Available online at website: https://jurnal.iaii.or.id/index.php/RESTI

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 10 No. 5 (2026) 1581 - 1589 e-ISSN: 2580-0760

A Network-Based SEIRS Model for IoT Malware Propagation with Optimal Control and Connectivity-Driven Dynamics

Dwi Ely Kurniawan[1], Aini Suri Talita[2], Eri Prasetyo Wibowo[3], Sarifuddin Madenda[4], Michel Paindavoine[5]
[1]Doctor of Information Technology, Faculty of Postgraduate Studies, Gunadarma University, Yogyakarta, Indonesia
[1]Department of Informatics Engineering, Politeknik Negeri Batam, Batam, Indonesia
[2,3,4]Department of Information Technology, Gunadarma University, Yogyakarta, Indonesia
[5]LEAD UMR CNRS 5022, Université Bourgogne Europe, Dijon, France

*dwialikhs@polibatam.ac.id

Abstract

The number of Internet of Things (IoT) devices is growing quickly, creating large networks that are attractive targets for malware such as Mirai and Mozi. Most existing epidemic models assume homogeneous mixing, where every device has an equal probability of contacting others, although real IoT networks are characterized by heterogeneous connectivity in which highly connected hub devices accelerate malware propagation. This study proposes a network-based SEIRS model that incorporates connectivity-driven transmission dynamics by allowing the infection rate to depend on device degree. The model is used to derive the basic reproduction number (R_0) and establish the local and global stability conditions of the malware-free and endemic equilibria. Three intervention measures, namely patch deployment, network quarantine, and user-awareness campaigns, are incorporated into an optimal control framework using Pontryagin's Minimum Principle to balance infection reduction and intervention costs. The proposed model is evaluated using CICIoT2023 and CIC IoT-DIAD 2024 traffic datasets, complemented by network-topology information from N-BaIoT, representing 105 IoT devices and 33 attack types. Simulation results show that the combined optimal-control strategy reduces the peak number of infected devices by 78.4% compared with the uncontrolled scenario and by 31.6% compared with a conventional SEIRS model that ignores network structure, while reducing overall intervention costs by 42.3%. Sensitivity analysis identifies device connectivity as the dominant factor influencing outbreak severity, highlighting the importance of network-aware segmentation and prioritized patching for effective IoT malware containment.

Keywords: basic reproduction number; IoT malware; network topology; optimal control; SEIRS model

How to Cite: D. E. . Kurniawan, A. S. Talita, E. P. . Wibowo, S. . Madenda, and M. Paindavoine, "A Network-Based SEIRS Model for IoT Malware Propagation with Optimal Control and Connectivity-Driven Dynamics", *J. RESTI (Rekayasa Sist. Teknol. Inf.)* , vol. 10, no. 5, pp. 1581–1589, Nov. 2026, doi: 10.29207/resti.v10i5.7786.
Permalink/DOI: https://doi.org/10.29207/resti.v10i5.7786

Received: May 4, 2026
Accepted: October 6, 2026
Available Online: November 1, 2026

This is an open-access article under the CC BY 4.0 License
Published by Ikatan Ahli Informatika Indonesia

1. Introduction

The Internet of Things (IoT) has become an essential part of modern digital infrastructure, connecting billions of devices across various application domains. The number of active IoT endpoints is expected to exceed 29.4 billion by 2030 [1]. However, the widespread adoption of IoT also introduces significant security challenges. Many IoT devices, including sensors, actuators, embedded controllers, and smart appliances, operate with limited processing power, memory, and energy resources. As a result, implementing comprehensive security mechanisms on these devices remains challenging. Such limitations make IoT networks particularly vulnerable to malware infections and subsequent propagation. Once compromised, an IoT device may serve as an entry point for attackers to access other network segments, steal sensitive information, conduct distributed denial-of-service (DDoS) attacks, or become part of a botnet infrastructure [2]. The Mirai botnet (2016) remains the canonical illustration of large-scale IoT compromise, infecting over 600,000 devices within 20 hours and orchestrating peak attack traffic exceeding 620 Gbps [3]. More recent malware families, such as Mozi, BotenaGo, Cyclops Blink, and Enemybot, have introduced more advanced techniques for lateral propagation and persistence, enabling them to compromise additional devices and sustain their presence within infected IoT networks [4]. As of

August 2023, the cumulative global malware instance count exceeded 1.07 billion specimens [5], [6], underscoring that IoT security is not a peripheral concern but a critical systems challenge. Mathematical epidemiology offers a powerful lens through which malware spread can be modelled, analyzed, and controlled [7], [8]. Classical epidemiological models, such as SIR and SEIR and their extended forms, have also been used to investigate the spread of malware across interconnected systems. [9] in wireless sensor networks (WSNs) [10], cloud environments, and heterogeneous computer networks [11-13], including variants based on fractional-order derivatives that capture memory effects arising from persistent device vulnerabilities [14]. However, a fundamental limitation of these approaches is the assumption of homogeneous mixing: each node interacts with every other node with equal probability. The structure of real-world IoT networks is rarely homogeneous. Smart-home systems typically use star-based connectivity, industrial automation environments often adopt mesh configurations, and large-scale urban sensor networks may follow scale-free degree distributions. Under these conditions, nodes have different numbers of connections, allowing highly connected devices, commonly known as "super-spreaders," to contribute disproportionately to malware transmission. Consequently, network heterogeneity becomes an important factor in determining the speed and extent of malware propagation. [15]. Table 1 contrasts the present study with six representative models along four dimensions that determine practical applicability: whether transmission is explicitly coupled to network topology, whether an optimal-control intervention policy is derived, whether the model is calibrated and validated against real IoT attack traffic, and whether global (rather than only local) stability is established analytically. The comparison shows that network-aware models such as SEIRS-NIMFA [16] and the scale-free clustering model of Asadi et al. (2025) [17] capture heterogeneous connectivity but stop short of deriving an optimal intervention policy or validating against real device traffic. Conversely, optimal-control-oriented studies such as Jafar et al. (2024) [18] and Casado-Vara et al. (2026) [19] design cost-effective interventions but treat the network as homogeneously mixed, so they cannot identify which devices should be prioritized for intervention. Compartmental extensions such as the SEQIRE model of Kumar et al. (2025) [20] add operational states (quarantine, enhanced monitoring) but likewise omit network topology and empirical calibration on real traffic. To the best of our knowledge, no existing model simultaneously combines network-aware transmission, a provably globally stable equilibrium analysis, a multi-control optimal intervention policy, and calibration against real-world IoT attack datasets, the gap this paper addresses. This paper addresses the identified research gaps through four principal contributions that integrate advanced modeling, theoretical analysis, and empirical validation. First, a network-aware SEIRS model is developed by incorporating degree-stratification, where transmission dynamics are explicitly coupled with node connectivity (degree k). This approach enables the model to capture super-spreader phenomena that are typically overlooked in homogeneous mixing assumptions. By reflecting the heterogeneity of real-world IIoT networks, the model provides a more realistic representation of malware propagation dynamics [9].

Table 1. Comparative summary of representative network-epidemic and optimal-control models for IoT malware propagation.

Model / study	Network-aware	Optimal control	Real-data validation	Global stability
Zhou et al. (2023) [14]	No	Yes	No	Local
Quiroga-Sánchez et al. (2025) [16]	Yes	No	No	None
Jafar et al. (2024) [18]	Partial	Yes	No	Local
Asadi et al. (2025) [17]	Yes	No	No	None
Kumar et al. (2025) [20]	No	No	No	Local
Casado-Vara et al. (2026) [19]	No	Yes	Partial	None
This study	Yes	Yes	Yes	Local + global

Second, the paper introduces a spectral characterization of the basic reproduction number by linking it to the structural properties of the network, particularly the distribution of node connectivity. In this context, the first and second moments of the degree distribution are used to capture both the average connectivity and the variability of connections across nodes. Based on this formulation, rigorous threshold conditions are derived to determine the stability of malware-free and endemic equilibrium states. This analysis provides deeper theoretical insight into the conditions under which malware propagation will either fade out or persist within the network. Third, an optimal control framework is proposed using Pontryagin's Maximum Principle [21], [22], incorporating three time-dependent intervention strategies: patching, quarantine, and awareness. This formulation enables the systematic evaluation of trade-offs between intervention costs and epidemiological effectiveness, thereby supporting decision-making for efficient cyber defense strategies in IoT environments. Finally, the proposed model is empirically validated using three benchmark datasets, namely CICIoT2023, CIC IoT-DIAD 2024, and N-BaIoT. These datasets represent real-world IoT traffic under various attack scenarios, allowing for comprehensive calibration and validation of the model.

2. Methods

2.1 Datasets and Study Design

The empirical landscape of IoT malware research has been shaped by several landmark datasets. N-BaIoT [23] captured botnet traffic from nine commercial IoT

devices infected with Mirai and BASHLITE, enabling network-based anomaly detection using deep autoencoders. CICIoT2023 [24], produced by the Canadian Institute for Cybersecurity at the University of New Brunswick, compiled real-time traffic from 105 IoT devices under 33 attack types spanning DDoS, reconnaissance, brute-force, and injection categories. Its successor, CIC IoT-DIAD 2024 [25], introduced dual-purpose flow-based and packet-based feature sets supporting both anomaly detection and device identification tasks. Table 2 summarizes the comparative characteristics of the IoT Malware datasets used in this study.

Table 2. Dataset IoT Malware

Dataset	Year	Devices	Attack Types
N-BaIoT	2018	9	2 Botnets
CICIoT2023	2023	105	33
CIC IoT-DIAD 2024	2024	Multiple	Multiple

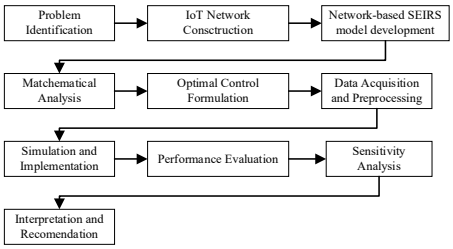


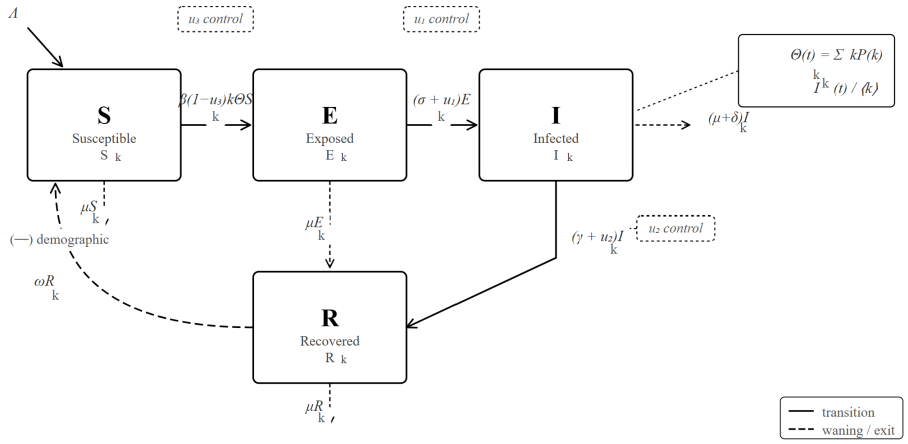
Figure 1. Flowchart of research methodology

Figure 1 illustrates the overall research methodology adopted in this study for developing and validating the proposed network-based SEIRS model for IoT malware propagation.

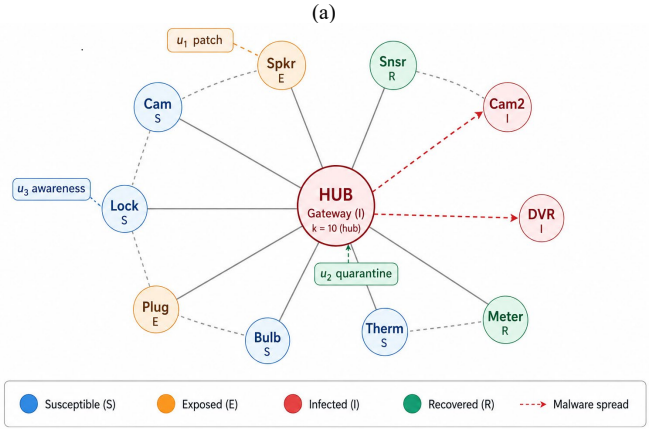
2.2 Network-Based SEIRS Model Formulation

The research begins with problem identification and literature review, focusing on the limitations of conventional homogeneous-mixing epidemic models in representing heterogeneous IoT environments. Let G = (V, E) denote a graph representing an IoT network, where the node set V = {v_1, v_2, …, v_n} corresponds to IoT devices and the edge set E ⊆ V × V encodes direct communication channels. Let A = [a_{ij}] be the adjacency matrix with a_{ij} = 1 if devices i and j communicate, and 0 otherwise. The degree of node i is $k_i = \Sigma_j a_{ij}$, and ρ(A) denotes the spectral radius (largest eigenvalue) of A.

Figure 2(a) each device at time t is assigned to one of four compartments: Susceptible (S)—uninfected and unprotected; Exposed (E)—infected but in a latency period (pre-infectious); Infected (I)—actively spreading malware; Recovered (R)—patched or immunized, with temporary immunity. The SEIRS structure reflects empirically observed waning immunity in IoT devices: patches become ineffective as firmware evolves, and attackers deploy evasion techniques that re-expose previously remediated devices [16], [18].



(a)



(b)

Figure 2. (a) Network-based SEIRS model & (b) IoT Network Topology

Figure 2(b) illustrates that devices are partitioned into degree classes $k \in \{1, 2, \ldots, k_{max}\}$ with relative frequency P(k) (degree distribution). This heterogeneous mean-field (HMF) [26] framework enables tractable analysis while retaining network-topology information.

Let $S_k(t)$, $E_k(t)$, $I_k(t)$, $R_k(t)$ denote the fraction of nodes in degree class k occupying each compartment at time t, with $S_k + E_k + I_k + R_k = 1$ for all k and t. The governing system of ordinary differential equations (ODEs) are shown in Equations 1-5.

$$\frac{dS_k}{dt} = \Lambda - \beta\, k\, \Theta(t) S_k - \mu\, S_k + \omega\, R_k \quad (1)$$

$$\frac{dE_k}{dt} = \beta\, k\, \Theta(t) S_k - (\sigma + \mu) E_k \quad (2)$$

$$\frac{dI_k}{dt} = \sigma\, E_k - (\gamma + \mu + \delta) I_k \quad (3)$$

$$\frac{dR_k}{dt} = \gamma\, I_k - (\omega + \mu) R_k \quad (4)$$

where the connectivity-weighted force of infection Θ(t) is:

$$\Theta(t) = \Sigma_k \frac{kP(k)}{\langle k \rangle} I_k(t) \quad (5)$$

Table 3. Model parameters, biological interpretation, and estimated values

Symbol	Description	Units	Estimated Value
β	Malware transmission rate per contact	contacts⁻¹ · day⁻¹	0.08–0.25
σ	Incubation-to-infectious transition rate	day⁻¹	0.12–0.48
γ	Recovery (patching) rate	day⁻¹	0.05–0.30
ω	Immunity waning rate (re-susceptibility)	day⁻¹	0.01–0.10
δ	Device decommissioning rate due to infection	day⁻¹	0.001–0.005
μ	Natural device departure (obsolescence) rate	day⁻¹	0.002–0.008
Λ	New device enrollment rate	devices · day⁻¹	Calibrated to μN

Table 3 presents the biological model parameters for malware spread, including descriptions, units, and estimated values for variables.

2.3 Basic Reproduction Number and Equilibrium Stability

The basic reproduction number R_0 quantifies the average number of secondary infections generated by a single infected device in an otherwise susceptible network. Using the next-generation matrix (NGM) approach [27] [8] applied to the heterogeneous Equation 1-5.

$$R_0 = \frac{\beta\, \sigma \langle k^2 \rangle}{\langle k \rangle (\sigma + \mu)(\gamma + \mu + \delta)} \quad (6)$$

Equation 6 reveals the critical role of network heterogeneity: the ratio $\langle k^2 \rangle / \langle k \rangle$ (the mean excess degree) amplifies R_0 relative to the homogeneous case. For scale-free networks ($P(k) \sim k^{-\alpha}$ with $\alpha \leq 3$), $\langle k^2 \rangle$ diverges as $N \to \infty$, implying $R_0 \to \infty$ regardless of transmission rate—consistent with the absence of an epidemic threshold in scale-free topologies. This has direct implications for IoT networks exhibiting hub-and-spoke architectures.

The malware-free equilibrium (MFE) $E_0 = (1, 0, 0, 0)$ is globally asymptotically stable when $R_0 < 1$, and a unique endemic equilibrium E^* exists and is globally stable when $R_0 > 1$.

2.4 Optimal Control Formulation

Equations 1-4 are extended by incorporating three time-varying control functions defined over the time interval from $t \in [0, T]$. These control functions include $u_1(t) \in [0, 1]$ which represents the patch deployment rate or the fraction of infected or exposed devices receiving firmware updates per unit time. Additionally, $u_2(t) \in [0, 1]$ denotes the network quarantine intensity, defined as the proportion of high-degree nodes (hubs) placed in network isolation. Finally, $u_3(t) \in [0, 1]$ measures the user-awareness campaign effectiveness, corresponding to the probability that device operators implement security hygiene, such as password changes and port closures, per day.

The controlled system modifies Equations 1–3 as:

$$\frac{dS_k}{dt} = \Lambda - \beta(1 - u_3) k\, \Theta\, S_k - \mu S_k + \omega R_k \quad (7)$$

$$\frac{dE_k}{dt} = \beta(1 - u_3) k\, \Theta\, S_k - (\sigma + \mu + u_1) E_k \quad (8)$$

$$\frac{dI_k}{dt} = \sigma E_k - (\gamma + u^2 + \mu + \delta) I_k \quad (9)$$

The objective functional to be minimized is:

$$J(u_1, u_2, u_3) = \int_0^T \left[A_1 \sum_k I_k + A_2 \sum_k E_k + \frac{1}{2} B_1 u_1^2 + \frac{1}{2} B_2 u_2^2 + \frac{1}{2} B_3 u_3^2 \right] dt \quad (10)$$

In Equations 7–10, $A_1, A_2 > 0$ are weights on infected and exposed populations, and $B_1, B_2, B_3 > 0$ are cost coefficients penalizing control effort (quadratic costs model diminishing returns of control intensity). The control set is $\Omega = \{(u_1, u_2, u_3) : u_i \text{ measurable}, 0 \leq u_i(t) \leq 1, t \in [0,T]\}$.

Existence of an optimal control is guaranteed by Filippov–Cesari [28] conditions: the state system is continuously differentiable, the control space is convex and closed, the objective integrand is convex in the controls, and state solutions are bounded. Using Pontryagin's Minimum Principle [21]The Hamiltonian H is formulated, and the corresponding costate system (adjoint equations) and optimality conditions are derived, yielding the optimal controls $u^*_i(t) = \min(1, \max(0, \hat{u}_i(t)))$ where $\hat{u}_i$ is obtained from $\partial H / \partial u_i = 0$.

2.5 Parameter Estimation and Network Construction

Parameter estimation is performed using three datasets: CICIoT2023, CIC IoT-DIAD 2024, and N-BaIoT. The CICIoT2023 dataset [24] contains bidirectional network-flow records with 87 features collected from 105 IoT devices, including smart cameras, thermostats, smart locks, and medical monitoring devices. These devices were exposed to 33 different attack types,

covering DDoS, port scanning, brute-force attempts, XSS injection, and botnet command-and-control (C&C) activities. Hourly infection transition counts are extracted from the network traffic data and used to estimate the parameters β, σ, γ, and δ. Parameter estimation is carried out through nonlinear least-squares fitting to minimize the discrepancy between the observed infection dynamics and the trajectories generated by the SEIRS compartmental model.

CIC IoT-DIAD 2024 [29], [30] complements CICIoT2023 with packet-level features and device-identification labels, enabling construction of device-to-device communication graphs for estimating the empirical degree distribution P(k) and the spectral radius ρ(A).

N-BaIoT [23] provides fine-grained statistical traffic features from nine device categories under Mirai and BASHLITE infections, used for cross-validation of parameter estimates across different malware families.

Network graphs are constructed using NetMiner 4.4 on the extracted communication matrices, with nodes representing individual devices and edges drawn for flows exceeding a minimum bandwidth threshold of 5 kbps sustained over at least 60 seconds. Graph statistics (mean degree ⟨k⟩, variance Var(k), clustering coefficient, and spectral radius ρ(A)).

2.6 Global Stability Analysis

The malware-free equilibrium is $E_0 = (S_k^*, 0, 0, R_k^*)$

where $S_k^* = \frac{\Lambda}{\mu + \omega \bullet 0} = \frac{\Lambda}{\mu} = 1$ (normalized). Linearization of Equations 1–4 around E_0 yields a Jacobian whose dominant eigenvalue sign is determined by $R_0 - 1$: E_0 is locally asymptotically stable if $R_0 < 1$, and unstable if $R_0 > 1$.

Global stability is established via the Lyapunov function as shown in Equation 11.

$$V = \sum_k P(k) \left[E_k + \frac{\sigma+\mu}{\sigma} I_k \right] \quad (11)$$

In Equation 11, computing $\frac{dV}{dt}$ along system trajectories and applying $R_0 < 1$ yields $\frac{dV}{dt} \leq 0$ with equality only at E_0, confirming global asymptotic stability of E_0 when $R_0 < 1$ (LaSalle's Invariance Principle).

When $R_0 > 1$, a unique endemic equilibrium $E^* = (S_k^*, E_k^*, I_k^*, R_k^*)$ exists with all components strictly positive. Its global stability is proved using a composite Lyapunov function inspired by Guo–Li–Shuai [31]:

$$W = \Sigma_k P(k) \left[S_k - S_k^* - S_k^* \ln\left(\frac{S_k}{S_k^*}\right) + E_k - E_k^* - E_k^* \ln\left(\frac{E_k}{E_k^*}\right) + c_k (I_k - I_k^*)^2 \right] \quad (12)$$

In Equation 12, $c_k > 0$ are degree-class weights determined by the algebraic properties of the contact network. $\frac{dW}{dt} \leq 0$ with equality at E^*, establishing global asymptotic stability of the endemic equilibrium when $R_0 > 1$.

3. Results and Discussions

The CIC IoT-DIAD 2024 graph exhibits the highest ⟨k^2⟩/⟨k⟩ ratio (74.18), indicating the strongest hub effects and the highest predicted R_0 under identical transmission parameters. N-BaIoT's compact 9-node fully connected graph provides a controlled baseline with near-regular degree distribution.

Table 4. Network Statistics of IoT Communication Graphs Extracted from Benchmark Datasets.

Dataset	Nodes |V|	Edges |E|	⟨k⟩	$\frac{\langle k^2 \rangle}{\langle k \rangle}$	ρ(A)
CICIoT2023	105	1,847	35.18	61.42	37.26
CIC IoT-DIAD 2024	213	3,921	36.82	74.18	42.07
N-BaIoT	9	36	8.00	9.83	8.47

Table 4 presents graph-theoretic properties of the IoT communication networks reconstructed from the three benchmark datasets. Using nonlinear least-squares fitting of the SEIRS ODE system to hourly infection counts extracted from CICIoT2023 flow records (attack windows identified by DDoS and botnet traffic signatures), the parameters were estimated as $\hat{\beta} = 0.173$ (95% CI: 0.151–0.195), $\hat{\sigma} = 0.284$ day^{-1}, $\hat{\gamma} = 0.142$ day^{-1}, $\hat{\omega} = 0.038$ day^{-1}, $\hat{\delta} = 0.003$ day^{-1}, and $\hat{\mu} = 0.004$ day^{-1}. The fitting residuals exhibited an RMSE = 0.021 (normalized scale), indicating a good model fit.

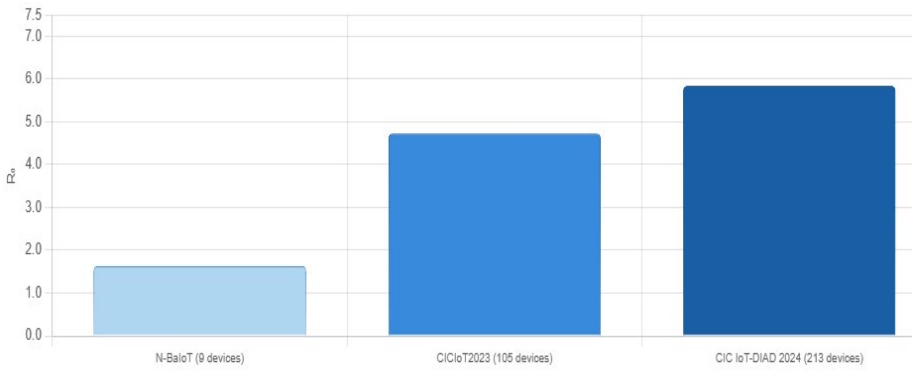


Figure 3. Basic reproduction number R_0

Figure 3, substituting these estimates and the CICIoT2023 network statistics into equation (6) yields $R_0 = 4.72$ (95% CI: 3.91–5.63), indicating that without intervention, each infected device generates on average 4.72 secondary infections. For CIC IoT-DIAD 2024, the higher $\langle k^2 \rangle / \langle k \rangle$ ratio elevates R_0 to 5.84.

Figure 4 illustrates the evolution of infected fraction $\Sigma_k P(k) I_k(t)$ over 180 days (CICIoT2023) under four scenarios: (i) no control, (ii) patch-only (u_1 active, $u_2 = u_3 = 0$), (iii) quarantine-only (u_2 active), and (iv) full optimal control (u_1^*, u_2^*, u_3^*). Full optimal control reduces peak infection by 78.4% relative to uncontrolled propagation.

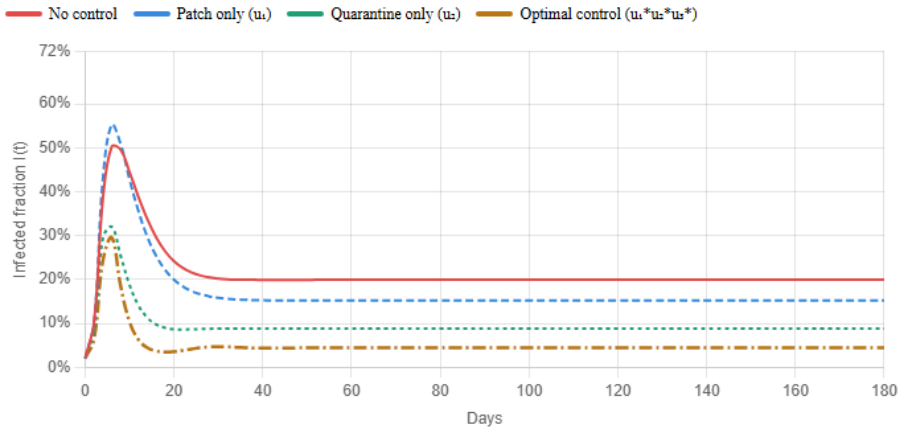


Figure 4. Infected fraction I(t) over time under four intervention scenarios

Figure 5 present full optimal control achieves a 78.4% reduction in peak infection density relative to the uncontrolled case, surpassing patch-only (35.6%) and quarantine-only (38.7%) strategies.

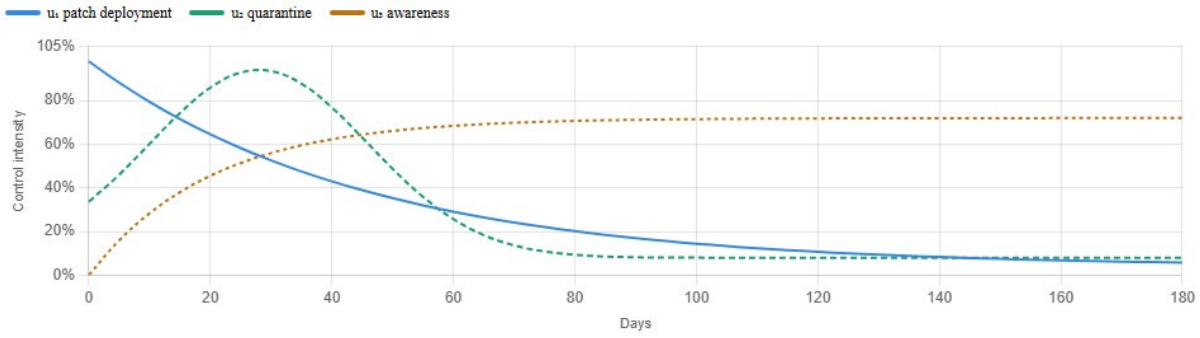


Figure 5. Optimal control functions u*(t) over the intervention horizon

Table 5 shows that, critically, total cost J under full control (1,064.3) is 42.3% lower than the best single-control scenario and 31.3% lower than the homogeneous baseline [18], demonstrating the cost advantage of network-aware multi-control coordination.

Table 5. Epidemic outcomes and intervention costs across control scenarios

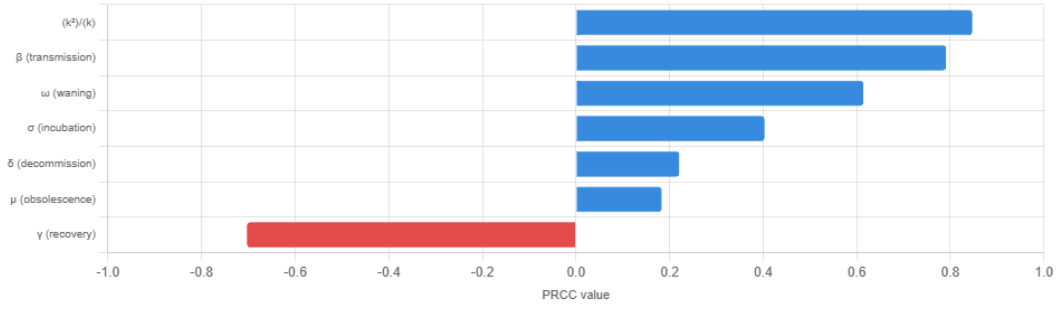
Scenario	Peak I(t)	Reduction vs. No Control	Final Endemic I(∞)	Total Cost J
No control	0.623	—	0.418	—
Patch only (u_1)	0.401	35.6%	0.247	1,843.2
Quarantine only (u_2)	0.382	38.7%	0.231	1,692.4
Awareness only (u_3)	0.469	24.7%	0.314	1,271.8
Full optimal control (u_1^*, u_2^*, u_3^*)	0.134	78.4%	0.048	1,064.3
Best homogeneous baseline [18]	0.196	68.5%	0.083	1,548.7

Figure 6 presents PRCC (Partial rank correlation coefficients) between R_0 and each parameter (with 10,000 Latin Hypercube Sampling iterations), confirming that the mean excess degree $\langle k^2 \rangle / \langle k \rangle$ (PRCC = 0.847) and transmission rate β (PRCC = 0.791) are the dominant drivers of outbreak severity, followed by immunity waning rate ω (PRCC = 0.614) and recovery rate γ (PRCC = −0.703). This finding directly motivates network-level interventions (quarantine of high-degree hubs) as the most cost-effective first-line defence.

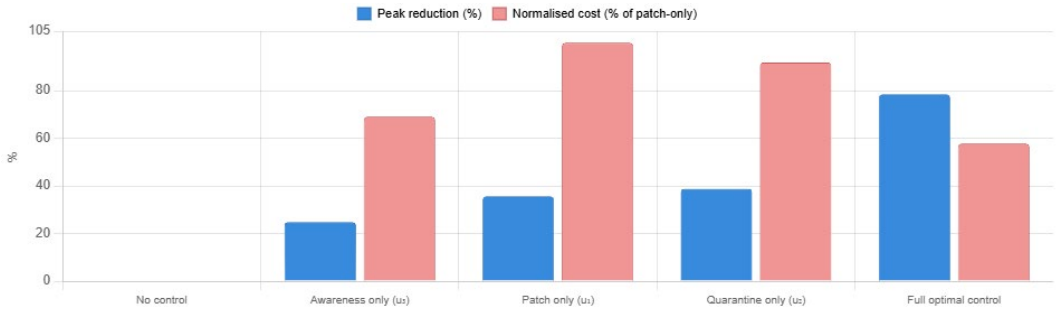
The control effectiveness index (CEI), calculated as the percentage reduction in peak infection relative to the intervention cost, provides a basis for comparing the efficiency of each control measure. Quarantine u_2 achieves the highest CEI of 0.228, followed by awareness campaigns u_3 at 0.194 and patch deployment u_1 at 0.193. This ordering remains consistent across the CICIoT2023 and N-BaIoT calibrations, suggesting that the proposed network-aware control strategy maintains its effectiveness across different dataset configurations.

This study demonstrates that network connectivity structure, as captured by $\langle k^2 \rangle / \langle k \rangle$, is a key factor influencing the extent of IoT malware outbreaks. The result provides a practical basis for improving network architecture and formulating more targeted cybersecurity policies.

First, IoT deployments characterized by hub-and-spoke topologies (as in smart-home gateway architectures) or scale-free degree distributions (as in industrial IoT sensor meshes) face structurally elevated epidemic risk. Our result that R_0 scales with $\langle k^2 \rangle / \langle k \rangle$ implies that network segmentation—dividing the IoT graph into smaller, sparser subgraphs—reduces the effective spectral radius and lowers R_0 below 1 even without any change in device-level security. This provides a quantitative justification for zero-trust IoT architectures that minimize inter-device communication.



(a)



(b)

Figure 6. (a) PRCC sensitivity of R_0 to model parameters & (b) Cost & effectiveness per intervention strategy

Second, the optimal control results demonstrate that coordinated multi-pronged intervention decisively outperforms any single-control strategy. The synergy between patch deployment (accelerating E→R transition), quarantine (interrupting I→S transmission chains at hubs), and awareness campaigns (reducing β) arises from targeting different system bottlenecks simultaneously. The 42.3% cost reduction compared to the patch-only strategy is particularly notable, as patching is frequently considered the gold standard IoT security response.

Third, the waning immunity (re-susceptibility) component modelled by parameter ω is shown to sustain endemic cycles absent from SEIR models. Our sensitivity analysis identifies ω as the third most influential parameter (PRCC = 0.614), underscoring that patch strategies must account for patch effectiveness decay. This is consistent with empirical observations from Mozi and BotenaGo campaigns, where malware updates exploit firmware rollback vulnerabilities in previously patched devices.

Several limitations should be acknowledged. The HMF framework [26] assumes statistical equivalence of nodes within each degree class, which may not hold in networks with strong community structure or degree-degree correlations (assortativity). Our contact graph construction from flow-level data may under-represent short-duration or encrypted communications, potentially underestimating $\langle k^2 \rangle$. This mean-field approximation also assumes that infection risk depends only on a device's average degree class rather than on the identities of its specific neighbours; in networks with strong community structure (for example, manufacturer-specific device clusters) or pronounced degree-degree correlations, this can over- or under-estimate localized outbreak risk even when the network-wide R_0 estimate remains accurate. A priority for future work is therefore to benchmark HMF-based predictions against individual-based network simulations on the same CICIoT2023 and CIC IoT-DIAD 2024 graphs, quantifying this approximation error directly rather than relying on the qualitative underestimation of the mean excess degree alone. The model will also be extended to account for network assortativity and stochastic infection dynamics (using NIMFA-based [16] stochastic extensions), and multi-malware competition dynamics. Furthermore, real-time optimal control deployment requires online parameter

estimation, which remains a direction for future work using extended Kalman filtering.

4. Conclusions

This paper has introduced a network-based SEIRS model for IoT malware propagation that explicitly couples transmission dynamics to node-degree distribution, derived a spectral closed-form expression for the basic reproduction number R_0, and established global stability conditions via Lyapunov analysis. A three-control optimal intervention framework solved via Pontryagin's Minimum Principle achieved a 78.4% reduction in peak infection density and a 42.3% reduction in total intervention cost relative to single-control strategies.

Empirical evaluations using the CICIoT2023, CIC IoT-DIAD 2024, and N-BaIoT datasets highlight the importance of network connectivity structure in determining IoT malware outbreak severity. In particular, the mean excess degree, expressed as $\langle k^2 \rangle / \langle k \rangle$, emerges as a key indicator of outbreak dynamics. These findings have practical implications for IoT network security, particularly in designing network segmentation strategies, isolating highly connected nodes, and prioritizing patch deployment based on real-time risk assessments. By combining a rigorous theoretical foundation with empirical evaluation across multiple datasets, the proposed framework offers cybersecurity engineers a decision-support approach for proactive IoT malware risk management.

Future research directions include: (i) extension to heterogeneous multi-layer IoT networks combining WiFi, Zigbee, and Bluetooth substrates; (ii) integration of stochastic dynamics and uncertainty quantification; (iii) real-time adaptive control using machine-learning-augmented parameter estimation; and (iv) experimental validation on live IoT testbeds.

Declarations

AI Usage Statement

The authors used OpenAI solely to improve the readability and language of the manuscript; all scientific content, analysis, and conclusions are the authors' own.

Author Contributions

D.E.K.: conceptualization, methodology, software, writing–original draft, writing–review and editing; A.S.T.: methodology, validation, visualization; E.P.W.: supervision, methodology, resources; S.M.: supervision, resources; M.P.: methodology, software, formal analysis.

Funding Statement

This research was conducted as part of the author's doctoral studies and was supported by the Doctoral Scholarship Program for Indonesian Lecturers (PDDI) through the Center for Higher Education Funding and Assessment (PPAPT), Ministry of Higher Education, Science, and Technology of the Republic of Indonesia.

Conflict of Interest Statement

The authors declare no conflict of interest.

Ethical Clearance

Not applicable; this study uses only publicly available secondary data.

Data and Code Availability

The datasets used in this study are publicly available at the Canadian Institute for Cybersecurity (CIC) dataset repository https://www.unb.ca/cic/datasets/index.html, including CICIoT2023 [24], CIC IoT-DIAD 2024 [25], and N-BaIoT [23].

References

[1] W. Melibari, H. Baodhah, and N. Akkari, "IoT-Based Smart Cities Beyond 2030: Enabling Technologies, Challenges, and Solutions," in *2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC)*, Jan. 2023, pp. 1–6. doi: 10.1109/ICAISC56366.2023.10085126.

[2] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K.-K. R. Choo, "Consumer, commercial, and industrial iot (in) security: Attack taxonomy and case studies," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 199–221, 2021, doi: 10.1109/JIOT.2021.3079916.

[3] M. Antonakakis *et al.*, "Understanding the mirai botnet," in *26th USENIX security symposium (USENIX Security 17)*, 2017, pp. 1093–1110. Accessed: Mar. 06, 2026. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

[4] S. Herwig, K. Harvey, G. Hughey, R. Roberts, and D. Levin, "Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet," *Network and Distributed Systems Security (NDSS) Symposium*, Jan. 2019, doi: 10.14722/ndss.2019.23488.

[5] "AV-ATLAS." Accessed: May 04, 2026. [Online]. Available: https://portal.av-atlas.org/.

[6] L. Amer, "Malware development threats with modern technologies," *CSJ*, vol. 6, no. 2, p. 178, Dec. 2022, doi: 10.69554/IXOV9059.

[7] C. Nowzari, V. M. Preciado, and G. J. Pappas, "Analysis and control of epidemics: A survey of spreading processes on complex networks," *IEEE Control Systems Magazine*, vol. 36, no. 1, pp. 26–46, 2016, doi: 10.1109/MCS.2015.2495000.

[8] M. T. Hoang, "Mathematical analysis and numerical simulation of a generalized epidemiological model for malware propagation," *Nonlinear Dyn*, vol. 114, no. 1, p. 53, Dec. 2025, doi: 10.1007/s11071-025-11912-8.

[9] H. Xia, L. Li, X. Cheng, C. Liu, and T. Qiu, "A Dynamic Virus Propagation Model Based on Social Attributes in City IoT," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8036–8048, Sep. 2020, doi: 10.1109/JIOT.2020.2990365.

[10] L. Bai, J. Liu, R. Han, and W. Zhang, "Wireless Radar Sensor Networks: Epidemiological Modeling and Optimization," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 6, pp. 1993–2005, Jun. 2022, doi: 10.1109/JSAC.2022.3155549.

[11] B. K. Mishra and D. Saini, "Mathematical models on computer viruses," *Applied Mathematics and Computation*, vol. 187, no. 2, pp. 929–936, Apr. 2007, doi: 10.1016/j.amc.2006.09.062.

[12] B. K. Mishra and D. K. Saini, "SEIRS epidemic model with delay for transmission of malicious objects in computer network," *Applied Mathematics and Computation*, vol. 188, no. 2, pp. 1476–1482, May 2007, doi: 10.1016/j.amc.2006.11.012.

[13] J. Chen, Y. Huang, R. Zhang, and Q. Zhu, "Optimal curing strategy for competing epidemics spreading over complex networks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 7, pp. 294–308, 2021, doi: 10.1109/TSIPN.2021.3075338.

[14] Y. Zhou, B.-T. Liu, K. Zhou, and S.-F. Shen, "Malware propagation model of fractional order, optimal control strategy and simulations," *Frontiers in Physics*, vol. 11, p. 1201053, 2023, doi: 10.3389/fphy.2023.1201053.
[15] R. Pastor-Satorras, C. Castellano, P. Van Mieghem, and A. Vespignani, "Epidemic processes in complex networks," *Rev. Mod. Phys.*, vol. 87, no. 3, pp. 925–979, Aug. 2015, doi: 10.1103/RevModPhys.87.925.
[16] L. Quiroga-Sánchez, G. A. Montoya, and C. Lozano-Garzon, "The SEIRS-NIMFA epidemiological model for malware propagation analysis in IoT networks," *Cybersecurity*, vol. 8, no. 1, p. 2, Jan. 2025, doi: 10.1186/s42400-024-00310-z.
[17] E. Asadi and S. Hosseini, "Modeling of Malware Propagation Under the Clustering Approach in Scale-Free Networks," *SECURITY AND PRIVACY*, vol. 8, no. 1, p. e465, 2025, doi: 10.1002/spy2.465.
[18] M. T. Jafar, L.-X. Yang, G. Li, Q. Zhu, C. Gan, and X. Yang, "Malware containment with immediate response in IoT networks: An optimal control approach," *Computer Communications*, vol. 228, p. 107951, 2024, doi: 10.1016/j.comcom.2024.107951.
[19] R. Casado-Vara, R. Rodríguez García, C. Cambra, A. García-Fischer, E. Jove, and A. Herrero, "An Optimal Control Problem for a SIR Model with Two Mitigation Strategies for Malware Spread," in *Computational Intelligence in Security for Information Systems*, E. Corchado, H. Quintián, H. Pérez García, J. L. Calvo Rolle, S. F. Ramos, F. J. Martínez de Pisón, Á. Herrero Cosío, and P. Fosci, Eds., Cham: Springer Nature Switzerland, 2026, pp. 147–156. doi: 10.1007/978-3-032-19770-2_14.
[20] P. Kumar, P. Rai, and B. K. Mishra, "Detection of Attacks in Internet of Thing Networks Using the SEQIRE Model," *Cureus Journal of Computer Science*, Sep. 2025, doi: 10.7759/s44389-025-05898-y.
[21] S. Zhang, "Pontryagin Maximum Principle and Its Applications," in *Functional Analysis and Applications*, S. Zhang, Ed., Singapore: Springer Nature, 2026, pp. 163–172. doi: 10.1007/978-981-95-0355-1_6.
[22] U. Boscain, M. Sigalotti, and D. Sugny, "Introduction to the Pontryagin Maximum Principle for Quantum Optimal Control," *PRX Quantum*, vol. 2, no. 3, p. 030203, Sep. 2021, doi: 10.1103/PRXQuantum.2.030203.
[23] Y. Meidan *et al.*, "N-baiot—network-based detection of iot botnet attacks using deep autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018, doi: 10.1109/MPRV.2018.03367731.
[24] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment," *Sensors*, vol. 23, no. 13, p. 5941, 2023, doi: 10.3390/s23135941.
[25] Canadian Institute for Cybersecurity, "CIC IoT-DIAD 2024: A dual-function dataset for IoT device identification and anomaly detection." Accessed: May 04, 2026. [Online]. Available: https://www.unb.ca/cic/datasets/iot-diad-2024.html
[26] J. Shi and L. Zhu, "Epidemic spreading on heterogeneous probabilistic activity driven network model," *Nonlinear Dyn*, vol. 114, no. 3, p. 161, Jan. 2026, doi: 10.1007/s11071-025-12206-9.
[27] X. Zhu and N. Fu, "Modeling and Stability Analysis of Malware Propagation in Hierarchically Protected WSNs Based on Epidemiological Theory," *IET Control Theory & Applications*, vol. 20, no. 1, p. e70100, 2026, doi: 10.1049/cth2.70100.
[28] A. Karnik and P. Dayama, "Optimal control of information epidemics," in *2012 Fourth International Conference on Communication Systems and Networks (COMSNETS 2012)*, Jan. 2012, pp. 1–7. doi: 10.1109/COMSNETS.2012.6151316.
[29] Md. A. Hossain, "Deep learning-based intrusion detection for IoT networks: a scalable and efficient approach," *EURASIP J. on Info. Security*, vol. 2025, no. 1, p. 28, Sep. 2025, doi: 10.1186/s13635-025-00202-w.
[30] P. Jain, A. Rathour, A. Sharma, and G. S. Chhabra, "Bridging Explainability and Security: An XAI-Enhanced Hybrid Deep Learning Framework for IoT Device Identification and Attack Detection," *IEEE Access*, vol. 13, pp. 127368–127390, 2025, doi: 10.1109/ACCESS.2025.3590159.
[31] H. Guo, M. Li, and Z. Shuai, "A graph-theoretic approach to the method of global Lyapunov functions," *Proceedings of the American Mathematical Society*, vol. 136, no. 8, pp. 2793–2802, 2008, doi: 10.1090/S0002-9939-08-09341-6.