Scilight

Journal of Machine Learning and Information Security
https://www.sciltp.com/journals/jmlis

Article

A Dynamic Countermeasure-Based Worm Propagation Model in Wireless Sensor Networks: Critical Threshold Analysis and Validation of Benign Worm Effectiveness

Liping Feng *, Yaojun Hao, Qinshan Zhao and Peng Wei

Computer Science Department, Xinzhou Normal University, Xinzhou 034000, China
* Correspondence: fenglp@yeah.net

How To Cite: Feng, L.; Hao, Y.; Zhao, Q.; et al. A Dynamic Countermeasure-Based Worm Propagation Model in Wireless Sensor Networks: Critical Threshold Analysis and Validation of Benign Worm Effectiveness. *Journal of Machine Learning and Information Security* **2025**, *1*(1), 2.

Received: 8 July 2025
Revised: 2 September 2025
Accepted: 15 September 2025
Published: 24 September 2025

Abstract: In this paper, we propose an innovative i-SIR model to characterize the co-propagation dynamics of malicious worms ("bad worms") and defensive worms ("good worms") in wireless sensor networks (WSNs)—where "bad worms" refer to malware that invades sensor nodes to steal data, disrupt communication, or paralyze network functions, while "good worms" are benign programs designed to repair infected nodes, block "bad worm" intrusion, and build immune barriers. The model is designed to comprehensively analyze worm spread and its countermeasures in the complex and resource-constrained WSN environments, especially addressing the critical threat of "bad worms": in WSNs widely used for environmental monitoring, industrial control, and smart agriculture, "bad worm" outbreaks can lead to irreversible data loss, large-scale node failure, and even cascading damage to physical systems connected to the network. Through rigorous mathematical analysis, we derive the basic reproduction number R0, which serves as a critical threshold determining the extinction or persistence of worm propagation, and further explore its sensitivity to key network parameters such as node density, communication range, and energy constraints that are inherent to WSNs. Numerical simulations confirm the theoretical validity of R0 and demonstrate that the i-SIR model is superior to classical statistical immune models in controlling both the speed and scale of worm outbreaks—specifically, it reduces the worm outbreak speed by 50% and curbs the final infection scale by 60%. Furthermore, we investigate the impact of the infection rate ratio between bad and good worms on propagation dynamics, considering temporal variations in worm activity patterns. Results reveal that reducing the infection rate ratio between bad and good worms significantly suppresses the virulence and the scale of malicious worm spread, with more pronounced effects in densely deployed networks. This work provides a robust theoretical foundation for designing dynamic defense strategies in WSNs, highlighting the efficacy of deploying benign worms as active countermeasures against cyber-physical threats and offering performable insights for optimizing the timing and density of good worm deployment in real-world sensor network operations.

Keywords: wireless sensor network; stability; worm propagation model; countermeasures

1. Introduction

Wireless sensor networks (WSNs) have emerged as a cornerstone of modern distributed sensing systems, celebrated for their cost-efficiency, structural simplicity, and seamless deployability across diverse environments. Comprising hundreds to thousands of miniature sensor nodes, these networks are uniquely positioned to operate in harsh or remote settings—such as deep forests, disaster-stricken areas, or battlefield zones—where conventional wired infrastructure is impractical to install. Equipped with sensing, computing, and wireless communication capabilities, each node collaboratively monitors and records environmental parameters (e.g., temperature, humidity, motion, or chemical concentrations) before relaying aggregated data to a central base station for analysis [1]. This decentralized architecture has propelled WSNs into a myriad of critical applications, spanning both civilian and defense domains. In intelligent transportation systems, for instance, WSNs enable real-time traffic flow monitoring, collision avoidance, and adaptive signal control; in perimeter security, they detect unauthorized intrusions with high precision; in forest fire prevention, they provide early warnings by tracking microclimatic changes; and in logistics, they facilitate Cognitive Supply Orchestration by optimizing resource allocation in uncharted terrains [2–4]. Beyond these, WSNs also play pivotal roles in environmental conservation (e.g., wildlife tracking), industrial automation (e.g., predictive maintenance), and healthcare (e.g., remote patient monitoring), underscoring their versatility and societal impact.

As WSNs continue to scale in size and adopt heterogeneous connectivity frameworks—integrating with 5G, IoT, and edge computing—they have become increasingly vulnerable to cyber threats, with systemic security gaps emerging as prime targets for malicious actors [5]. A key vulnerability stems from the inherent resource constraints of sensor nodes: limited battery life, modest processing power, and constrained memory. These limitations severely weaken their defensive capabilities, making them highly susceptible to worm attacks—self-replicating malware that can rapidly propagate through the network. Worm propagation in WSNs is particularly insidious: once a node is compromised, it transforms into a malicious hub, disseminating malware to adjacent nodes via wireless communication links. This process follows epidemic-like dynamics, where the infection spreads exponentially until it reaches a critical threshold, potentially contaminating the entire network and disabling critical functionalities [6,7]. Consequently, developing quantitative models to characterize worm propagation and designing robust, lattice-based defense mechanisms are imperative to ensuring the cyber resilience of WSNs [8].

The similarity between worm propagation in WSNs and biological epidemic spread has long been recognized, prompting researchers to adapt classical epidemic models to analyze malware dynamics. In these frameworks, sensor nodes transition through distinct states analogous to epidemiological categories: Susceptible (S) nodes are vulnerable but not yet infected; Infected (I) nodes are compromised and actively propagate the worm; and Recovered (R) nodes are either cured (e.g., via antivirus measures) or rendered non-functional (e.g., due to energy depletion). Since seminal works by Kermack and McKendrick [9], which laid the foundation for epidemic modeling, scholars have employed stochastic differential equations and agent-based simulations to quantify malware propagation in various network topologies [10–16]. These studies have clarified key factors influencing worm spread, such as transmission rate, network density, and node mobility, providing a theoretical basis for understanding WSN vulnerabilities.

Notably, researchers have adapted these models to address the unique characteristics of WSNs. Wang et al., for example, proposed an improved SIR model that incorporates node energy constraints—a critical factor in WSNs [17], where nodes rely on finite batteries. In their framework, infected nodes gradually exhaust energy as they propagate the worm, eventually being "removed" from the network once their power is depleted. Their simulations demonstrated that worm propagation is highly sensitive to energy consumption rates: nodes with faster energy depletion slow the infection spread but also reduce network lifetime, highlighting a trade-off between security and operational longevity. Similarly, Ahmad et al. developed a modified virus propagation model for WSNs [18], leveraging fixed-point theorems to prove the existence and uniqueness of solutions, and deriving Lyapunov stability conditions to assess model robustness. Their work revealed that small perturbations in parameters (e.g., infection rate) can lead to bifurcations—sudden shifts in system behavior—emphasizing the need for adaptive defense strategies.

Beyond propagation modeling, recent studies have explored complementary aspects of WSN security. Angurala et al. introduced the MRCRLB (Magnetic Resonant Coupling Based Recharging and Load Balancing) scheme [19], which addresses energy inefficiency and battery constraints by enabling wireless recharging, thereby indirectly enhancing security by prolonging node functionality. Premkumar et al. focused on denial-of-service (DoS) attacks [20], developing a lightweight deep learning model to detect anomalies in data routing—critical given the lack of node synchronization in WSNs. Moslehi et al. integrated coverage and security analysis [21], showing that node deployment strategies (e.g., uniform vs. clustered) significantly impact both sensing range and

vulnerability to attacks. Meanwhile, Kovtun et al. enhanced epidemic forecasting accuracy by incorporating stochastic parameters and noise optimization into SIR models [22], reducing prediction errors compared to classical methods and improving proactive defense planning.

Despite these advancements, a critical gap remains: the dynamic interplay between attack and defense strategies in WSNs. Existing models assume static antivirus measures (e.g., pre-deployed firewalls or periodic scans), but in reality, worm propagation and defense form a continuous, adaptive game. Worms evolve to bypass defenses, while security measures must dynamically adjust to counter new threats. This challenge is exacerbated in WSNs, where nodes are often deployed in uncharted or inaccessible areas—such as post-disaster rubble or remote deserts—making it nearly impossible to manually update countermeasures [23]. Wireless updates, though feasible, are risky: they consume limited energy, can be intercepted by attackers, or fail in low-connectivity regions. Consequently, there is an urgent need for self-sustaining, dynamic defense mechanisms that can propagate and adapt alongside emerging threats.

This study addresses this gap by proposing a novel computational framework that models worm propagation in WSNs while integrating the dynamics of "good worms"—benign, self-replicating agents designed to neutralize malicious worms. Unlike static defenses, these good worms propagate through the network autonomously, adjusting their spread based on real-time infection rates, node energy levels, and connectivity patterns. By treating defense as an active, propagating process, our model captures the co-evolution of attack and defense, providing insights into how to optimize good worm deployment for maximum network resilience.

The remainder of this paper is structured as follows: Section 2 introduces a new infection function that accounts for WSN-specific factors (e.g., node density, residual energy, and communication range) and presents the improved SIR (i-SIR) model, which integrates both malicious and good worms. Section 3 analyzes the long-term stability of the i-SIR model using Lyapunov stability theory and eigenvalue analysis, identifying conditions under which the network can achieve an infection-free equilibrium. Section 4 presents empirical results from simulations, comparing the i-SIR model with classical SIR and Wang's model across metrics such as infection peak time, network survival rate, and energy efficiency. Finally, Section 5 summarizes key findings, discusses limitations, and outlines future work—including the integration of machine learning for adaptive good worm behavior.

2. The improved Epidemiological Compartmental Model (i-SIR)

This section introduces an enhanced computational framework, which extends the classical SIR (Susceptible-Infected-Recovered) model originally established in epidemiological research [24]. Specifically, we commence by formalizing the four compartmental states and their transition mechanisms within the i-SIR architecture. Next, a transmission function incorporating nonlinear interaction dynamics is rigorously derived. The model is ultimately governed by a system of ordinary differential equations, mathematically encoding its epidemiological behavior [25].

2.1. Epidemiological Compartments and Their Transition Mechanisms in the i-SIR Framework

WSNs fundamentally exhibit a discrete network topology composed of nodes (sensor nodes) and edges (wireless communication channels). During communication, these nodes can transition among four discrete states within the defined state space, each tailored to capture the nuanced dynamics of worm propagation and defense in resource-constrained sensor environments. These states—Susceptible (S), Infected by Bad Worms (I_A), Infected by Good Worms (I_B), and Dead (D)—form a closed system where nodes are continuously redistributed based on interactions, energy levels, and defensive strategies.

(1) S (Susceptible) state: Nodes in the S state are pristine, having not yet been infected by any worm, but lack endogenous worm prevention mechanisms such as pre-installed security patches or real-time monitoring programs. In the threat landscape of WSNs, such nodes are primary targets for "bad worms".

(2) I_A (State-1-Infected): In this state, compromised nodes by "bad worms" exhibit active propagation vectors, capable of contaminating up to susceptible nodes through worm payload replication.

(3) I_B (State-2-Infected): Nodes in the I_B state are embedded with benign propagation vectors (i.e., "good worms") that actively deploy security patches to neighboring nodes in each time epoch. Unlike I_A-state nodes, the behavior of I_B-state nodes is self-limiting: they prioritize evaluating the status of neighboring nodes, sending patches only to S or I_A-state nodes.

(4) D (Dead) state: Nodes in the D state are permanently non-operational due to complete energy exhaustion. The battery capacity of sensor nodes is typically between 100–500 mAh, and their lifespan is generally 3–12 months under continuous communication, but I_A or I_B-state nodes may deplete energy within 1–4 weeks due to high-intensity activities. After entering the D-state, nodes no longer participate in any network activities, cannot be infected, nor can they propagate any worms. Their physical location may still affect network topology (such as

causing communication link interruptions), but is regarded as a "network hole" in the model. Notably, the proportion of *D*-state nodes is a key indicator for evaluating network health: when more than 30% of nodes die, WSNs typically experience coverage blind spots and communication delays.

Initially, all nodes in the WSN are in the S state, with a small number (usually set to 1–5% of the total nodes) seeded as I_A nodes to simulate initial worm intrusion. State transitions follow probabilistic rules shaped by network dynamics:

(1) Transition from *S* to I_A: This occurs when a susceptible node receives a malicious payload from an I_A node.The probability of this transition in each time step is determined by the formula $P(S \rightarrow I_A)$.

(2) Transition from *S* or I_A to I_B: Triggered by the deployment of "good worms," this transition has two modes. For $S \rightarrow I_B$: When an I_B node detects an unprotected *S* node, it sends a security patch with a success probability, depending on the integrity of patch transmission. For $I_A \rightarrow I_B$: "Good worms" need to neutralize the malicious payload first, with a lower success rate, and may trigger defensive mechanisms of I_A nodes (such as worm variants). The activity strategy of "good worms" adopts an intermittent mode: working for 10 min and sleeping for 5 min to balance defense effectiveness and energy consumption, which can extend the lifespan of I_B nodes by 2–3 times compared to continuous operation.

(3) Transition to D state: Nodes in *S*, I_A, or I_B states transition to *D* when their energy drops to 0.

These transitions form a dynamic equilibrium: In the early stage of infection, I_A nodes show exponential growth; as I_B nodes spread, the growth of I_A nodes is inhibited; ultimately, the network may stabilize in a low-infection state (I_B nodes dominate) or collapse (excessive proportion of *D* nodes), depending on the effectiveness ratio between "good worms" and "bad worms." Figure 1 visualizes this tetrahedral state space, with edge weights representing transition probabilities and arrow thickness indicating the frequency of state changes in typical scenarios.

2.2. State Migration Probabilities

In Figure 1, A indicates the number of new sensor nodes, and μ reflects dead rate of nodes. Note that all parameters remain time-invariant except for $\vartheta(t)$, i.e., the pathogen transmission function serves as the principal determinant quantifying malware dissemination efficacy across wireless sensor topologies.

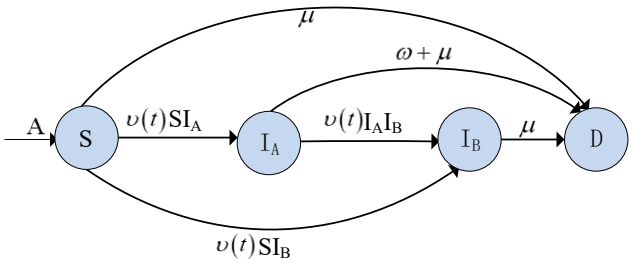

Figure 1. State machine for nodes in WSNs.

To portray the pathogen transmission function, define network topology $G(V,E)$ where vertex set $|V| = N$ represents edge computing nodes with embedded environmental sensors. The nodes are homogeneously distributed in the operational terrain, and the wireless propagation radius of every node is *r*. The network topology of a WSN is depicted in Figure 2.

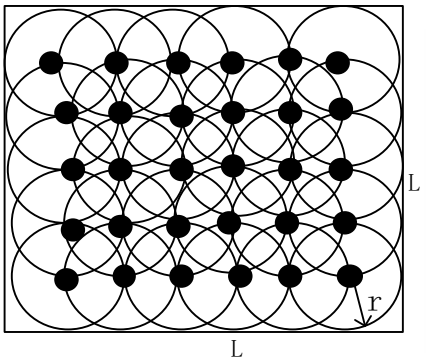

Figure 2. The network topology of an LXL WSN.

Given that: (1) the distribution of *S*-state nodes in the WSN is homogenous, (2) I_A and I_B have different worm spread efficiency due to different routing table information for communication among nodes, and spread efficiency is $\eta_i (i = A, B)$. So, the increased number of I_i-state ($i = A, B$) nodes transited from state *S* in a very short period $\triangle t$ can be derived as [26]

$$\Delta SI_i = \eta_i I_i \rho \Delta t, \tag{1}$$

where ρ is the average communication ratio of the *S*-state nodes among all nodes. Then we can rewrite Equation (1) by further exploring the properties of the WSN. The coverage footprint of a network entity is mathematically represented by S_r, and the density of infection-prone devices in a sensing grid in a WSN is parameterized via $p(t)$. Then the following equations hold:

$$\begin{aligned} p(t) &= \frac{S(t)}{L^2}, \\ S_r &= \pi r^2, \\ \rho &= S_r p(t). \end{aligned} \tag{2}$$

From Equation (2), we can get

$$\rho = \frac{\pi r^2}{L^2} S(t). \tag{3}$$

Moreover, it is noteworthy that not all the nodes are active for energy saving. $\beta_i (i = A, B)$ represents the averaged active ratio of the nodes in I_i-state. That means Equation (1) can be substituted by

$$\Delta SI_i = \eta_i \beta_i I_i \frac{\pi r^2}{L^2} S(t) \Delta t, \tag{4}$$

For convenience, we rewrite Equation (4) as $\Delta SI_i = \nu_i(t) S(t) \Delta t$, where $\nu_i(t)$ is state transition probability from state *S* to *I*, i.e., the infection function. So, we have

$$\nu_i(t) = \frac{\Delta SI_i(t)}{S(t)\Delta t} = \eta_i \beta_i \frac{\pi r^2}{L^2} I_i(t). \tag{5}$$

Similarly, we can have the transition probability from state I_A to I_B as follows:

$$\pi(t) = \eta_B \beta_B \frac{\pi r^2}{L^2} I_B(t). \tag{6}$$

2.3. The i-SIR Model

The i-SIR epidemiological architecture is formally presented in a set of partial differential equations based on Figure 1 as outlined below.

$$\begin{aligned} \frac{dS(t)}{dt} &= \mathrm{A} - \nu_1(t) S(t) - \nu_2(t) S(t) - \mu S(t), \\ \frac{dI_A(t)}{dt} &= \nu_1(t) S(t) - \pi(t) I_A(t) - (\varepsilon + \mu) I_A(t), \\ \frac{dI_B(t)}{dt} &= \nu_2(t) S(t) + \pi(t) I_A(t) - \mu I_B(t), \\ \frac{dD(t)}{dt} &= \mu S(t) + (\varepsilon + \mu) I_A(t) + \mu I_B(t), \end{aligned} \tag{7}$$

where $\nu_i(t)$ and $\pi(t)$ is the state conversion probabilities, A, ε and μ are substitution rate of nodes.

For convenience, let $w_i = \eta_i \beta_i \frac{\pi r^2}{L^2}$. Equations (5) and (6) can be rewritten as follows:

$$\nu_i(t) = \frac{\Delta SI_i(t)}{S(t)\Delta t} = w_i I_i(t). \tag{8}$$

$$\pi(t) = w_B I_B(t). \tag{9}$$

Since the state D does not appear explicitly in the first three equations in system (7), the dynamic of the system (7) is the same as the following system:

$$\begin{aligned}
\frac{dS(t)}{dt} &= \mathrm{A} - w_A I_A(t) S(t) - w_B I_B(t) S(t) - \mu S(t), \\
\frac{dI_A(t)}{dt} &= w_A I_A(t) S(t) - w_B I_B(t) I_A(t) - (\varepsilon + \mu) I_A(t), \\
\frac{dI_B(t)}{dt} &= w_B I_B(t) S(t) + w_B I_B(t) I_A(t) - \mu I_B(t),
\end{aligned} \tag{10}$$

with the initial condition $(S(0), I_A(0), I_B(0)) \in \Omega$, where

$$\Omega = \left\{ (S, I_A, I_B) \in R_+^3 : S + I_A + I_B \le \frac{\mathrm{A}}{\mu} \right\}.$$

For the system (10), we devise a propagation algorithm (see Algorithm 1) to describe the propagation rules for nodes in the WSN.in this algorithm, for each iteration in time, the state of each node should be made.

Algorithm 1: The state transformation of sensor nodes in the WSN

Input: The initial sensor network $G = (v,e)$

Output: Number of nodes in each state

Initialize the number of nodes in each state;
Set the number of iterations t^*
for $t = 0$ to t^* with the step of 1 **do**
  new nodes will be online into S state with probability A
  if node(i) is S state at time t and does not leave the network at time $t + 1$ **then**
    if neighbor nodes of node(i) is I_A state **then**
      it will become I_A state with probability w_A or it will become D state with probability μ or its state remains unchanged
    else if neighbor nodes of node(i) is I_B state **then**
      i it will become I_B state with probability w_B or it will become D state with probability μ or ts state remains unchanged
  end
  else if node(i) is I_A state at time t and does not leave the network at time $t + 1$ **then**
    if neighbor nodes of node(i) is I_B state **then**
      it will become I_B state with probability w_B or it will become D state with probability $\mu + \varepsilon$ or its state remains unchanged
  end
  else if node(i) is I_B state at time t and does not leave the network at time $t + 1$ **then**
      it will become D state with probability μ or its state remains unchanged
  end
end

3. Steady-State Analysis for Equilibria

As outlined below, we intend to investigate the equilibria of system (10) and study their Steady-state. Steady states of system (10) comply with the following equations:

$$\begin{cases} \dfrac{dS(t)}{dt} = 0, \\ \dfrac{dI_A(t)}{dt} = 0, \\ \dfrac{dI_B(t)}{dt} = 0. \end{cases} \tag{11}$$

Let $dI_A(t)/dt = 0,$ we have $I_A = 0 \; or \; I_A > 0.$ With respect to $I_A = 0,$ we have virus-free equilibrium

$$E_{vf} = \left(S^0, I_A^0, I_B^0\right) = \left(\frac{\mu}{w_B}, 0, \frac{\mathrm{A} - \mu^2}{\mu w_B}\right). \tag{12}$$

For $I_A > 0,$ we have a virus-endemic equilibrium

$$E_{ve} = \left(S^*, I_A^*, I_B^*\right) = \left(\frac{\mathrm{A}w_B}{w_1\mu - \varepsilon w_B}, \frac{\mu - w_B S(t)}{w_B}, \frac{w_B S(t) - (\varepsilon + \mu)}{w_B}\right). \tag{13}$$

Let

$$R_0 = \frac{\mu\left(w_B\mu - \varepsilon w_B\right)}{\mathrm{A}w_B^2}. \tag{14}$$

It is worth noting that the endemic equilibrium is biologically relevant only if $R_0 > 1.$

3.1. Virus-Free Steady State and Its Stability Analysis

We analyze the stability of system (10) at the equilibria to study the virus-epidemic behaviors. The Jacobian matrix at the virus-free equilibrium E_{vf} is

$$J\left(E_{vf}\right) = \begin{bmatrix} -w_B I_B & -w_A S^0 & -w_B S^0 \\ 0 & w_A S^0 - w_B I_B - (\varepsilon + \mu) & 0 \\ w_B I_B & w_B I_B & -w_B S^0 - \mu \end{bmatrix}. \tag{15}$$

The characteristic equation of the matrix $J\left(E_{vf}\right)$ is

$$\det\left(J - \lambda\mathbf{E}\right) = \left[-\lambda - w_B I_B\right] \times \left[-\lambda + w_A S^0 - w_B I_B - (\varepsilon + \mu)\right] \times \left[-\lambda - w_B S^0 - \mu\right]. \tag{16}$$

Equation (16) has two negative real roots $\lambda_1 = -w_B I_B, \lambda_2 = -2\mu.$ Besides, there exists another root $\lambda_3 = w_A S^0 - w_B I_B - (\varepsilon + \mu) = \dfrac{1}{\mu w_B}(R_0 - 1).$ Obviously, all of the roots of the characteristic equation are negative if $R_0 < 1.$

Based on the above statements, the following lemma can be obtained.

Lemma 1. *The virus-free equilibrium E_{vf} is locally asymptotically stable when $R_0 < 1$ and unstable when $R_0 > 1.$*

Furthermore, we can conclude the following theorem.

Theorem 1. *The virus-free equilibrium E_{vf} is globally asymptotically stable when $R_0 \le 1.$*

Proof. Learn from the first equation of system (10)

$$\dot{S}(t) \le \mathrm{A} - \mu S(t).$$

So,

$$S(t) \le \frac{\mathrm{A}}{\mu} + \left(S(0) - \frac{\mathrm{A}}{\mu} \right) \exp(-\mu t).$$

When $t \to \infty$, we can get

$$S(t) \le \frac{\mathrm{A}}{\mu}. \tag{17}$$

Replace Equation (17) in the second equation of system (10), we have

$$\dot{I}_A(t) \le \left(w_A \frac{\mathrm{A}}{\mu} - \mu - \varepsilon \right) I_A(t) = (R_0 - 1)(\mu + \varepsilon) I_A(t).$$

Hence, we have $\lim_{t\to\infty} I_A(t) = 0.$

Similarly, we can prove that $\lim_{t\to\infty} I_B(t) = 0.$

The proof is completed. □

3.2. Epidemic Steady State and Its Stability Analysis

For the virus-epidemic equilibrium E_{ve} in Equation (10). The Jacobian matrix at E_{ve} is

$$J(E_{ve}) = \begin{bmatrix} -w_A I_A^* - w_B I_B^* - \mu & w_A I_A^* & w_B I_B^* \\ w_A S^* & w_A S^* - w_B I_B^* - (\varepsilon + \mu) & w_B I_B^* \\ -w_B S^* & -w_B I_A^* & w_B S^* + w_B I_A^* - \mu \end{bmatrix}. \tag{18}$$

For convenience, let

$$\begin{aligned} a &= -w_A I_A^* - w_B I_B^* - \mu, \\ b &= \left(w_A S^* - w_B I_B^* - \varepsilon - \mu \right)\left(w_B S^* + w_B I_A^* - \mu \right), \\ c &= w_A S^* - w_B I_B^* - \varepsilon + w_B S^* + w_B I_A^* - 2\mu, \\ d &= w_B^2 I_A^* I_B^*. \end{aligned}$$

Then, the eigenfunction of $J(E_{ve})$ is given as follows:

$$f(\lambda) = \lambda^3 + m_1 \lambda^2 - m_2 \lambda + m_3, \tag{19}$$

where $m_1 = c - a, m_2 = ac + b, m_3 = ab + d.$

By the Routh-hurwitz criterion, all roots of Equation (19) have negative real parts if and only if $m_i > 0, (i = 1, 2, 3)$ and $A > 0,$ where $A = \begin{vmatrix} m_1 & 1 \\ m_3 & m_2 \end{vmatrix}.$

Hence, the following Lemma can be got.

Lemma 2. *When* $R_0 > 1$*, the endemic equilibrium* E_{ve} *is locally asymptotically stable if* $m_i > 0$ *and* $A > 0.$

Furthermore, we have the following theorem.

Theorem 2. *When* $R_0 > 1$*, the endemic equilibrium* E_{ve} *is globally asymptotically stable if* $m_i > 0$ *and* $A > 0.$

Proof. We consider the Lyapunov function for $t \ge 0$

$$V(t) = k_1 \int_{S^*}^{S} \frac{t - S^*}{t} dt + k_1 \int_{I_A^*}^{I_A} \frac{t - I_A^*}{t} dt + \int_{1}^{I_B^*} \frac{t - I_B^*}{t} dt, \tag{20}$$

combining Equation (10), we have

$$
\begin{aligned}
V'(t) &= \left(A - w_A I_A S - w_B I_B S - \mu S\right) - \left(\frac{S^*}{S} A - w_A I_A S^* - w_B I_B S^* - \mu S^*\right) + \left[w_A I_A S - w_B I_B I_A - (\varepsilon + \mu) I_A\right] \\
&\quad - \left[w_A S I_A^* - w_B I_B I_A^* - (\varepsilon + \mu) I_A^*\right] + \left(w_B I_B S + w_B I_B I_A - \mu I_B\right) - \left(w_B S I_B^* + w_B S I_A I_B^* - \mu I_B^*\right) \\
&\le -A \frac{S}{S^*} \left(\frac{S^*}{S} - 1\right)^2 - w_A S I_A^* - w_B S I_B^* - w_B S I_A I_B^* \\
&\le 0.
\end{aligned}
$$

So, we conclude that the epidemic equilibrium is globally asymptotically stable.

4. Numerical Simulations

This section focuses on implementing computational modeling to empirically validate the theoretical predictions derived in the mathematical analysis. To further demonstrate the superiority and effectiveness of the proposed model, a systematic comparative study is conducted between the model presented in this paper and the classical statistical immune model, to highlight the advancements and practical value of our approach.

(i) Validation of Theorem 1: Disappearance of Bad Worms

First, we define the core parameters and initial values of the system based on realistic network scenarios. Specifically, the parameters are set as: $A = 1, \pi = 3.14, r = 5, L = 10, \eta_A = 0.01, \beta_A = 0.01, \eta_B = 0.05, \beta_A = 0.005, \mu = 0.001,$ and initial values $S(0) = 998, I_A(0) = 1, I_B(0) = 1.$ By calculation, we have $R_0 = 0.0494 < 1.$ Through numerical simulation using the Runge-Kutta method (order 4), the dynamic evolution curves of each state variable over time are obtained, which are depicted in Figure 3. As clearly shown in Figure 3, as time elapse(t), the number of nodes infected by bad worms exhibits a continuous downward trend—starting from the initial value, it rapidly decreases in the early stage, and gradually converges to 0 after a certain time step. Meanwhile, the number of susceptible nodes (*S*) decreases to a stable low level, and the number of nodes infected by good worms first increases and then stabilizes, forming a dynamic balance. This simulation result is completely consistent with the conclusion of Theorem 1, thus verifying the correctness of the theoretical analysis.

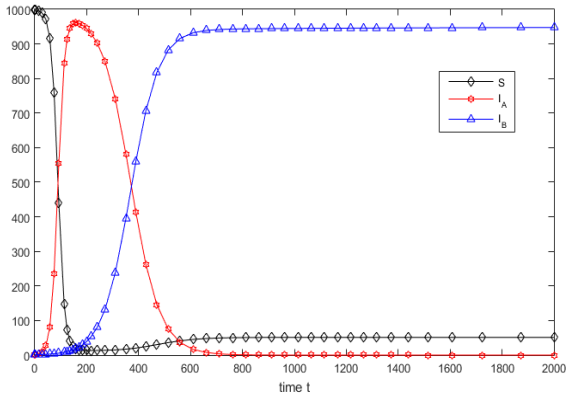

Figure 3. Infection wave dynamics mapping with $R_0 = 0.0494 < 1.$

(ii) Validation of Theorem 2: Asymptotic Convergence to Virus-Endemic Equilibrium

We adjust the system parameters to satisfy the condition of Theorem 2. The parameters are reset as: $A = 1, \pi = 3.14, \mu = 0.001, \beta_A = 0.008, \beta_B = 0.0002, \varepsilon = 0.00005, r = 8, L = 8, \eta_A = 0.01, \eta_B = 0.009$, and initial values $S(0) = 998, I_A(0) = 1, I_B(0) = 1.$ By calculation, we have $R_0 = 6.6840 > 1.$ We characterize the evolutionary patterns of the virus-endemic equilibrium I_A of system (10) in Figure 4. Figure 4 demonstrates that all state variables of the system do not tend to extinction or infinite growth; instead, they gradually approach fixed constant values as time evolves. This phenomenon of asymptotic convergence to the virus-endemic equilibrium point is fully consistent with the conclusion of Theorem 2.

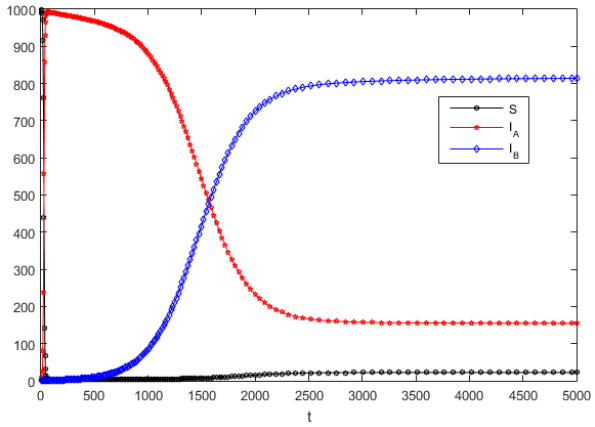

Figure 4. Infection wave dynamics mapping with $R_0 = 6.6840 > 1$.

(iii) Impact of Infection Rate on Worm Propagation

To further investigate the quantitative impact of the infection rate on the propagation dynamics of worms, we design a control variable experiment: we fix other parameters and only adjust the value of ($w_A : w_B$), then plot the evolution curves of the number of bad worm-infected nodes under different $w_A : w_B$ values in Figure 5. From Figure 5, we can see that the higher the ratio of $w_A : w_B$, the faster the worm spreads, and the bigger the scale reaches. From this point of view, improving the infection ratio of good worms is an effective method for restraining the spread of worms.

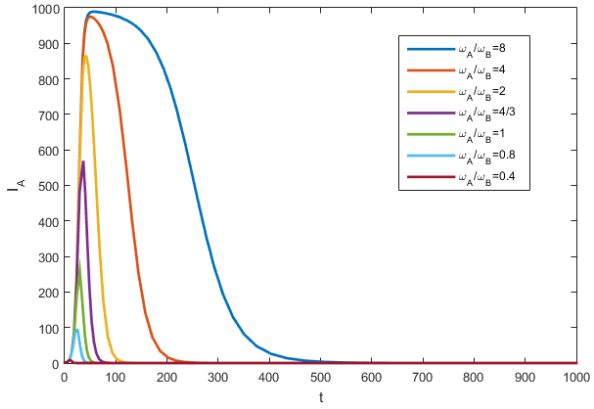

Figure 5. The trajectory of I_A for different values of $w_A : w_B$.

(iv) Comparison of this model with the classical model

In the following, we perform the comparison between the i-SIR model and the classical statistical immune model [27]. For clarity, the classical statistical immune model is written as follows.

$$\begin{cases} \dfrac{dS(t)}{dt} = \mathrm{A} - \nu_1(t) S(t) - (\mu + \omega) S(t), \\ \dfrac{dI_A(t)}{dt} = \nu_1(t) S(t) - (\varepsilon + \mu + \gamma) I_A(t), \\ \dfrac{dR(t)}{dt} = \omega S(t) + \gamma I_A(t) - \mu R(t), \\ \dfrac{dD(t)}{dt} = \mu S(t) + (\varepsilon + \mu) I_A(t) + \mu R(t), \end{cases} \tag{21}$$

where ω and γ are statistic immune ratio, and the meaning of other parameters is the same to the system (7). Set parameters $A = 1; \pi = 3.14; \mu = 0.001; \beta_A = 0.008; \beta_B = 0.002; \varepsilon = 0.0005; r = 8; L = 8; \eta_B = 0.009; \omega = 0.008;$

$\gamma = 0.008$. Figure 6 depicts simulation results, which show that the i-SIR model can restrain the spread of worms more effectively than the classical statistical immune model.

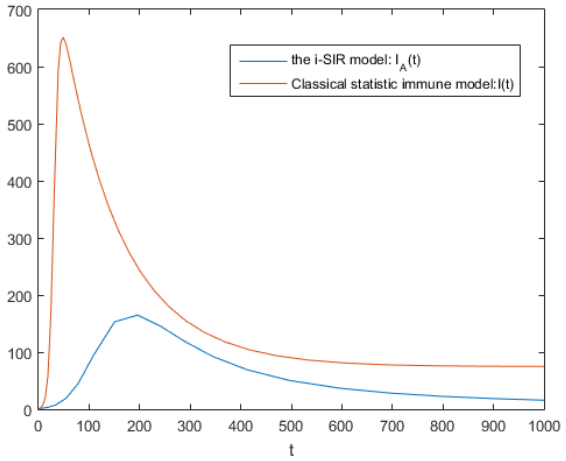

Figure 6. The comparison of the i-SIR model and the classical statistical immune model.

In summary, the simulations confirm the theoretical robustness of the i-SIR model, quantify the impact of key parameters on worm dynamics, and demonstrate its superiority over classical models in balancing defense efficacy and network longevity.

5. Conclusions

In view of the growing complexity of wireless sensor network (WSN) architectures and the aggravating threats posed by malicious worms, which can lead to widespread node failures and data security breaches, this study introduces an innovative i-SIR model designed to characterize the propagation dynamics of both good and bad worms in such networks. Unlike traditional models that often oversimplify worm behavior, the i-SIR model incorporates a more nuanced classification: bad worms, which actively exploit vulnerabilities to infect and corrupt sensor nodes, and good worms (or "benign worms"), which are deployed as a defensive mechanism to counteract malicious infections by immunizing nodes or inhibiting bad worm replication.

Through rigorous mathematical analysis, the research derives the basic reproduction number R_0 for the i-SIR model—a critical threshold parameter that dictates whether a worm outbreak will persist or eventually die out. Specifically, if R_0 <1, the spread of bad worms is suppressed, and the network tends toward a stable, uninfected state; conversely, an R_0 >1 indicates that bad worms can sustain their propagation, potentially leading to a large-scale epidemic. This theoretical derivation is validated through systematic numerical simulations, which not only confirm the accuracy of the R_0 calculation but also vividly illustrate the temporal evolution of infected, susceptible, and immunized node populations under varying initial conditions.

A key focus of the study is a comparative analysis between the i-SIR model and the classical statistical immune model, a widely adopted framework in worm control research. Under identical experimental parameters—including initial node density, initial infection rate, and resource constraints for worm deployment—the simulation results reveal that the i-SIR model exhibits a significantly enhanced control effect on bad worm spread. This superiority is reflected in several metrics: a faster reduction in the number of infected nodes, a higher rate of node immunization by good worms, and a smaller overall scale of the worm epidemic. The improved performance stems from the i-SIR model's ability to dynamically balance the interaction between good and bad worms, leveraging the defensive properties of good worms to proactively disrupt the propagation chain of their malicious counterparts. Furthermore, the research delves into the impact of varying the ratio of infection rates between bad and good worms on the propagation process. The infection rate ratio, defined as the quotient of the bad worm infection rate (w_A) to the good worm infection rate (w_B), emerges as a pivotal factor influencing both the speed and scale of worm spread. Simulation results demonstrate a clear trend: as this ratio decreases (i.e., when good worms exhibit a relatively higher infection/immunization efficiency compared to bad worms), the propagation speed of bad worms is drastically retarded, and the ultimate scale of the epidemic is significantly reduced. For instance, a 50% reduction in the $w_A : w_B$ ratio leads to a nearly 20% decrease in the peak number of infected nodes and a 50% shortening of the time required to contain the outbreak. These findings underscore the strategic

value of optimizing the deployment of good worms to minimize the $w_A : w_B$ ratio, thereby enhancing the overall resilience of WSNs against worm attacks.

Author Contributions

L.F.: Methodology, Investigation, Writing (original draft, review and editing); Y.H.: Methodology, Validation, Writing (original draft, review and editing); Q.Z.: conceptualization, Writing (review and editing); P.W.: conceptualization. All authors have read and agreed to the published version of the manuscript.

Funding

This work was supported by the Research Project supported by the Shanxi Provincial Natural Science Foundation (202203021211116).

Data Availability Statement

Not applicable.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Amutha, J.; Sharma, S.; Sharma, S. Strategies based on various aspects of clustering in wireless sensor networks using classical, optimization and machine learning techniques: Review, taxonomy, research findings, challenges and future directions. *Comput. Sci. Rev.* **2021**, *40*, 100376. https://doi.org/10.1016/j.cosrev.2021.100376.
2. Qamar, T. The measurement and monitoring of Quality of service based on security analysis in wireless sensor network using deep learning architecture. *Measurement* **2023**, *220*, 113434.
3. Shanmathi, M.; Sonker, A.; Hussain, Z.; et al. Enhancing wireless sensor network security and efficiency with CNN-FL and NGO optimization. *Meas. Sens.* **2024**, *32*, 101057.
4. Zhang, H.; Madhusudanan, V.; Geetha, R.; et al. Dynamic analysis of the e-SITR model for remote wireless sensor network with noise and Sokol-Howell functional response. *Results Phys.* **2022**, *38*, 105643.
5. Wu, Y.; Pu, C.; Zhang, G.; et al. Epidemic spreading in wireless sensor networks with node sleep scheduling. *Phys. A Stat. Mech. Its Appl.* **2023**, *629*, 12904.
6. Dong, C.; Zhao, L. Sensor network security defense strategy based on attack graph and improved binary PSO. *Saf. Sci.* **2019**, *117*, 81–87.
7. Zhang, Z.; Zou, J.; Upadhyay, R. An epidemic model with multiple delays for the propagation of worms in wireless sensor networks. *Results Phys.* **2020**, *19*, 103424. https://doi.org/10.1016/j.rinp.2020.103424.
8. Dutta, K. Dynamic optimization of multi-layered defenses inspired by Chakravyuh. *Int. J. Crit. Infrastruct. Prot.* **2025**, *51*, 100794.
9. Kephart, J.O.; White, S.R. Measuring and modeling computer virus prevalence. In Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, USA, 24–26 May 1993, pp. 2–15.
10. Dong, N.P.; Long, H.V.; Son, N.T.K. The dynamical behaviors of fractional-order SE_1E_2IQR epidemic model for malware propagation on Wireless Sensor Network. *Commun. Nonlinear Sci. Numer. Simul.* **2022**, *111*, 106428.
11. Kumar, P.M.; Shahwar, T.; Gokulnath, G. Improved sensor localization with intelligent trust model in heterogeneous wireless sensor network in Internet of Things (IoT) environment. *Sustain. Comput. Inform. Syst.* **2025**, *46*, 101122.
12. Tang, W.; Yang, H.; Pi, J.X.; et al. Network virus propagation and security situation awareness based on Hidden Markov Model. *J. King Saud Univ. Comput. Inf. Sci.* **2023**, *35*, 101840.
13. Yang, L.; Li, P.; Yang, X.; et al. Simultaneous Benefit Maximization of Conflicting Opinions: Modeling and Analysis. *IEEE Syst. J.* **2020**, *14*, 1623–1634. https://doi.org/10.1109/JSYST.2020.2964004.
14. Jafar, M.T.; Yang, L.X.; Li, G.; et al. Malware containment with immediate response in IoT network: An optimal control approach. *Comput. Commun.* **2024**, *228*, 107951.
15. Dong, N.P.; Long, H.V.; Giang, N.L. The fuzzy fractional SIQR model of computer virus propagation in wireless sensor network using Caputo Atangana-Baleanu derivatives. *Fuzzy Sets Syst.* **2022**, *429*, 28–59.
16. Liu, G.; Peng, Z.L.; Tian, T.T.; et al. Malware attack and defense game in fractional-order Internet of underwater Things: Model-based and model-free approaches. *Eng. Appl. Artif. Intell.* **2025**, *161*, 111970.
17. Wei, L.V.; Ke, Q.; Li, K. Dynamic stability of an SIVS epidemic model with imperfect vaccination on scale-free networks and its control strategy. *J. Frankl. Inst.* **2020**, *357*, 7092–7121.

18. Ahmad, I.; Bakar, A.A.; Jan, R.; et al. Dynamic behaviors of a modified computer virus model: Insights into parameters and network attributes. *Alex. Eng. J.* **2024**, *103*, 266–277.
19. Angurala, M.; Bala, M. Bamber. Implementing MRCRLB technique on modulation schemes in wireless rechargeable sensor networks. *Egypt. Inform. J.* **2021**, *22*, 473–478. https://doi.org/10.1016/j.eij.2021.03.002.
20. Premkumar, M.; Sundararajan, T. DLDM: Deep learning-based defense mechanism for denial f service attacks in wireless sensor networks. *Microprocess. Microsyst.* **2020**, *79*, 103278. https://doi.org/10.1016/j.micpro.2020.103278.
21. Moslehi, M.M. Exploring coverage and security challenges in wireless sensor networks: A survey. *Comput. Netw.* **2025**, *260*, 111096.
22. Acarali, D.; Rajarajan, M.; Komninos, N.; et al. Modelling the spread of botnet worm in IoT-based wireless sensor networks. *Secur. Commun. Netw.* **2019**, *2019*, 3745619.
23. Yuan, Y.; Shen, X.; Sun, L.; et al. Modeling Cascading Failures and Invulnerability Analysis of Underwater Acoustic Sensor Networks Based on Complex Network. *Comput. Netw.* **2024**, *5*, 6942–6952.
24. Bailey, N. *The Mathematical Theory of Infectious Diseases and Its Applications*, 2nd ed.; Oxford University Press: New York, NY, USA, 1975.
25. Yuan, H.; Chen, G.; Wu, J.; et al. Towards controlling virus propagation in information systems with point-to-group information sharing. *Decis. Support Syst.* **2009**, *48*, 57–68.
26. Yuan, H.; Chen, G. Network virus-epidemic model with the point-to-group information propagation. *Appl. Math. Comput.* **2008**, *206*, 357–367.
27. Zou, C.C.; Gong, W.B.; Towsley, D.; et al. Code red worm propagation modeling and analysis. In Proceedings of the CCS02: ACM Conference on Computer and Communications Security, Washington, DC, USA, 18–22 November 2022.