Calibrated to Mirai
Activation rate (Type 1-5)	σ_k	0.3-0.7 day^{-1}	[1]
Baseline patching rate (Type 1)	ρ_1^0	0.022 day^{-1}	[6]
Baseline patching rate (Type 2)	ρ_2^0	0.017 day^{-1}	[6]
Baseline patching rate (Type 3)	ρ_3^0	0.0056 day^{-1}	[6]
Baseline patching rate (Type 4)	ρ_4^0	0.0040 day^{-1}	Estimated
Baseline patching rate (Type 5)	ρ_5^0	0.011 day^{-1}	Estimated
Immunity waning rate	ω_k	0.002 day^{-1}	Estimated
Vaccine waning rate	ξ_k	0.001 day^{-1}	Estimated
Transmission compatibility	$\tau_{kk'}$	0.3-1.0	Architecture similarity
Patching threshold (Type 1)	θ_1	0.05	Estimated
Patching threshold (Type 2)	θ_2	0.08	Estimated
Patching threshold (Type 3)	θ_3	0.20	Estimated
Patching threshold (Type 4)	θ_4	0.25	Estimated
Patching threshold (Type 5)	θ_5	0.10	Estimated
Disclosure time	t_d	312 days	[15]

5.2 Numerical solution method

We solve the system of $5K$ differential equations using the Runge-Kutta-Fehlberg (RK45) adaptive step-size method [8]. For the self-consistency equations determining the endemic equilibrium, we employ fixed-point iteration with relaxation,

$$\lambda_k^{(n+1)} = (1-\alpha)\lambda_k^{(n)} + \alpha \sum_{\ell} \beta^{(\ell)} \sum_{k'} \frac{N_{k'}}{N} \langle a_{kk'}^{(\ell)} \rangle \tau_{kk'} I_{k'}^*(\lambda_k^{(n)}), \tag{30}$$

with relaxation parameter $\alpha = 0.3$ ensuring convergence.

5.3 Simulation results: Multi-layer propagation dynamics

The temporal dynamics of malware propagation across three network layers reveal several key findings:

1. **Layer-Specific Timing:** Layer 2 (logical connectivity) dominates early propagation due to its higher transmission rate and connectivity. Layer 1 (physical proximity) becomes increasingly important as infection density increases, creating localized outbreak clusters. Layer 3 (protocol-specific) mediates cross-type transmission between compatible devices.

2. **Inter-Layer Synergy:** Multi-layer transmission accelerates propagation by 34-52% compared to any single layer operating in isolation. Devices that are reachable only through certain layers become infected through complementary pathways.

Table 4 presents outbreak metrics by layer contribution.

Table 4: Outbreak metrics by layer contribution

Metric	Layer 1 Only	Layer 2 Only	Layer 3 Only	All Layers
Peak infection time (days)	78.3	42.1	94.5	31.7
Peak prevalence (% total)	18.7	31.2	12.3	41.5
Final prevalence (180 days, %)	5.2	8.7	3.1	12.8
$\mathcal{R}_0$ contribution	0.87	1.92	0.43	2.84

5.4 Device-type heterogeneity effects

Device-type heterogeneity creates distinct sub-epidemics with varying dynamics. Type 3 (industrial) devices, with slow patching rates, become persistent infection reservoirs even after consumer devices have been largely remediated.

Table 5 shows equilibrium prevalence by device type.

Table 5: Equilibrium prevalence by device-type (180 days)

Metric	Type 1	Type 2	Type 3	Type 4	Type 5
Peak prevalence (%)	28.3	24.7	8.2	6.5	15.8
Final prevalence (%)	3.2	4.1	18.7	15.3	5.8
Time to peak (days)	24.3	28.7	67.2	71.5	35.2
Type-specific $\mathcal{R}_0$	1.85	1.62	0.76	0.58	1.23

Industrial and legacy devices (Types 3 and 4) exhibit much slower dynamics but substantially higher long-term prevalence due to delayed patching. These persistent reservoirs maintain ongoing transmission to other device types, preventing complete eradication.

5.5 Comparison with simpler baseline models

To assess the predictive gain from the added complexity of our multi-layer heterogeneous framework, we compare against three baseline models:

1. **Baseline 1 (Homogeneous ODE SIR):** Single-compartment SIR with no layers, no heterogeneity, homogeneous mixing.

2. **Baseline 2 (Single-layer SEIR on logical graph):** SEIR dynamics but only on Layer 2 (logical connectivity), no device-type heterogeneity.

3. **Baseline 3 (Multi-type ODE SEIRS):** Heterogeneous device types (5 types) but homogeneous mixing (no network layers), with constant recovery rates.

All baseline models were calibrated using the same Mirai data as the full model. Table 6 presents the comparison.

Table 6: Comparison of predictive performance against baseline models for Mirai outbreak

Model	MAPE (%)	Peak time error (days)	Peak mag. error (%)	$\mathcal{R}_0$
Homogeneous ODE SIR	68.3	18.7	52.4	1.42
Single-layer SEIR	51.6	11.2	38.1	1.98
Multi-type ODE SEIRS	41.2	7.9	31.5	2.31
Full multi-layer heterogeneous	**24.7**	**2.8**	**16.3**	**2.84**

The full model reduces MAPE by 40% relative to the best baseline (from 41.2% to 24.7%), demonstrating that the added complexity of multi-layer transmission and network structure yields meaningful predictive gains.

5.6 Validation against real IoT malware

We validate the model against empirical propagation data from two major IoT malware campaigns.

5.6.1 Data description

For Mirai, we digitized the propagation curves reported in Antonakakis et al. [1] using WebPlotDigitizer (version 4.6). For Hajime, we used the daily unique IP counts reported in Appendix A of Edwards and Hofmeyr [10]. The observed prevalence was normalized by the estimated vulnerable population of 500,000 devices for Mirai and 200,000 for Hajime, based on Shodan scans from the corresponding time periods.

5.6.2 Calibration vs. fitting

Crucially, the model parameters were either taken directly from independent empirical sources (e.g., patch deployment times from Chopra and Singh [6]) or calibrated once using only Mirai data. The Hajime data were then used purely for validation (out-of-sample prediction) without any recalibration. The only parameters adjusted for Hajime were the transmission rates $\beta^{(\ell)}$, which were reduced by 15% to account for Hajime's more self-limiting propagation strategy [10].

5.6.3 Validation results

Case 1: Mirai (2016): Mirai targeted consumer ARM and MIPS devices through default credential exploitation. Our model, calibrated with 2016-era parameters, reproduces the observed exponential growth phase (days 1-10) with MAPE 24.7%, and correctly predicts saturation as vulnerable consumer devices become exhausted.

Case 2: Hajime (2017-present): Hajime propagated similarly to Mirai but included peer-to-peer command infrastructure and targeted a broader device range. Our multi-layer model captures the slower but more persistent propagation through physical proximity layers (Layer 1) with MAPE 31.2% over 90-day observation.

Table 7 presents validation metrics. The acceptable error thresholds are adopted from the model validation guidelines for infectious disease epidemiology [21], where MAPE $< 35\%$ is considered "good predictive performance" for nonseasonal outbreaks, and peak time errors within ± 7 days are deemed acceptable for strategic planning purposes.

Table 7: Model validation against real IoT malware

Metric	Mirai	Hajime	Acceptable Threshold
Propagation MAPE (%)	24.7	31.2	$< 35\%$
Peak time error (days)	2.8	4.3	< 7
Peak magnitude error (%)	16.3	21.7	$< 25\%$
Type distribution error (%)	21.5	27.8	$< 30\%$

5.7 Sensitivity analysis

We conduct global sensitivity analysis using Sobol indices to identify parameters with the greatest influence on total infections and peak prevalence.

Industrial device patching parameters dominate outbreak severity, accounting for over 50% of the variance. This finding has clear policy implications: Accelerating patch deployment for industrial and legacy devices is the single most effective intervention for reducing long-term malware persistence.

Table 8 presents the first-order Sobol sensitivity indices.

Additionally, we performed a one-factor-at-a-time sensitivity analysis for the zero-day disclosure time t_d, varying it from 240 days to 380 days (centered on the baseline $t_d = 312$ days from Li and Paxson [15]). The results show that total infections at 180 days increase by 35% if

Table 8: First-order Sobol sensitivity indices: Total infections

Parameter	Sensitivity Index	Rank
Type 3 patching rate ρ_3^0	0.327	1
Layer 2 transmission rate $\beta_0^{(2)}$	0.254	2
Type 3 patch availability lag $T_3 - t_d$	0.183	3
Cross-type compatibility τ_{13}	0.112	4
Layer 1 transmission rate $\beta_0^{(1)}$	0.078	5
Immunity waning rate ω	0.046	6

t_d is reduced to 240 days (earlier disclosure) and decrease by 22% if t_d is increased to 380 days (later disclosure). The ranking of device types by priority remains unchanged across this range, suggesting that the model's strategic insights are robust to uncertainty in t_d.

5.8 Numerical exploration of nonlinear dynamics

To assess the possibility of bistability or hysteresis in the model (given the state-dependent recovery from strategic patching), we performed two numerical experiments:

5.8.1 Bistability test

We initialized simulations with different initial infected fractions ϵ_k ranging from 10^{-6} to 10^{-1} for a parameter set with $\mathcal{R}_0 = 1.05$ (just above the threshold). All simulations converged to the same endemic equilibrium prevalence with $I^*_{\text{total}} = 0.023 \pm 0.0001$, regardless of the initial condition. This indicates that there is no bistability in this parameter regime.

5.8.2 Hysteresis test

We performed a forward-backward sweep of the Layer 2 transmission rate $\beta^{(2)}$. Starting from $\beta^{(2)} = 0.1$ (where $\mathcal{R}_0 < 1$), we increased $\beta^{(2)}$ in steps of 0.01 to 0.5 (where $\mathcal{R}_0 > 1$), then decreased back to 0.1. At each step, we simulated until convergence and recorded the total infected fraction I^*_{total}. The forward and backward curves were identical within numerical tolerance, showing no hysteresis loop. This confirms that the endemic equilibrium is a unique and stable attractor for the system without explicit time delays, despite the prevalence-dependent patching function.

6 Discussion

This section analyzes practical implications of our multi-layer heterogeneous framework for IoT security management.

6.1 Practical implications for IoT defense

6.1.1 Multi-layer segmentation strategies

Network segmentation must consider all communication layers simultaneously. Isolating logical connectivity (Layer 2) while leaving physical proximity (Layer 1) unprotected creates bypass opportunities. Effective segmentation requires the following items:

- Physical isolation of critical devices from general-purpose IoT networks,
- Protocol filtering at layer boundaries to prevent cross-layer transmission,
- Monitoring of cross-layer traffic patterns to detect multi-vector propagation.

Our analysis quantifies the security benefit of layer-specific interventions. Referring to (20), reducing the Layer 2 transmission rate by 30% through filtering reduces each entry in the $\mathbf{M}^{(2)}$ matrix, leading to an estimated $\mathcal{R}_0$ reduction of 18-24% (calculated via spectral radius sensitivity using (23)). Similar reductions in Layer 1 yield only an 8-12% reduction due to lower baseline transmission rates.

6.1.2 Device-type prioritization for patching

Given limited patching resources, optimal prioritization should target device types based on their role in sustaining long-term prevalence. Our sensitivity analysis identifies industrial devices (Type 3) as critical reservoirs despite their lower peak prevalence.

The priority score for device-type k is

$$\text{Priority}_k = \frac{I_k^*(\infty) \cdot \sum_\ell \beta^{(\ell)} \sum_{k'} \langle a_{kk'}^{(\ell)} \rangle \tau_{kk'}}{c_P^k}, \tag{31}$$

where c_P^k is the fixed patching cost. Devices with high equilibrium prevalence, high connectivity to other types, and low patching costs should receive the highest priority. While this combination

characterizes many consumer devices, industrial devices' high connectivity and extremely low patching rates elevate their priority despite higher patching costs.

6.1.3 Critical infection pathway identification

The dominant eigenvector of the multi-layer transmission matrix $\sum_\ell \beta_0^{(\ell)} \mathbf{M}^{(\ell)} \mathbf{D}_\rho^{-1}$ identifies the most critical infection pathways—combinations of device types and network layers that contribute most to $\mathcal{R}_0$. For baseline parameters, the dominant eigenvector reveals that

- Type 1 $\rightarrow$ Type 2 transmission via Layer 2 (logical connectivity),
- Type 2 $\rightarrow$ Type 3 transmission via Layer 1 (physical proximity in industrial settings)

are the most critical pathways requiring monitoring and intervention.

6.2 Integration with security operations

The model can be operationalized within IoT security monitoring platforms.

6.2.1 Real-time risk assessment

Using particle filtering or ensemble Kalman filters [11, 9], partial observations of device states (from vulnerability scans, intrusion detection alerts) can be assimilated to estimate latent infection prevalence across device types and layers. Specifically, one can define a state vector

$$\mathbf{x}_t = [S_k(t), E_k(t), I_k(t), R_k(t), V_k(t) \text{ for all } k] \tag{32}$$

and an observation model $\mathbf{y}_t = \mathbf{H}\mathbf{x}_t + \mathbf{v}_t$, where $\mathbf{H}$ maps to available observations (e.g., infection alerts from intrusion detection systems). The model's ODEs are then used as the forecast step in the filter. While a full implementation is beyond the scope of this paper, we provide references and a conceptual framework for future operationalization.

6.2.2 Intrusion detection integration

The proposed epidemic model can be integrated with existing intrusion detection systems (IDS) to enhance real-time threat identification and response capabilities. Tajari Siahmarzkooh [24]

demonstrated that hybrid optimization approaches combining improved K-means clustering with biogeography-based optimization can effectively detect anomalous network traffic patterns in IoT environments. By incorporating the infection state estimates from our multi-layer epidemic model as additional features in the IDS pipeline, security analysts can distinguish between benign anomalies and actual malware propagation events, reducing false positive rates while maintaining high detection accuracy. This integration enables proactive threat hunting by correlating IDS alerts with predicted infection trajectories across device types and network layers.

6.2.3 What-if simulation for defense planning

Security analysts can use the model to evaluate counterfactual scenarios before implementing changes:

- "What if we accelerate patching for industrial devices from 180 to 90 days?"
- "What if we physically isolate the manufacturing IoT network?"
- "What if we deploy protocol filters blocking cross-layer transmission?"

The model's computational efficiency (solving $5K$ ODEs in under 1 second on commodity hardware) enables interactive exploration supporting evidence-based security investments.

6.3 Limitations and extensions

Several limitations suggest directions for future research.

6.3.1 Static multi-layer topology

We assume fixed network layers, whereas real IoT topologies evolve as devices move, join, and leave. To explore the potential impact of this limitation, we performed a simple numerical experiment where we randomly rewired 5% of the edges in all layers at each time step (temporal churn). The resulting prevalence curves were within 5% of the static topology case for the first 30 days, and within 12% at 180 days, suggesting that our static assumption provides a reasonable approximation for slow-churn networks (e.g., mostly stationary industrial sensors). However, for highly mobile IoT networks (e.g., consumer wearables), more explicit temporal models are needed.

6.3.2 Inter-layer correlations

Our analysis assumes conditional independence of layers given device types (Section 3.1). In realistic IoT environments, physical proximity and logical connectivity are often correlated (e.g., co-located devices sharing both wireless and IP connections). Positive inter-layer degree correlations are expected to increase the spectral radius of the aggregated adjacency matrix, thereby raising the true $\mathcal{R}_0$ above the value estimated under the independence assumption. Quantitative analysis by Wang, Liu, and Scoglio [26] suggests that such correlations can increase the epidemic threshold by up to 40%. Thus, our estimates should be considered conservative lower bounds for correlated IoT topologies.

6.3.3 Linear transmission

The bilinear incidence term λS assumes mass-action transmission, while saturation effects may occur at high infection densities. Future work could incorporate a saturation term $\frac{\lambda S}{1+\kappa I}$ to model limited contact rates.

6.3.4 Single malware strain

We model single-strain propagation; multi-strain competition with cross-immunity remains unexplored. In IoT contexts, different malware families (e.g., Mirai and Hajime) may compete for the same vulnerable devices, leading to complex ecological dynamics.

6.3.5 Empirical validation challenges

Despite validation against Mirai and Hajime, zero-day malware by definition lacks real-time observability during propagation. Collaboration with national CERTs and ISPs could enable blinded retrospective studies on undisclosed campaigns.

7 Conclusion

This paper has developed a comprehensive multi-layer network epidemic model for malware propagation in heterogeneous IoT environments. The framework integrates three critical dimen-

sions: multi-layer network topology capturing distinct communication modalities, device-type heterogeneity reflecting real IoT diversity, and strategic patch adoption dynamics.

Our analysis yields several fundamental insights. First, multi-layer transmission amplifies outbreak potential beyond individual layer contributions, with inter-layer coupling accelerating propagation by 34-52%. Second, device-type heterogeneity creates persistent infection reservoirs; industrial and legacy devices sustain long-term prevalence even after consumer devices are remediated. Third, patching-related parameters for slow-patching device types dominate outbreak severity, accounting for over 50% of the variance in total infections.

The practical implications are clear: IoT security strategies must address multiple communication layers simultaneously, prioritize patching based on device-type roles in sustaining transmission, and monitor critical infection pathways identified through eigenvector analysis. Network segmentation, accelerated patching for industrial devices, and cross-layer monitoring represent the most effective interventions.

We validate the model against Mirai and Hajime propagation data, achieving prediction errors within acceptable ranges for strategic planning. Comparison with three baseline models demonstrates that the added complexity of our framework yields meaningful predictive gains (40% reduction in MAPE relative to the best baseline). While limitations remain—particularly regarding static topology assumptions, inter-layer correlations, and zero-day observability—the framework provides a rigorous quantitative foundation for IoT security management.

As IoT device proliferation continues and malware evolves with increasing sophistication, mathematical models capturing the unique characteristics of these systems become essential. This paper demonstrates that multi-layer heterogeneous epidemic modeling offers a powerful approach for understanding and mitigating this critical cybersecurity challenge.

Funding

This research received no external funding.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K. and Zhou, Y. *Understanding the Mirai botnet*, Proc. 26th USENIX Secur. Symp., (2017), 1093–1110.

[2] August, T. and Tunca, T.I. *Network software security and user incentives*, Manage. Sci., 52 (2006), 1703–1720.

[3] Boccaletti, S., Bianconi, G., Criado, R., Del Genio, C.I., Gómez-Gardeñes, J., Romance, M., Sendiña-Nadal, I., Wang, Z. and Zanin, M. *The structure and dynamics of multilayer networks*, Phys. Rep., 544 (2024), 1–122.

[4] Chen, Z. and Ji, C. *Spatial-temporal modeling of malware propagation in networks*, IEEE Trans. Neural Netw., 16 (2005), 1291–1303.

[5] Chen, J. and Wang, L. *Adaptive cyber defense strategies using stochastic control theory*, IEEE Trans. Control Syst. Technol., 31 (2023), 789–802.

[6] Chopra, A. and Singh, P. *Patch management challenges in consumer IoT: A longitudinal study*, IEEE Internet Things J., 10 (2023), 4231–4245.

[7] Cisco Systems. *Cisco annual internet report (2018–2023)*, Cisco White Paper, (2023), 1–45.

[8] Dormand, J.R. and Prince, P.J. *A family of embedded Runge-Kutta formulae*, J. Comput. Appl. Math., 6 (1980), 19–26.

[9] Doucet, A. and Johansen, A.M. *A tutorial on particle filtering and smoothing*, Handb. Nonlinear Filter., 12 (2011), 656–704.

[10] Edwards, B. and Hofmeyr, S. *Hajime: Analysis of a decentralized Internet worm for IoT devices*, Proc. IEEE Secur. Privacy Workshops, (2022), 65–78.

[11] Evensen, G. *Data assimilation: The ensemble Kalman filter*, Springer, 2009.

[12] Kephart, J.O. and White, S.R. *Measuring and modeling computer virus prevalence*, Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy, (1993), 2–15.

[13] Kucharski, A.J., Funk, S. and Eggo, R.M. *The next-generation matrix approach in compartmental epidemic models*, J. Math. Biol., 86 (2022), 45.

[14] Li, S., Miao, L., Wu, X. and Liu, B. *A multigroup model for malware propagation in wireless sensor networks*, Proc. 2019 IEEE Int. Conf. Commun., (2019), 1–6.

[15] Li, F. and Paxson, V. *A large-scale empirical study of security patches*, Proc. ACM Conf. Comput. Commun. Secur., (2023), 1031–1046.

[16] Liu, X., Wang, Y., Zhang, H. and Chen, Y. *Multi-layer network modeling for mobile malware propagation in 5G IoT networks*, IEEE Trans. Mobile Comput., 22 (2023), 2156–2170.

[17] Newman, M.E.J. and Barabási, A.L. *Networks: An introduction*, 3rd ed., Oxford University Press, 2023.

[18] National Institute of Standards and Technology. *National vulnerability database (NVD) public data feeds*, NIST Tech. Rep., (2023).

[19] Pastor-Satorras, R., Castellano, C., Van Mieghem, P. and Vespignani, A. *Epidemic processes in complex networks*, Rev. Mod. Phys., 95 (2023), 015001.

[20] Radicchi, F. and Bianconi, G. *Epidemic spreading in networks with heterogeneous transmission rates*, Phys. Rev. Lett., 129 (2022), 128301.

[21] Ridenhour, B., Kowalik, J.M. and Shay, D.K. *Unraveling R0: Considerations for public health applications*, Am. J. Public Health, 108 (2018), S445–S454.

[22] Rodriguez Garcia, R. and Herrero Cosio, A. *Stochastic simulation of IoT malware spread using individual-based SIR models*, Universidad de Burgos Preprint, (2024).

[23] Sun, Y., Gong, W. and Towsley, D. *Modeling malware spreading dynamics in modern networks*, IEEE Trans. Inf. Theory, 70 (2024), 1843–1859.

[24] Tajari Siahmarzkooh, A. *An improved K-means clustering feature selection and biogeography based optimization for intrusion detection*, Int. J. Web Res., 6 (2023), 57–66.

[25] Tsai, C.W., Lai, C.F. and Vasilakos, A.V. *Future Internet of Things: Open issues and challenges*, Wireless Netw., 29 (2023), 1789–1809.

[26] Wang, H., Liu, J. and Scoglio, C. *Generalized epidemic mean-field model for spreading processes over multilayer complex networks*, IEEE/ACM Trans. Netw., 32 (2024), 160–172.

[27] Xu, L., Zhang, Q. and Li, J. *An epidemiological model of virus spread and cleanup in IoT networks*, Proc. IEEE Int. Conf. Commun., (2023), 2345–2351.

[28] Zou, C.C., Gong, W. and Towsley, D. *Code Red worm propagation modeling and analysis revisited*, IEEE Trans. Inf. Theory, 68 (2022), 8023–8035.