Sensitivity Analysis of the Multi Malware Attacks Model in Wireless Sensor Networks

Leila Moradi[1(✉)], Eslam Farsimadan[1], Marcello Trovati[2], and Francesco Palmieri[1]

[1] Department of Computer Science, University of Salerno, 84084 Fisciano, Italy
{lmoradi,efarsimadan,fpalmieri}@unisa.it
[2] School of Business, University of Lancashire, Preston, Lancashire, UK
mtrovati@lancashire.ac.uk

Abstract. Wireless Sensor Networks (WSNs) technology is extensively utilized in various applications necessitating monitoring and control functionalities. Nonetheless, some unresolved difficulties impede its effective deployment, primarily related to security concerns. This study investigates and analyzes the parameter sensitivity of the Susceptible-Exposed1-Exposed2-Infected-Recovered (SE_1E_2IR) model, derived from the classical Susceptible-Exposed-Infected-Recovered (SEIR) epidemic theory and used for the early detection of multi-malware activities in WSNs. In this model, two exposed states have been considered based on the assumption of two different types of malware attacks in the network. The primary SE_1E_2IR model develops a mechanism for the earlier detection of malware attack incidents in WSNs. The model is structured upon a system of ordinary differential equations. The basic reproduction number is also determined as a crucial factor for characterizing malware propagation within the network. It can be helpful to identify the circumstances in which the network remains almost safe or the risk of a malware outbreak. This work offers a fundamental comprehension of sensitivity analysis for the epidemic SE_1E_2IR model. Furthermore, it examines the efficacy of the parameters and analyzes the impact of different model parameters on malware spread in WSNs. Then, an analytical comparison of the suggested model with existing models is presented. Numerical simulations are run in MATLAB to augment the theoretical analyses.

Keywords: Differential Equations · Wireless sensor networks · Malware propagation · Basic reproductive number · Sensitivity analysis

1 Introduction

Wireless Sensor Networks (WSNs) are gaining an ever-increasing interest in modern communication scenarios due to their essential roles in cyber-physical systems and their related applications. They are now extensively used in environmental monitoring, intelligent transportation, fire prevention, rescue management, security monitoring, traffic control, target tracking, and many other

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2027
O. Gervasi et al. (Eds.): ICCSA 2026 Workshops, LNCS 16760, pp. 398–414, 2027.
https://doi.org/10.1007/978-3-032-30521-3_25

domains due to their simple configuration, extreme adaptability, and inherently scalable nature [2,14,31]. However, several known issues and open challenges, mainly due to hardware constraints and limitations, can adversely affect their secure deployment on mission-critical infrastructures. Indeed, WSNs are still susceptible to various menaces, Sybil [16,35], wormhole [9] and selective forwarding [37] attacks, as well as malware propagation [1,25] and related malicious activities. Among these menaces, malware propagation can be considered particularly dangerous, mostly in large-scale WSNs, since any infected sensor node can easily spread malware to its neighbors, leading to the rapid compromise of the entire infrastructure. To easily harm the entire network, an attacker may target particular nodes (e.g., cluster heads or gateways), inject malware components, and rely on the native propagation mechanism characterizing these infrastructures (i.e., clustering properties associated with scale-free dynamics) to immediately infect the whole system. In addition, radio communications, pervasively used in modern WSNs, offer extremely suitable circumstances for massive malware propagation, mainly when ad-hoc mesh connection architectures are involved. New-generation malware propagates autonomously through the mesh, rapidly affecting the whole network without human involvement. Accordingly, knowledge of malware propagation dynamics is crucial to preserving network security and integrity. Usually, more sophisticated WSNs can deploy protection strategies against the spread of malware, together with detection and recovery mechanisms that can discover and repair malware-infected nodes. However, managing such a mix of proactive and reactive strategies requires non-negligible activities on communication channels, resulting in additional energy consumption and, hence, reduced lifetimes of sensor nodes. It is straightforward to consider that a better understanding of the malware diffusion process in WSNs can be extremely helpful in driving more targeted protection strategies that are able to effectively reduce the overhead by minimizing the overall power loss [38]. Some recent research efforts on the propagation of malware in WSNs are presented in [11,12,18].

Since a variety of epidemic models for infectious diseases have been proposed, the dynamics of malware propagation in networks may also be explained by these models. Therefore, in order to describe the process of malware propagation in network systems, researchers developed theoretical models that took inspiration from existing ideas of biological viral transmission across populations. Nevertheless, limited effort has been devoted to malware propagation models that are specific to WSNs. In several recent studies, researchers have used epidemic models to study how malware spreads in WSNs [4,23,39]. Since WSNs have special dynamic properties, the models of spreading epidemics in the human population cannot be simply applied to investigate malware propagation in WSNs. Furthermore, the behaviors of different malware affecting WSNs varied significantly and unexpectedly. In particular, common models only consider a single type of malware infection active at any time, and more realistic schemes considering the possibility of multiple simultaneous malware attacks (multi-malware models) can be extremely interesting for more realistic modeling. On the other hand, the majority of models that have been suggested to study the spread of mal-

ware in these networks rely on Ordinary Differential Equations (ODEs), which are an ineffective tool for describing the behaviors of a complicated networked system [5–7,10]. Researchers have suggested multiple epidemiological models to examine the stability and effectiveness of WSN.

Sensitivity analysis of model parameters is crucial in mathematical model formulation, as it clarifies the relationship between alterations in model outputs and fluctuations in model inputs [8]. This study aims to serve as an initial guide for individuals interested in exploring parameter sensitivity in the mathematical modeling of malware dissemination in WSNs through ODEs. The direct differential method is a fast way to do sensitivity analysis. It analyzes local sensitivities, allowing researchers to gain a thorough understanding of the impacts of slight parameter variations on model outcomes. In the subsequent sections of this study, we analyze the local and global sensitivity of the SE_1E_2IR model.

The rest of this paper is organized as follows: Sect. 2 reports some related work. In Sects. 3, description and formulation of the proposed model are presented. Section 4 discusses the basic properties of the model. The sensitivity analysis of the model parameters is covered in Sect. 5. The simulation outcomes of the modified model and the discussion of the achieved results are presented in Sect. 6. Finally, Sect. 7 presents the conclusion and the upcoming work.

2 Related Work

Recent studies on malware propagation on networked systems, such as WSNs, are based on epidemic theories, which, in turn, rely on mathematical models where differential equations play an essential role. A mathematical model for an epidemic phenomenon is fundamentally built on a few significant assumptions regarding the problem of interest. For instance, concerning malware propagation, the hypotheses are entirely correlated with the characteristics associated with malware infection and network connections, allowing its diffusion among involved entities. By employing these mathematical models, investigations on the dynamics of malware propagation in WSNs have yielded notable advancements. Most of the available propagation models, including SIS, SIRS, SEIR, SEIRS, SITR, SNIRD, HSIRD, SEIRV, and VSCIQRS are established based on the conventional SIR model.

Ojha et al. [22] introduced a Susceptible-Exposed-Infected-Recovered-Susceptible (SEIRS) model to address the limitations of previous models. The suggested SEIRS model contains a finite communication radius and the corresponding node density for WSNs, offering a method to mitigate the propagation of worms. Upadhyay and Kumari [29] presented an energy-efficient e-epidemic Susceptible-Infected-Terminally Infected-Recovered (SITR) model to examine the attacking behaviors of worms in WSNs utilizing a cytoid-type functional response. Geetha et al. [13] suggested a modified SEIRS model using background noise as an additional variable. The effectiveness of the model has been validated through Lyapunov-based analysis. Shen et al. [26,27] proposed a heterogeneous Susceptible-iNsidious-Infected-Recovered-Dysfunctional(SNIRD) model

that takes into account the connectivity of multiple heterogeneous sensor nodes while also reflecting the properties of malware concealment and dysfunctional nodes. Moreover, they suggested another Heterogeneous Susceptible-Infected-Removed-Dead (HSIRD) model for heterogeneous WSNs, in which they determined the epidemic threshold and conducted stability assessments for equilibrium points.

Regarding agent-based modeling, Nwokoye and Umeh [20] introduced the agent equivalent of the mathematical Susceptible-Exposed-Infected-Recovered-Susceptible with a Vaccination class (SEIRS-V) model. Furthermore, Xu et al. [33] established the Susceptible-Exposed-Infected-Recovered with a Failed type (SEIRS-F) agent-based model to deal with malware propagation and component reliability in WSNs.

Han et al. [15] suggested an approach to intrusion detection in WSNs utilizing an autoregressive model and game theory to minimize energy consumption in case of deploying Intrusion Detection Systems. Besides decreasing energy usage, this model can forecast attack targets. Singh et al. [28] presented an enhanced Susceptible-Exposed-Infected-Recovered-Vaccination (SEIRV) model to address the effects of the radius of communication and density of nodes on malware spreading in WSNs, aiming at identifying the essential conditions for the continuous spread of malware within the network. Wu et al. [32] conducted experiments on malware propagation in heterogeneous WSNs leveraging the Markov chain technique and infectious disease theories, revealing that network availability correlates with the vulnerability, distribution, and degree of network nodes. Acarali et al. [1] developed a Susceptible-Infected-Susceptible (SIS) malware propagation model to examine the dynamics of the spread of botnet within Internet of Things (IoT)-based WSNs, disclosing that node distribution density and energy constraints influence the botnet generation process.

Wu et al. [30] studied a virus propagation model to analyze the propagation of a virus in the Social Internet of Things (SIoT), taking into account the variable number of associated devices. They employed game theory to mitigate the virus propagation among the devices. Zhang et al. [36] suggested a method based on epidemic theory to mitigate the propagation of malware in WSNs. It involves sensor network heterogeneity by considering sensor nodes and sink nodes. They examined the impact of malware attacks on several kinds of topologies and proposed a framework for setting up, distributing, and preserving WSNs. Ye et al. [34] developed a Susceptible-Infected-Basically Recovered-Completely Recovered (SIR_1R_2) theory that examined the influence of secondary immunity mechanisms on malware propagation in WSNs. Zhou et al. [38] leveraged game theory to examine the malware spread dynamics in WSNs. Furthermore, the Nash equilibrium technique is utilized to assess the propagation patterns of malware in such networks. The correlation between the steady-state infection ratio and game characteristics and the presence of malware in WSNs is investigated. Cellular automata have also been used to simulate malware spread in WSNs and validate the accuracy of the proposed theory with simulation outcomes. Liu et al. [17] proposed an alternative SEIR model to characterize the spreading

of mutated viruses in WSNs. The basic reproductive number is calculated by implementing the next-generation matrix approach. The stability analysis of the system has also been conducted, resulting in the identification of two equilibrium points: global and local. They tried to propose a practical control approach for managing the spread of viruses in WSNs.

Although many studies investigate the behavior of malware propagation in WSNs, few have investigated the sensitivity analysis of multi-malware propagation in WSNs. Motivated by this shortage, we consider epidemic model for multi-malware attacks in WSNs based on ODEs and we discuss the local and global sensitivity analysis methods.

3 Background Concepts

Recently, Awasthi et al. [3] designed a deterministic model for multi-malware propagation in WSNs considering five node classes: Susceptible, Exposed 1, Exposed 2, Infected, and Recovered. Such a model investigates two distinct forms of malware spread in WSNs, considering that the nodes fail or malfunction due to hardware or software issues when subjected to malware attacks. At first, it was considered that all nodes were susceptible to malware attacks. The operational efficiency of sensor nodes is decreased as they become infected. This model includes two latent phases, revealing that malware requires a certain time to become really infectious. The average duration spent in the E_i subclass is determined as $\frac{1}{(\lambda_i+\sigma)}$ [24]. The authors suggested that states in a WSN can be classified into several categories at any time t. They have developed a series of ODEs to describe the dynamic process of malware spread in WSNs. The four distinct states constituting the proposed model are illustrated as follows:

- Susceptible $S(t)$: It refers to the sensor nodes that remain unaffected by malware but are susceptible to infection at any moment.
- Exposed $E(t)$: It denotes malware-infected sensor nodes that are not capable of spreading the malware despite their infection. However, over time, they distribute infection. Given the hypothesis that two distinct types of malware may simultaneously target the network, two categories of exposed nodes, $E_1(t)$ and $E_2(t)$, are considered. Given the hypothesis that two distinct types of malware may simultaneously target the network, two categories of exposed nodes, $E_1(t)$ and $E_2(t)$, are considered.
- Infected $I(t)$: It refers to the sensor nodes that are infected and have the potential to propagate the infection to adjacent sensor nodes.
- Recovered $R(t)$: It signifies the category that includes sensor nodes within the network that have been restored following an infected state.

The dynamical malware propagation formulated in the set of ODEs known as the SE_1E_2IR model is as follows [3]:

$$\begin{cases} \frac{dS}{dt} = b - \varphi\, S\, I - (\sigma + \omega)\, S \\ \frac{dE_1}{dt} = p\varphi\, S\, I - (\lambda_1 + \sigma)\, E_1 \\ \frac{dE_2}{dt} = q\varphi\, S\, I - (\lambda_2 + \sigma)\, E_2 \\ \frac{dI}{dt} = \lambda_1\, E_1 \;+\; \lambda_2\, E_2 \;-\; (\sigma + \gamma)\, I \\ \frac{dR}{dt} = \gamma\, I - \sigma\, R + \omega\, S \end{cases} \tag{1}$$

The system is characterized within the domain $\Gamma = \{(S, E_1, E_2, I, R) \in \mathbb{R}^5\}$ in which $S(0) = S_0$, $E_1(0) = 0$, $E_2(0) = 0$, $I(0) = I_0$, $R(0) = R_0$ for all $t \geq 0$. Because the model observes distinct states for sensor nodes, all state variables are positive for all $t \geq 0$.

$N(t)$ uniformly distributed within the designated area L^2, denotes the total number of sensor nodes in the WSN at any given time t ($N(t) = S(t) + E_1(t) + E_2(t) + I(t) + R(t)$). The region covered by a sensor node of the WSN is πr^2, where r represents the communication radius. It should be mentioned that $p + q = 1$, $\lambda_1 > \lambda_2$, and $\varphi = \frac{\beta \pi r^2}{L^2}$. The most important parameters in the SE_1E_2IR model (1) are summarized in Table 1.

Table 1. Parameters of the SE_1E_2IR model.

Parameters	Description
b	The addition rate of new nodes in WSN
σ	The failure rate of nodes caused by battery depletion or hardware/software problems
β	The coefficient of malware transmission in WSN
p	The rate of susceptible nodes that became exposed and enter into E_1 state
q	The rate of susceptible nodes that became exposed and enter into E_2 state
λ_1	The rate of exposed state E_1 of nodes become infectious
λ_2	The rate of exposed state E_2 of nodes become infectious
γ	The rate of recovery of infectious nodes
ω	The rate at which susceptible nodes become immunized and move to the recovered state R

4 Main Results of the Model and Stability Analysis

The analysis of sensitivity investigates the impact of parameters on these equilibria, consequently validating models through the comparison of actual and predicted values. We will calculate the basic reproduction number and conduct a sensitivity analysis based on the free equilibrium points.

4.1 Free Equilibrium Points

The free equilibrium points of the system of the SE_1E_2IR model (1) can be identified by solving the equations $\frac{dS}{dt} = 0, \frac{dE_1}{dt} = 0, \frac{dE_2}{dt} = 0, \frac{dI}{dt} = 0, \frac{dR}{dt} = 0$. Consequently, we set

$$\begin{cases} b - \varphi\, S\, I - (\sigma + \omega)\, S = 0, \\ p\varphi\, S\, I - (\lambda_1 + \sigma)\, E_1 = 0, \\ q\varphi\, S\, I - (\lambda_2 + \sigma)\, E_2 = 0, \\ \lambda_1\, E_1 \, + \, \lambda_2\, E_2 \, - \, (\sigma + \gamma)\, I = 0, \\ \gamma\, I - \sigma\, R + \omega\, S = 0. \end{cases} \tag{2}$$

A straightforward computation will determine the free equilibrium points (Ξ_0) as follows:

$$\Xi_0 = (\frac{b}{(\sigma + \omega)}, 0\,, 0,\, 0,\, \frac{\omega b}{\sigma(\sigma + \omega)}). \tag{3}$$

4.2 Basic Reproduction Number

The basic reproduction number, R_0, is the primary parameter for categorizing the spread of malware in WSN. R_0 represents the total number of secondary infected nodes caused by a single infected individual over a certain period. Hence, R_0 is a dimensionless metric identifying the probability of malware propagation. Various methodologies exist for determining R_0 in the context of epidemic spread. This study employs the next-generation matrix technique. Just E_1, E_2, and I are presently directly engaged in the spread of malware. Upon examination of the issue, we have delineated three classes, denoted as (E_1, E_2, I), to determine the parameter R_0. Consequently, we recall the SE_1E_2IR model (1) here:

$$\begin{cases} \dfrac{dE_1}{dt} = p\varphi\, S\, I - (\lambda_1 + \sigma)\, E_1 \\ \dfrac{dE_2}{dt} = q\varphi\, S\, I - (\lambda_2 + \sigma)\, E_2 \\ \dfrac{dI}{dt} = \lambda_1\, E_1 \, + \, \lambda_2\, E_2 \, - \, (\sigma + \gamma)\, I \end{cases} \tag{4}$$

Employing the approach (the next generation matrix [8]), the system (4) can be expressed as $\dfrac{dX}{dt} = P(X) - Q(X)$, where

$$X = \begin{bmatrix} E_1 \\ E_2 \\ I \end{bmatrix}, \quad P(X) = \begin{bmatrix} p\varphi\, S\, I \\ q\varphi\, S\, I \\ \lambda_1\, E_1 \, + \, \lambda_2\, E_2 \end{bmatrix}, Q(X) = \begin{bmatrix} (\lambda_1 + \sigma)\, E_1 \\ (\lambda_2 + \sigma)\, E_2 \\ (\sigma + \gamma)\, I \end{bmatrix}.$$

The Jacobian matrices of $P(X)$ and $Q(X)$ are calculated as follows:

$$\mathcal{J}(P(X)) = \begin{bmatrix} 0 & 0 & p\varphi S \\ 0 & 0 & q\varphi S \\ \lambda_1 & \lambda_2 & 0 \end{bmatrix}, \mathcal{J}(Q(X)) = \begin{bmatrix} (\lambda_1 + \sigma) & 0 & 0 \\ 0 & (\lambda_2 + \sigma) & 0 \\ 0 & 0 & (\sigma + \gamma) \end{bmatrix}.$$

The Jacobian matrices of $P(X)$ and $Q(X)$ at the free equilibrium points (Ξ_0) are calculated according to (3), as follows:

$$K := \mathcal{J}(P|_{\Xi_0}) = \begin{bmatrix} 0 & 0 & \frac{p\varphi b}{(\sigma+\omega)} \\ 0 & 0 & \frac{q\varphi b}{(\sigma+\omega)} \\ \lambda_1 & \lambda_2 & 0 \end{bmatrix}, H := \mathcal{J}(Q|_{\Xi_0}) = \begin{bmatrix} (\lambda_1+\sigma) & 0 & 0 \\ 0 & (\lambda_2+\sigma) & 0 \\ 0 & 0 & (\sigma+\gamma) \end{bmatrix}.$$

The inverse of H is given by

$$H^{-1} = \begin{bmatrix} \frac{1}{(\lambda_1+\sigma)} & 0 & 0 \\ 0 & \frac{1}{(\lambda_2+\sigma)} & 0 \\ 0 & 0 & \frac{1}{(\sigma+\gamma)} \end{bmatrix}. \tag{5}$$

The next generation matrix $M = KH^{-1}$ is:

$$M = \begin{bmatrix} 0 & 0 & \frac{p\varphi b}{(\sigma+\omega)(\sigma+\gamma)} \\ 0 & 0 & \frac{q\varphi b}{(\sigma+\omega)(\sigma+\gamma)} \\ \frac{\lambda_1}{(\lambda_1+\sigma)} & \frac{\lambda_2}{(\lambda_2+\sigma)} & 0 \end{bmatrix}. \tag{6}$$

Consequently, the basic reproduction number R_0 (which indicates the largest eigenvalue) is calculated as follows:

$$R_0 = \frac{b\varphi}{(\sigma+\omega)(\sigma+\gamma)}\Big(\frac{p\lambda_1}{(\lambda_1+\sigma)} + \frac{q\lambda_2}{(\lambda_2+\sigma)}\Big). \tag{7}$$

5 Efficiency of the Parameters

This part investigates the efficacy of the parameters and explores how various model parameters affect malware propagation in WSNs. This implies, in sensitivity analysis, a minor alteration of any parameter can result in a significant variation in the malware's ability to propagate over WSNs. Here, we consider two invaluable tools for efficiency analysis: local and global sensitivity. It is possible to identify the most influential parameters of the proposed model using both local and global sensitivity analysis.

Local Sensitivity Analysis. Analyzing the sensitivity of R_0 is crucial for effectively suppressing malware propagation in WSNs, as R_0 is an essential factor in its transmission. There is an index that represents the sensitivity of R_0 to changes in the parameter Υ. Thus, by employing partial derivatives, we can calculate the variations in all parameters in the R_0 equation.

The formula demonstrating the R_0 sensitivity index concerning the parameter Υ is:

$$\Gamma_\Upsilon = (\frac{\partial R_0}{\partial \Upsilon})(\frac{\Upsilon}{R_0}) \tag{8}$$

where Υ is a parameter that describes R_0. A negative (positive) index signifies that an augmentation in the parameter Υ results in a reduction (an increase) of R_0. The sensitivity indices for the parameters $b, \beta, \lambda_1, \lambda_2, \sigma, \omega$, and γ can be derived from the basic reproduction number, as shown in Table 2. It is clear that among these six indices, R_0 exhibits the most significant sensitivity to variations in ω, γ, and σ.

Table 2. Sensitivity indices.

Parameters	The sensitivity index of R_0 with respect to the parameters	Indexes of sensitivity
b	1	Positive
β	1	Positive
λ_1	$\frac{bp\varphi\sigma\lambda_1}{R_0(\sigma+\gamma)(\sigma+\omega)(\sigma+\lambda_1)^2}$	Positive
λ_2	$\frac{bq\varphi\sigma\lambda_2}{R_0(\sigma+\gamma)(\sigma+\omega)(\sigma+\lambda_2)^2}$	Positive
σ	$-\sigma\left[\frac{p\frac{\lambda_1}{(\lambda_1+\sigma)^2}+q\frac{\lambda_2}{(\lambda_2+\sigma)^2}}{p\frac{\lambda_1}{\lambda_1+\sigma}+q\frac{\lambda_2}{\lambda_2+\sigma}}+\frac{2\sigma+\gamma+\omega}{(\sigma+\gamma)(\sigma+\omega)}\right]$	Negative
ω	$\frac{-\omega}{(\sigma+\omega)}$	Negative
γ	$\frac{-\gamma}{(\gamma+\sigma)}$	Negative

Global Sensitivity Analysis. The most crucial model parameters can be determined using global sensitivity analysis. Indeed, the most important characteristics are identified by combining Latin Hypercube Sampling (LHS) with the Partial Rank Correlation Coefficient (PRCC) [19]. The LHS is a stratified Monte Carlo sampling technique that makes equal probability intervals of sample size N out of the parameter distribution. Each interval is sampled just once, without any replacement. Additionally, every parameter's whole range is investigated. After ranking the inputs and outputs, PRCC indices are calculated. The PRCC analysis identifies the model's most influential parameters, some of which have a positive correlation and others a negative one with the number of infected nodes. This indicates that as the value of any parameter with a positive correlation increases, the number of infected nodes increases. Conversely, the number of infected nodes drops if the value of a parameter with negative correlation increases.

6 Simulations and Analysis of the Malware Propagation Model in WSNs

The simulation outcomes of the modified model and the discussion of the achieved results are presented in this section. In this section, based on its capabilities, we will use the ABM method to investigate stability and confirm the

obtained theoretical results. This method enables the precise computation of numerical solutions over time.

6.1 Local and Global Sensitivity Analysis of the Model Parameters

ω, σ, and γ are the most sensitive to changes among the parameters that characterize R_0. Let us describe how the parameters ω, σ, and γ of the model could control the spread of malware in WSN. The parameters $b = 0.4$, $\beta = 0.002$, $\lambda_1 = 0.002$, $\lambda_2 = 0.001$, $\sigma = 0.0001$, $\gamma = 0.003$, $\omega = 0.004$, $r = 1.5$, $L = 10$, and $p = 0.7$ will be fixed in order to examine the impact of the parameters ω, σ, and γ. Only the sensitive parameters will be changed.

First, we fix the parameter value $\omega = 0.004, 0.006, 0.008, 0.01$. A higher recovery rate of susceptible nodes ω leads to removing infected nodes from the WSN, as shown in Fig. 1. This figure illustrates how malware will become less prevalent throughout the network as recovery rates increase. This strategy can effectively stop malware from spreading. As illustrated in Fig. 1, the peak emerges earlier with fewer infected nodes in the WSN as the parameter ω value increases. The changes can be seen in Fig. 1, where the dynamic relation between time and infected nodes and time and recovered nodes are shown separately in Fig. 1. The dynamic relation between infected and recovered nodes is also shown in this figure for a range of ω values.

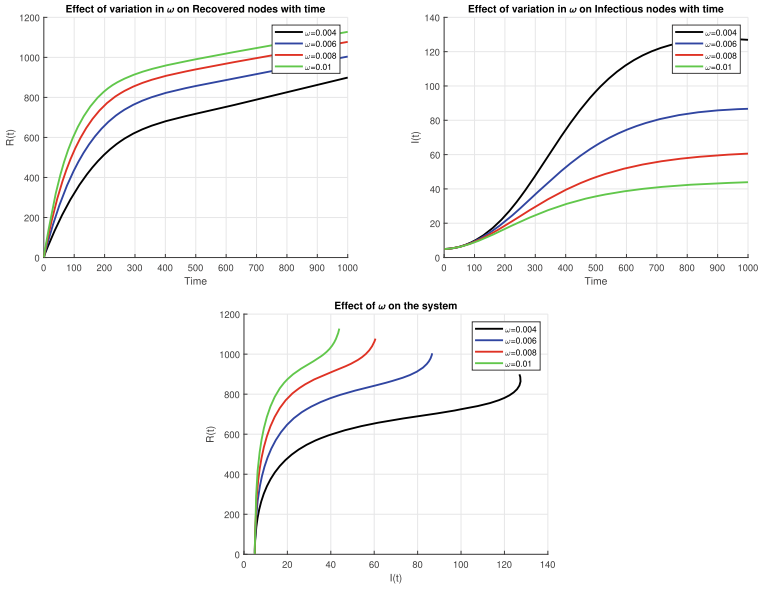

Fig. 1. Effect of ω on the system.

We change the parameter $\sigma = 0.0001, 0.0003, 0.0006, 0.0009$ to investigate the impact of σ on WSN. There are fewer infected and recovered nodes in WSN

as σ increases, which reduces the probability of becoming susceptible to malware spread. In WSN, the peak happens earlier when there are fewer infected nodes. The dynamic relation between the recovered, infected nodes with time is shown separately in Fig. 2. Under the given conditions, the number of recovered and infected nodes within WSN increases. It is evident from the data in Fig. 2 that the number of infected and recovered nodes in WSN is negatively correlated with the death rate. As a result, there will be a much lower chance of malware spreading throughout the network in this case. However, this removal procedure does not prevent infected nodes from spreading malware throughout the network. They may be categorized as spreaders because they are susceptible to being victimized by infected nodes. In particular, the dynamic link between time and infected people is shown in Fig. 2. In contrast, the other ones show the dynamic relation between infected-recovered nodes for varying values of σ, respectively. By changing the recovery rate γ to $\gamma = 0.003, 0.005, 0.007$, malware occurrence is significantly and quickly decreased. Increasing the parameter γ affects the number of infected nodes, slows the speed of the actively infected nodes, and may even prevent malware from spreading. An increase in γ similarly raises the number of recovered nodes over time from the WSN, as shown in Fig. 3. This method can stop malware from spreading within WSN. The number of recovered nodes increases as the parameter γ as a recovery rate increases in less time, as seen in the right image of Fig. 3. To be more specific, the dynamic relation between time and recovered nodes is depicted in Fig. 3. In contrast, the dynamic relation between infected and recovered nodes is also depicted in this figure for a range of γ values.

Figure 4 depicts the PRCC analysis findings of the most crucial parameters of the model, $b, \lambda_1, \lambda_2, \sigma, \omega, \gamma$, and β. Some of these parameters have a positive correlation with the number of infected nodes, while others have a negative correlation. According to the findings of the PRCC analysis, the proportion of nodes that propagate malware is positively correlated with $b, \lambda_1, \lambda_2, \sigma$, and β; when these parameters increase, the proportion of nodes that are affected by malware will also rise. However, σ has an almost insignificant effect in comparison with the other parameters. Moreover, it can be seen that b and β have a greater effect on the proportion of nodes that spread malware than λ_1 and λ_2. On the other side, ω, γ is negatively correlated with the proportion of nodes that spread malware. γ has an insignificant effect on it, whereas ω has a strong negative correlation. The aforementioned experiment outcomes are compatible with the results of the local sensitivity parameters shown in Figs. 1–3, demonstrating that the current proposed model is applicable to multi-malware propagation in WSNs.

6.2 Comparative Analysis with Existing Model

This part presents a comparison analysis between the proposed model and two existing models [3,21]. In the following case studies, we examine two distinct scenarios.

Case 1: For comparative study, in this case, we consider and fix all the parameters as: $b = 0.4, \beta = 0.002, \lambda_1 = 0.002, \lambda_2 = 0.001, \sigma = 0.0001, \gamma =$

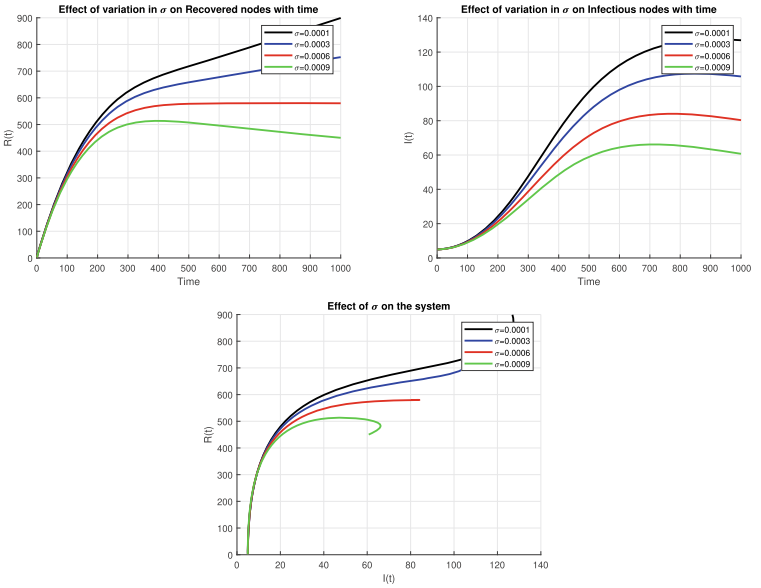

Fig. 2. Effect of σ on the system.

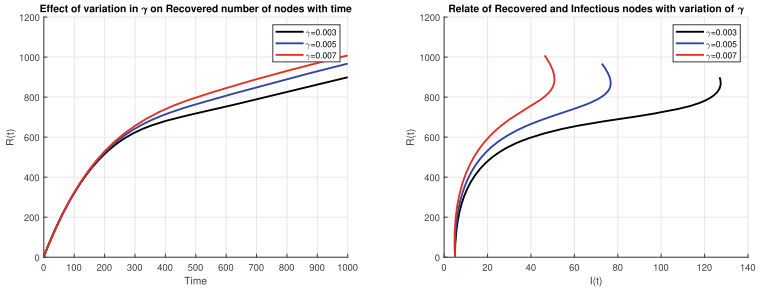

Fig. 3. Effect of recovery rate γ on the system.

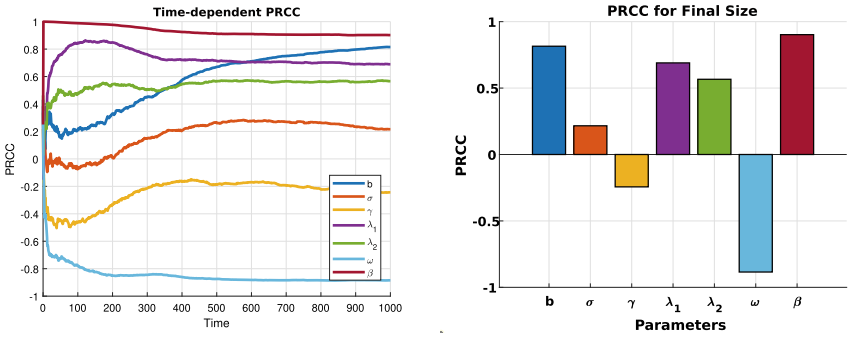

Fig. 4. PRCC of the parameters in the dynamical model.

$0.003, \omega = 0.004, L = 10, p = 0.7, N = 1000$, and we alter just the value of communication radius as $r = 1.0$ and $r = 1.5$. Table 3 summarizes the comparison of existing and proposed models. Considering Table 3, compared to the existing models, in the proposed model, a smaller number of susceptible nodes are affected as a result of a malware attack.

Table 3. Comparative study with different communication radius.

		Time		
		250	500	1000
Methods	r	Counts of Infected sensor nodes		
Ojha et al. [21]	1.0	280	240	180
Awasthi et al. [3]	1.0	3.8	10	25
Proposed method	1.0	3.8	10	22
Ojha et al. [21]	1.5	280	240	180
Awasthi et al. [3]	1.5	13	50	77
Proposed method	1.5	7.2	31	77

Case 2: In this case, we assume the parameters as: $b = 0.4, \beta = 0.001, \lambda_1 = 0.002, \lambda_2 = 0.001, \sigma = 0.001, \gamma = 0.003, \omega = 0.004, p = 0.7, N = 1000, r = 1.61$, and we only change the value of distributed node density as $\varphi = 11, L = 10$ and $\varphi = 16, L = 8$. Table 4 provides the comparison between existing and proposed models in this scenario. Table 4 shows that in the proposed strategy, fewer susceptible nodes are affected by malware attacks than in previous models.

Table 4. Comparative study with different distributed node density φ.

		Time		
		250	500	1000
Methods	φ	Counts of Infected sensor nodes		
Ojha et al. [21]	11	225	160	100
Awasthi et al. [3]	11	4.7	13.3	23
Proposed method	11	4.7	13.3	23
Ojha et al. [21]	16	225	160	100
Awasthi et al. [3]	16	13	22	25
Proposed method	16	3.2	7.1	10

Thus, it can be inferred from the aforementioned analysis that the design parameters, including the sensor node's communication radius, distributed node

density, and so on, must be determined following the requirements. Indeed, considering the additional needs of the sensor nodes that will be placed in the designated area is also crucial.

7 Conclusion

This work illustrated the propagation dynamics of multi-malware infections in WSNs using epidemiological modeling. The ABM approach was employed to confirm the theoretical findings and identify the problem of malware attacks. This study investigated the efficacy of the parameters and explored how various model parameters affect the propagation of malware in WSNs. The proposed model has given significant insight into the dynamics of multi-malware propagation in WSNs and provides a technique to control and prevent malware spread. The results of employing local and global sensitivity analysis were proposed. The study further provided a comparative analysis of the proposed model with existing ones.

Acknowledgements. This work was partially supported by SERICS (PE00000014) under PNRR MUR program funded by EU-NGEU.

References

1. Acarali, D., Rajarajan, M., Komninos, N., Zarpelão, B.B.: Modelling the spread of botnet malware in IoT-based wireless sensor networks. Secur. Commun. Netw. **2019**(1), 3745619 (2019). https://doi.org/10.1155/2019/3745619
2. AL-Mousawi, A.J., AL-Hassani, H.K.: A survey in wireless sensor network for explosives detection. Comput. Electric. Eng. **72**, 682–701 (2018). https://doi.org/10.1016/j.compeleceng.2017.11.013
3. Awasthi, S., et al.: An epidemic model for the investigation of multi-malware attack in wireless sensor network. IET Commun. **17**(11), 1274–1287 (2023). https://doi.org/10.1049/cmu2.12622
4. Chernikova, A., Gozzi, N., Perra, N., Boboila, S., Eliassi-Rad, T., Oprea, A.: Modeling self-propagating malware with epidemiological models. Appl. Netw. Sci. **8**(1), 52 (2023)
5. Conte, D., Farsimadan, E., Moradi, L., Palmieri, F., Paternoster, B.: Time-delay fractional optimal control problems: a survey based on methodology. In: Abdel Wahab, M. (ed.) FFW 2020 2020. LNME, pp. 325–337. Springer, Singapore (2021). https://doi.org/10.1007/978-981-15-9893-7_23
6. Conte, D., Farsimadan, E., Moradi, L., Palmieri, F., Paternoster, B.: A Galerkin approach for fractional delay differential equations using hybrid Chelyshkov basis functions. In: Gervasi, O. (ed.) Computational Science and Its Applications – ICCSA 2022, pp. 130–142. Springer International Publishing, Cham (2022). https://doi.org/10.1007/978-3-031-10522-7_10
7. Conte, D., Farsimadan, E., Moradi, L., Palmieri, F., Paternoster, B.: Numerical solution of delay Volterra functional integral equations with variable bounds. Appl. Numer. Math. **200**, 148–161 (2024). https://doi.org/10.1016/j.apnum.2023.05.002

8. De Santis, A., Farsimadan, E., Moradi, L., Palmieri, F.: Generalized defensive modeling of fake news propagation in social networks using fractional differential equations. IEEE Trans. Comput. Soc. Syst. **12**(2), 622–634 (2025). https://doi.org/10.1109/TCSS.2024.3492097
9. Farjamnia, G., Gasimov, Y., Kazimov, C.: Review of the techniques against the wormhole attacks on wireless sensor networks. Wireless Pers. Commun. **105**(4), 1561–1584 (2019)
10. Farsimadan, E., Moradi, L., Conte, D., Paternoster, B., Palmieri, F.: Comparison Between protein-protein interaction networks $CD4^+T$ and $CD8^+T$ and a numerical approach for fractional HIV infection of $CD4^+T$ cells. In: Gervasi, O., et al. (eds.) ICCSA 2021. LNCS, vol. 12949, pp. 78–94. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-86653-2_6
11. Farsimadan, E., Moradi, L., Palmieri, F.: A general study on the malware propagation models in wireless sensor networks. In: Gervasi, O. (ed.) Computational Science and Its Applications – ICCSA 2024 Workshops, pp. 83–99. Springer Nature Switzerland, Cham (2024). https://doi.org/10.1007/978-3-031-65223-3_6
12. Frutos-Bernal, E., Rodríguez-Rosa, M., Anciones-Polo, M., Martín-del Rey, A.: Analyzing malware propagation on wireless sensor networks: a new approach using queueing theory and HJ-BIPLOT with a sirs model. Mathematics **12**(1) (2024). https://doi.org/10.3390/math12010135
13. Geetha, R., Madhusudanan, V., Srinivas, M.N.: Influence of clamor on the transmission of worms in remote sensor network. Wireless Pers. Commun. **118**(1), 461–473 (2021)
14. Giri, P., Ng, K., Phillips, W.: Wireless sensor network system for landslide monitoring and warning. IEEE Trans. Instrum. Meas. **68**(4), 1210–1220 (2019). https://doi.org/10.1109/TIM.2018.2861999
15. Han, L., Zhou, M., Jia, W., Dalil, Z., Xu, X.: Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model. Inf. Sci. **476**, 491–504 (2019). https://doi.org/10.1016/j.ins.2018.06.017
16. Jamshidi, M., Zangeneh, E., Esnaashari, M., Darwesh, A.M., Meybodi, M.R.: A novel model of Sybil attack in cluster-based wireless sensor networks and propose a distributed algorithm to defend it. Wireless Pers. Commun. **105**(1), 145–173 (2019)
17. Liu, G., Chen, J., Liang, Z., Peng, Z., Li, J.: Dynamical analysis and optimal control for a seir model based on virus mutation in WSNs. Mathematics **9**(9) (2021). https://doi.org/10.3390/math9090929
18. Moradi, L., Farsimadan, E., D'Angelo, G., Carpentieri, B., Palmieri, F.: Epidemic analysis of the propagation of multiple malware infectious in wireless sensor networks. In: Barolli, L. (ed.) Advanced Information Networking and Applications, pp. 140–148. Cham (2025). https://doi.org/10.1007/978-3-031-87784-1_13
19. Ndii, M.Z., Djahi, B.S., Rumlaklak, N.D., Supriatna, A.K.: Determining the important parameters of mathematical models of the propagation of malware. In: Othman, M.A., Abd Aziz, M.Z.A., Md Saat, M.S., Misran, M.H. (eds.) Proceedings of the 3rd International Symposium of Information and Internet Technology (SYMINTECH 2018), pp. 1–9. Springer International Publishing, Cham (2019)
20. Nwokoye, C., Umeh, I.: Analytic-agent cyber dynamical systems analysis and design method for modeling spatio-temporal factors of malware propagation in wireless sensor networks. MethodsX **5**, 1373–1398 (2018). https://doi.org/10.1016/j.mex.2018.10.005

21. Ojha, R.P., Srivastava, P.K., Sanyal, G.: Mathematical model for wireless sensor network with two latent periods. In: Lobiyal, D.K., Mansotra, V., Singh, U. (eds.) Next-Generation Networks, pp. 497–504. Springer, Singapore (2018)
22. Ojha, R.P., Srivastava, P.K., Sanyal, G.: Improving wireless sensor networks performance through epidemic model. Int. J. Electron. **106**(6), 862–879 (2019). https://doi.org/10.1080/00207217.2019.1570563
23. Martín-del Rey, A.: A novel model for malware propagation on wireless sensor networks. Math. Biosci. Eng. **21**(3), 3967–3998 (2024). https://doi.org/10.3934/mbe.2024176
24. Roddam, A.W.: Mathematical epidemiology of infectious diseases: model building, analysis and interpretation. Int. J. Epidemiol. **30**(1), 186 (2001). https://doi.org/10.1093/ije/30.1.186
25. Shen, S., Huang, L., Zhou, H., Yu, S., Fan, E., Cao, Q.: Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in fog-cloud-based IoT networks. IEEE Internet Things J. **5**(2), 1043–1054 (2018). https://doi.org/10.1109/JIOT.2018.2795549
26. Shen, S., et al.: HSIRD: a model for characterizing dynamics of malware diffusion in heterogeneous WSNs. J. Netw. Comput. Appl. **146**, 102420 (2019). https://doi.org/10.1016/j.jnca.2019.102420
27. Shen, S., Zhou, H., Feng, S., Liu, J., Cao, Q.: SNIRD: disclosing rules of malware spread in heterogeneous wireless sensor networks. IEEE Access **7**, 92881–92892 (2019). https://doi.org/10.1109/ACCESS.2019.2927220
28. Singh, A., Awasthi, A.K., Singh, K., Srivastava, P.K.: Modeling and analysis of worm propagation in wireless sensor networks. Wireless Pers. Commun. **98**(3), 2535–2551 (2018)
29. Upadhyay, R.K., Kumari, S.: Bifurcation analysis of an e-epidemic model in wireless sensor network. Int. J. Comput. Math. **95**(9), 1775–1805 (2018). https://doi.org/10.1080/00207160.2017.1336550
30. Wu, G., Xie, L., Zhang, H., Wang, J., Shen, S., Yu, S.: STSIR: an individual-group game-based model for disclosing virus spread in social internet of things. J. Netw. Comput. Appl. **214**, 103608 (2023). https://doi.org/10.1016/j.jnca.2023.103608
31. Wu, J., Jiang, W., Mei, Y., Zhou, Y., Wang, T.: A survey on the progress of testing techniques and methods for wireless sensor networks. IEEE Access **7**, 4302–4316 (2019). https://doi.org/10.1109/ACCESS.2018.2887246
32. Wu, X., Cao, Q., Jin, J., Li, Y., Zhang, H.: Nodes availability analysis of NB-IoT based heterogeneous wireless sensor networks under malware infection. Wirel. Commun. Mob. Comput. **2019**(1), 4392839 (2019). https://doi.org/10.1155/2019/4392839
33. Xu, B., Lu, M., Zhang, H., Pan, C.: A novel multi-agent model for robustness with component failure and malware propagation in wireless sensor networks. Sensors **21**(14) (2021). https://doi.org/10.3390/s21144873
34. Ye, X., Xie, S., Shen, S.: SIR1R2: characterizing malware propagation in WSNs with second immunization. IEEE Access **9**, 82083–82093 (2021). https://doi.org/10.1109/ACCESS.2021.3086531
35. Yuan, Y., Huo, L., Wang, Z., Hogrefe, D.: Secure APIT localization scheme against sybil attacks in distributed wireless sensor networks. IEEE Access **6**, 27629–27636 (2018). https://doi.org/10.1109/ACCESS.2018.2836898
36. Zhang, H., Yang, S., Wu, G., Shen, S., Cao, Q.: Steady-state availability evaluation for heterogeneous edge computing-enabled WSNs with malware infections. Mob. Inf. Syst. **2022**(1), 4743605 (2022). https://doi.org/10.1155/2022/4743605

37. Zhang, Q., Zhang, W.: Accurate detection of selective forwarding attack in wireless sensor networks. Int. J. Distrib. Sens. Netw. **15**(1), 1550147718824008 (2019). https://doi.org/10.1177/1550147718824008
38. Zhou, H., Shen, S., Liu, J.: Malware propagation model in wireless sensor networks under attack–defense confrontation. Comput. Commun. **162**, 51–58 (2020). https://doi.org/10.1016/j.comcom.2020.08.009
39. Zhou, Y., Wang, Y., Zhou, K., Shen, S.F., Ma, W.X.: Dynamical behaviors of an epidemic model for malware propagation in wireless sensor networks. Front. Phys. **11** (2023). https://doi.org/10.3389/fphy.2023.1198410