A General Study on the Malware Propagation Models in Wireless Sensor Networks

Eslam Farsimadan(✉), Leila Moradi, and Francesco Palmieri

Department of Computer Science, University of Salerno, Fisciano 84084, Italy
{efarsimadan,lmoradi,fpalmieri}@unisa.it

Abstract. The propagation of malware in wireless sensor networks has recently garnered significant attention from researchers as a pressing issue. Wireless sensor networks consist of sensor nodes interconnected in a decentralized and distributed manner via wireless connectivity. Malware attacks can raise the energy consumption of wireless sensor network sensor nodes. The propagation of the infection initiates from a single infected node and utilizes neighboring nodes to increase throughout the entirety of the wireless sensor network. Hence, a comprehensive knowledge of spreading malware patterns in wireless sensor networks is advantageous. This paper examines the current models to analyze malware propagation in wireless sensor networks. This study presents a comprehensive overview of the strategies developed over the past decade. Equation-based epidemic models are observed to accurately represent the critical characteristics of wireless sensor networks and the spread of malware within them. The vulnerability of wireless sensor networks to malware attacks poses a significant challenge due to the limited defense capabilities of sensors. Consequently, the propagation of malware within these networks concerns the security community. This study examines the most crucial and up-to-date global epidemic models to explain network malware propagation.

Keywords: Wireless sensor networks · Malware propagation · Epidemic models · Basic reproductive number · Stability analysis

1 Introduction

Wireless Sensor Networks (WSNs) provide an instrument to connect the physical infrastructure with information and communication technologies [1]. WSNs have been extensively utilized for several innovative applications, including patient health care monitoring, military surveillance, and chemical or biological threats detection, including environmental monitoring, tracking, and targeting [2]. An essential concern in WSNs is the presence of several forms of security threats [3,4]. These networks operate in situations that are widely spread out and have limited resources. WSNs can be targeted by several types of attacks, including

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
O. Gervasi et al. (Eds.): ICCSA 2024 Workshops, LNCS 14816, pp. 83–99, 2024.
https://doi.org/10.1007/978-3-031-65223-3_6

denial of service attacks, worms, Sybil attacks, and other forms of malicious code. Moreover, with the extensive use of computer networks, the Internet, and WSNs, investigating attacks and malware detection, classification, and propagation models in these systems has become of great importance [5–7].

Malware creates one of the most significant problems in the contemporary society. The increasing number of malware is directly correlated with the rise in internet usage during this era, necessitating a substantial enhancement in computer security systems. Malicious software, also known as malware, is the product of several viruses designed to engage in harmful activities, such as stealing information or conducting scans. The primary objective of the malware is to inflict extensive damage to information and resources or to obtain unauthorized access to the network. Furthermore, it is defined as a category of computer software specifically created to harm the functionality of a legitimate user's device through various ways [8]. These dangers are pervasive in terms of their prevalence and the level of sophistication of the programs and viruses involved. The researchers proposed a range of remedies to safeguard against malware infections. Malware poses a significant challenge for contemporary internet users. The increase in malware attacks significantly threatens sensitive data and valuable computing resources. Hence, it is imperative to analyze the virus propagation model. Malware is an abbreviation for harmful software.

Malware has a significant impact on the growth and progress of organizations. Malware specifically targets internet-based apps. The Internet has become a fundamental and necessary part of our daily lives in the modern world. Over the past few years, there has been a significant rise in the prevalence of malware propagation in WSNs, and numerous study findings have been published on this topic by [9–11]. The security of WSNs is crucial due to the potentially sensitive nature of the data acquired by the sensor nodes [9]. Moreover, the majority of sensor devices can function in unsafe environments. WSNs are at risk from attacks, eavesdropping, and malware attacks that can disrupt their regular functioning [4,12] or perhaps cause their destruction [13]. According to [14], the propagation of malware has a more significant impact on WSNs than on the Internet.

Malware attacks provide serious security concerns for WSNs. The strategy of interleaving work and sleep schedules, high density, low communication range, power consumption (limited energy), and node topology all lead to the susceptibility to malware spreading. Based on the information provided, there are three distinct characteristics of the process of malicious software propagation in a WSN that are not present in other types of networks [15,16], as are listed following:

– Malware on a network, such as an Internet host, attempts to propagate itself by doing random scans of other hosts' IP addresses to infect them. As opposed to this, malware within a WSN node has the ability to propagate across its neighbors, allowing them to speak with the node directly.

– The malware on an active node can propagate to adjacent active nodes, but it does not infect inactive nodes. Furthermore, while a node is dormant, it cannot spread any malware to other nodes.
– Once the nodes' energy runs out, they transition into non-functional nodes that are no longer susceptible to infection and do not contribute to malware propagation in a WSN. When a dead node is infected with malware, it promptly vanishes from the network.

In order to investigate the propagation of malware in WSNs, researchers initially focused on traditional techniques of malware propagation observed on the Internet. The epidemic models have also been expanded to include this particular case [10]. The majority of mathematical models that address the dynamics of malware propagation in WSNs include systems of Ordinary Differential Equations (ODEs) (refer to [17,18]). The model presented in [19], which is based on a delayed ODE system and assumes that all network sensors are identical, is interesting.

The structure of this paper is as follows: The description and properties of WSNs are provided in Sect. 2. Section 3 focuses on the categorization of malware. The global models for malware spreading in WSN were recently proposed and are explained in Sect. 4. An example of one of the models described in Sect. 4 is selected to analyze the stability and basic reproductive number in Sect. 5. The conclusion is finally presented in Sect. 6.

2 Description of WSNs

A WSN is a set of networked microsensors dispersed in various locations without specified positions. Furthermore, in the absence of a particular configuration, it is near the phenomenon being assessed or situated within it. Each node is a sensor device that can autonomously arrange itself and is designed to observe and regulate physical phenomena. These phenomena include sensing various variables such as temperature, humidity, sound, vibration, pressure, pollutants, etc. The sensor node can gather data from its immediate environment and transmit it to the sink node, also known as the base station. In addition, they can analyze the collected data, retain it, and transmit it to other devices. While WSNs were initially developed and utilized for military applications like surveillance in conflict zones, their usage has now expanded to various other domains such as smart grids, smart water networks, intelligent transportation, smart homes, intelligent agriculture, and e-health [13,20,21]). The subsequent phases outline the implementation of a WSN:

– Placing: The sensors are put in the area that will be monitored (the sensor field). This placement could be random (the sensors are dropped from the air at random) or predictable (the sensors are placed in exact places already planned).
– Wake up and identify: Each sensor gets awake and identifies other sensors nearby.

– Connection: Using a predetermined topology (linear, star, tree, mesh, etc.), the sensor nodes are arranged into a connected network.
– Transmission: To send the gathered data, connecting paths that take the network consideration are calculated.

Fig. 1 illustrates the structure of the WSNs. The configuration of a WSN is determined by the specific applications it is designed for and is deployed in various types of terrain, including challenging conditions, to facilitate monitoring activities. WSNs have numerous applications, including military operations on battlefields, detecting fires in forests, and monitoring desert areas. The sensor network operates in a decentralized manner and utilizes wireless connections for the exchange of information. Malicious individuals and marketers take advantage of the weaknesses in the software and focus on a specific point of entry to deliver harmful software or worms into a WSN. When a WSN node becomes infected, it spreads gradually throughout the network by moving through neighboring nodes. Energy shortage is a significant issue in sensor networks. A malware assault reduces the energy of sensor nodes, causing a slowdown in the operation of the sensor network and an increase in network traffic. Researchers have discovered that biological worms spread is comparable to software-generated worms. Research on the security of WSNs related to malware assaults is currently a crucial area of study. To examine the dynamics of malware spreading in WSN, several researchers [22–26] have utilized epidemic modeling.
The characteristics of WSNs vary based on whether they are employed in indus-

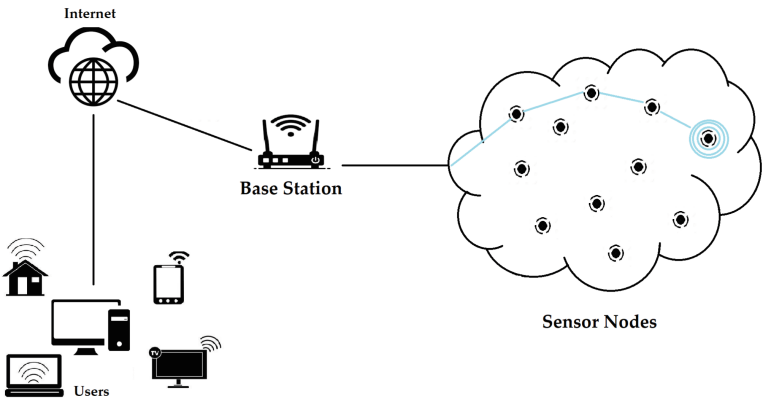

Fig. 1. Basic scheme of a WSNs

trial or conventional networks. In the first case, since all sensors are essential for the functioning of a plant, a malfunctioning node must be substituted. Conversely, in conventional networks, individual nodes have the potential to experience power loss or destruction. However, the network as a whole will remain operational. Since WSNs are inherently self-restoration capable, in the case of a

node loss, the network will find alternative paths for data packets to be transmitted. Therefore, the network will survive as a unified entity. Sensor nodes typically spend significant time in sleep mode due to their low power consumption.

3 Malware Classification

Categorizing malware is a challenging procedure. Software that allows illegal manipulation of a system is considered malicious. Malware exists in several forms and categories. To clarify, the malware makes the network temporarily inaccessible, resulting in significant harm or problems, and interrupts regular social or economic activities. The subsequent list presents prevalent categories of malware:

- **Virus:** A program reproduces by embedding its code into other programs for its advantage. Transmission of an infection can occur between machines and applications.
- **Worms:** Malicious software that replicates itself to damage and erase computer data and files. Worms can also encrypt data or transmit spam email messages. Unlike viruses, worms move themselves within their enclosures.
- **Trojan horse:** Trojan horses, posing as genuine software, engage in unauthorized and undesired activities. Trojans enable attackers to enter a fully operational computer and extract sensitive user data, including passwords and secret banking information.
- **Spyware:** Spyware is a computer software that constantly monitors and tracks user behavior. Without their awareness, the system clandestinely gathers user information, including frequently accessed online pages and payment card details, and transfers this data to the attackers.
- **Rootkit:** A rootkit program is a set of malicious software designed to infiltrate a computer network and grant unauthorized access to various types of malware within the system.
- **Ransomware:** Ransomware is a substantial threat to internet business and industry. Ransomware takes control of computers by encrypting data, disabling some applications, and allowing them to use operating systems only when their demands are met. The inquiries typically pertain to monetary funds. After making a financial payment, it is not guaranteed to restore power.
- **Adware:** Adware is a malware designed to continuously display advertisements on your computer. It is commonly bundled with free downloadable applications and software, such as free-to-play games.
- **Botnet:** Malicious software controls several devices, including computers, cell phones, and IoT devices. Then, they have been infected with malware and are under the control of a cybercriminal. A botnet is frequently employed to conduct denial-of-service attacks or spam operations. They can prevent unauthorized attacks on the system, distribute unsolicited emails, and steal information. Many users are often unaware that their infrastructure has been compromised by malware and is being used as part of a botnet.

- **Cookies:** Cookies are text documents that store data on the user's computer for a certain period. Internet browsers use them and are generally harmless; however, they can become dangerous when utilized by certain spyware.
- **Sniffers:** The software detects and tracks the organization's traffic. They explore different parcel fields and collect data to organize the virus attack.
- **Keyloggers:** The software detects and tracks the organization's traffic. It explores different parcel fields and collects data to organize the virus attack.
- **Spam:** Junk messages are another name for spam. These identical messages are generated and sent to multiple recipients simultaneously, consuming significant data bandwidth and slowing the system.

4 Global Models for Malware Propagation in WSN

Global models do not consider the unique features of particular devices or their specific interactions within local interactions. Therefore, they are expected to be evenly distributed and connected and have similar characteristics and behaviors. In our research, we delve into the complexity of the model variables, which are time-dependent and represent the number of devices in specific compartments. The interactions between these variables and parameters, which govern the system's dynamic behavior, are typically described by systems of ODEs. These equations, by capturing the temporal variability, allow us to determine how the observed characteristics change over time, despite not explicitly representing the interconnected actions of the devices in the model.

This section examines several epidemic models related to the spread of malware in WSNs. Various epidemic models have been employed to investigate malware propagation in WSNs. Kermack and Mckendrick [27] created the notion of epidemic modeling to analyze the transmission of infection among individuals. Academics employ this notion in diverse fields, such as social networks, computer networks, the Internet of Things, and WSN. The majority of malware propagation models, such as SI, SIR, SIRD, SEIRD, SEIVR, SILRD, etc., are based on and derived from the classical SIR model [10,18,28–36]. A mathematical model is constructed by making simplified assumptions about a significant problem, such as malware or network concerns. The assumptions are associated with the respective malware, network outages, and hacking incidents. WSN epidemic models aim to analyze the factors involved in transmitting harmful objects from a single node to the entire system. The malware propagation models in WSN consider various states of nodes, which are listed in Table 1. The number of sensor nodes in a WSN at any given time t is categorized into different states of nodes based on their condition. The number of nodes in any model is denoted as $N(t)$ that is eual to sumation of states of nodes for $t \geq 0$.

The researchers investigated the influence of secondary immunity on the spread of malware in WSNs. Generally, the basic reproductive number can be defined as the overall number of secondary infections induced by a single infectious device in a network where everyone is vulnerable. Therefore, the fundamental factor determining the system's evolution is a basic reproductive number

Table 1. Represent variables for epidemic models in WSN.

Subclasses of nodes	signify
S(t)	**Susceptible:** The sensor nodes currently remain unaffected by malware infections. However, they lack protection against attacks in WSNs
I(t)	**Infectious:** The sensor nodes in WSNs have been targeted by malware, which has the power to infect other susceptible nodes
V(t)	**Vaccinated:** The sensor nodes that are vaccinated are considered part of the vaccinated state
R(t)	**Recovered:** The sensor nodes were infected with malware and successfully disinfected by antivirus software
E(t)	**Exposed:** The sensor nodes have been infected with malware. However, they are not currently capable of infecting other nearby sensor nodes. Over time, these nodes become infected and spread malware in WSN
D(t)	**Dead:** The sensor nodes that have lost their energy can not communicate with other nodes, so they can not spread malware in a WSN

denoted as R_0. This coefficient is the most crucial threshold in the field of epidemiology. To examine the propagation patterns of the virus in WSN, the value of R_0 was calculated. It was determined that if $R_0 < 1$, the malware will cease to exist in WSNs. Conversely, if $R_0 > 1$, the number of infected nodes will continue to increase, and the malware will propagate across the entire WSN. Moreover, this parameter is crucial in analyzing the qualitative dynamics of the system of ordinary differential equations. Suppose $R_0 < 1$. In that case, the steady state without malware (the equilibrium point of the system when there are no infected devices) will be both locally and globally asymptotically stable. Otherwise, if $R_0 > 1$, the steady state of the malware epidemic (the point at which the number of infectious devices remains constant throughout time) will be locally and globally asymptotically stable.

4.1 SI Model

As proposed in [28–30], the SI model describes worm propagation behavior in WSNs. Several differential equations were used in the model's structure, and simulation results confirmed its validity. The authors attempted to ascertain the

fundamental elements of the network and the epidemic that hindered the dissemination of WSNs. The SI model is suggested for understanding the dynamics of worm propagation on the Internet [28–30]. According to the SI model, a host can be in one of two states: susceptible or infectious. The current state of a host infected by internet worms is called an infectious state. The susceptible state refers to the current condition of a worm that has not infected a host. This model delineates the attributes of malware propagation on the Internet. Figure 2 depicts the transitional condition of the sensor node, as mentioned in [28–30].

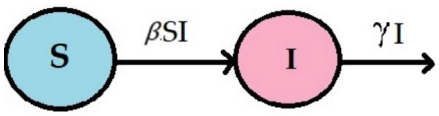

Fig. 2. Transition state diagram of the SI model [30,31]

The SI model is formalized as follows:

$$\begin{cases} \frac{dS}{dt} = -\beta SI, \\ \frac{dI}{dt} = \beta SI - \gamma I. \end{cases} \tag{1}$$

These nodes is categorized into two distinct states. The parameters used in model formulation are defined in Table 2.

Table 2. Present parameters for SI model

Parameters	Description
β	Rate of susceptible node become infected
γ	Rate of infected node become recovered

The SI model does not consider cases where specific hosts may be destroyed due to heavy infection by Internet worms. Furthermore, it does not account for situations where the host may have immunity to the same class of worms eradicated from that host. Therefore, the SI model needs to be revised to depict the worm propagation process on the Internet accurately.

4.2 SIR Model

The SIR model is an expanded version of the SI model, commonly used to analyze the spread of malware over the internet. Nevertheless, the SI and SIR models are not explicitly designed for WNSs. Therefore, these models cannot facilitate

the spread of malware while considering the energy consumption of nodes in WSNs. The SIR model expands the SI model by incorporating the presence of infectious hosts who are immunized, isolated, or dead while assuming that all susceptible hosts remain active indefinitely. Nevertheless, any individual node inside a WSN can become inactive due to its energy consumption. Rozenberg proposed the SIR Model, which concentrates on the spread of malware on WSN. The conventional global epidemic model typically assumes a population of N(t) identical sensor nodes that are uniformly and randomly dispersed. This SIR epidemic model classifies the population into three categories: susceptible S(t), infected I(t), and removed R(t) individuals. This case involves the SIR model, a type of epidemic model proposed in [30,31]. The model can be accurately solved on different kinds of networks. The SIR model assumes that all the sensitive sensor nodes will operate indefinitely, without considering any sleep and work schedule interweaving [30,31]. Figure 3 depicts the transitional condition of the sensor node, as referenced in [30,31].

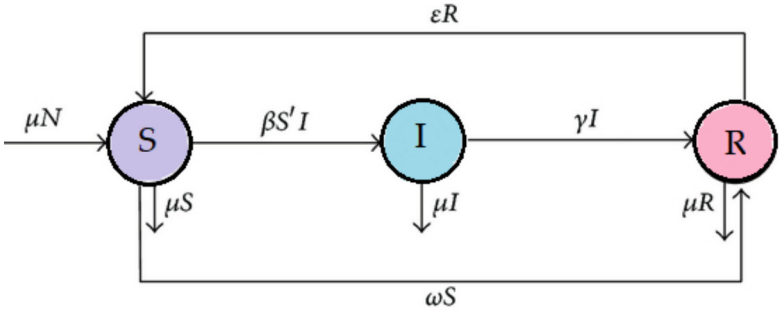

Fig. 3. Transition state diagram of the SIR model [30,31]

$$\begin{cases} \dfrac{dS}{dt} = \mu N - \xi SI - (\mu + \omega)S + \varepsilon R, \\ \dfrac{dI}{dt} = \xi SI - (\mu + \gamma)I, \\ \dfrac{dR}{dt} = \omega\, S + \gamma\, I - (\mu + \varepsilon)\, R, \end{cases} \tag{2}$$

where $\xi = \frac{\pi r^2}{L^2}\beta$. The number of sensor nodes in a WSN at any given time t is categorized into three distinct states: S(t), I(t), and R(t). The parameters employed in model formulation are described in Table 3.

Table 3. Present parameters for SIR model

Parameters	Description
β	Rate of susceptible node become infected
γ	Rate of infected node become recovered

4.3 SIRD Model

The Susceptible-Infectious-Recovered-Dead (SIRD) model was introduced in [31] for analyzing the dynamics of worm propagation in WSN. The SIRD model improved the SIR model by introducing the idea of the dead state of nodes in WSNs. It presented a novel model to evaluate the dynamics of worm propagation in WSNs. The SIRD model is derived from epidemic theory and comprises a set of differential equations. It can accurately represent the spread of worms in WSNs while considering the energy consumption of the network nodes. In the SIRD paradigm, susceptible sensor nodes become infected upon contact with the malware, and the infected nodes are restored to their original state after the malware is identified and eliminated. Conversely, specific devices restored to working order can again be susceptible if they lose resistance due to the antivirus software. Figure 4 illustrates the transition relationships between the states of the nodes.

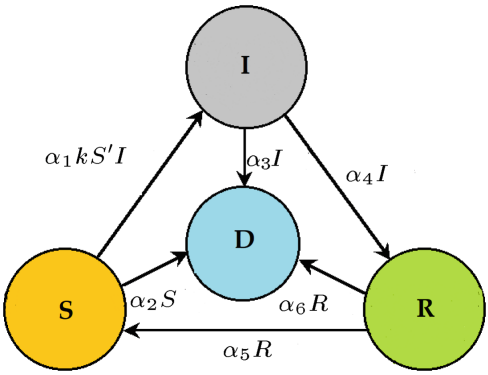

Fig. 4. Transition state diagram of the SIRD model [31]

$$\begin{cases} \dfrac{dS}{dt} = \dfrac{\alpha^2}{q^2}\alpha_1 k\, SI - \alpha_3 I - \alpha_4 I, \\ \dfrac{dE}{dt} = \alpha_5 R - \frac{\alpha^2}{q^2}\alpha_1 k\, SI - \alpha_2 S, \\ \dfrac{dI}{dt} = \alpha_4 I - \alpha_5 R - \alpha_6 R, \\ \dfrac{dR}{dt} = \alpha_2 S + \alpha_3 I + \alpha_6 R. \end{cases} \tag{3}$$

The number of sensor nodes in a WSN at any given time t is categorized into four individuals based on their current condition: S(t), I(t), R(t), and D(t). Table 4 lists the parameters employed in model formulation.

Table 4. Present parameters for SIRD model

Parameters	Description
k	The average number of malware residing in an infectious node
α_1	Rate of susceptible node become infected
α_2	Rate of susceptible node become dead
α_3	Rate of infected node become dead
α_4	Rate of infected node become recovered
α_5	Rate of recovered node become susceptible
α_6	Rate of recovered node become dead

4.4 SEIRD Model

The researchers in [32] introduced a Susceptible-Exposed-Infectious-Recovered-Dead (SEIRD) model established by epidemic theory. This model examined the spread of malware and developed strategies to control its propagation. The SEIRD model includes a system of differential equations that describe the relationship between various states of sensor nodes. The impact of early malware detection in WSN is elucidated by the revealed status in [32]. Early detection benefits in managing the spread of malware. Figure 5 depicts the transitional state of the sensor node.

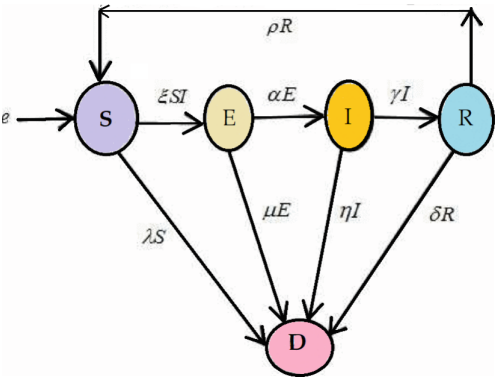

Fig. 5. Transition state diagram of the SEIRD model [32]

$$\begin{cases} \dfrac{dS}{dt} = e - \xi SI - \lambda S + \rho R, \\ \dfrac{dE}{dt} = \xi SI - (\mu + \alpha)E, \\ \dfrac{dI}{dt} = \alpha\, E - (\gamma + \eta)I, \\ \dfrac{dR}{dt} = \gamma\, I - (\delta + \rho)\, R, \\ \dfrac{dD}{dt} = \delta\, S + \mu\, E + \eta\, I + \delta\, R, \end{cases} \tag{4}$$

where $\xi = \frac{q^2}{L^2}\beta K$ and e is the constant rate at which new sensor nodes enter WSN. This proposed model includes five states: S(t), E(t), I(t), R(t), and D(t). The parameters used in model formulation are defined in Table 5.

Table 5. Present parameters for SEIRD model

Parameters	Description
K	The average number of malware present in each infected nodes
λ	Rate of Dead nodes
α	Rate of exposed node become infected
μ	Rate of exposed node become dead
γ	Recovery rate of infected node
η	Dead rate of infected node
ρ	Rate of recovered node become susceptible
δ	Rate of recovered node become dead

4.5 SEIVR Model

Therefore, a defense mechanism is necessary for protecting the WSN from malware attacks. To accomplish this goal, the authors in [33] introduced the Susceptible-Exposed-Infectious-Vaccinated-Recovered (SEIVR) model. The SEIVR model, based on epidemic theory, contains fractional differential equations. The SEIVR model considers two distinct infectious states of the sensor nodes. The states referred to are the "exposed state sensor node" and the "Infectious state sensor node." Malware transfers crucial data from one active sensor node to another in a WSN network. The suggested model provided a method to detect transitions of sensor nodes from a susceptible state to an infected state. This detection offers an opportunity to include additional methods for managing the sensor nodes and stabilizing WSNs under different situations. The SEIVR model investigated the dynamics of worm propagation in WSNs, with its transition state diagram depicted in Fig. 6. A set of differential equations is used to analyze the transmission dynamics of malware and the changing state of sensor nodes. The set of equations are expressed in the following form:

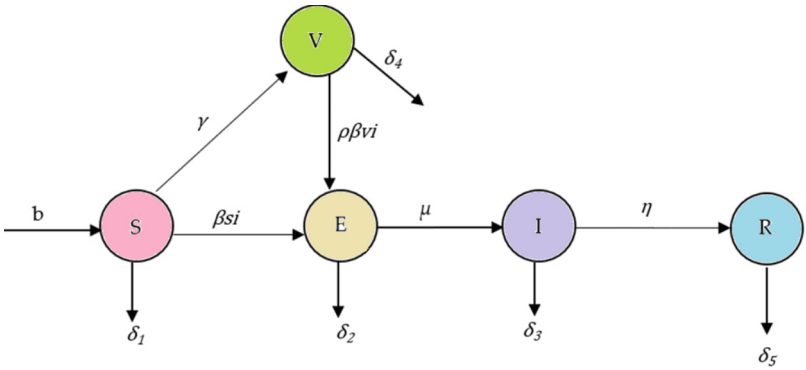

Fig. 6. Transition state diagram of the SEIVR model [33]

$$\begin{cases} \dfrac{dS}{dt} = b - \beta SI - (\sigma_1 + \lambda)S, \\ \dfrac{dE}{dt} = \beta SI + \rho\beta VI - (\sigma_2 + \eta)E, \\ \dfrac{dI}{dt} = \mu E - (\sigma_3 + \eta)I, \\ \dfrac{dV}{dt} = \lambda S - \rho\beta VI - \sigma_4 V, \\ \dfrac{dR}{dt} = \eta I - \sigma_5 R. \end{cases} \tag{5}$$

The total number of sensor nodes in a WSN at any given time t is categorized into five distinct states: $S(t)$, $V(t)$, $E(t)$, $I(t)$, and $R(t)$. The parameters used in model formulation are defined and explained in Table 6.

Table 6. Present parameters for SEIVR model

Parameters	Description
b	Susceptible rate
β	Vaccinated rate
μ	Rate of exposed node become infected
ρ	Rate of effectiveness vaccination
η	Recovery rate of Infected node
σ_1	Mortality rate of susceptible nodes
σ_2	Mortality rate of exposed nodes
σ_3	Mortality rate of infected nodes
σ_4	Mortality rate of vaccinated nodes
σ_5	Mortality rate of recovered nodes

5 Selected Example of One of the Models

In this section, a specific model example is chosen for analyzing stability and R_0 to evaluate the system. This section examines the SEIRD model described in [32] that relates to the spread of malware in WSN. The simulation findings are depicted in Figs. 7 and 8, representing the state of several categories of users in a WSN over time t. These categories include S, E, I, R, and D individuals.

- **Case 1**: Consider $L = 600, e = 0.38, K = 5, \alpha = 0.02, \beta = 0.03,\ \rho = 0.13, \lambda = 0.00005, \mu = 0.0004, \gamma = 0.07, q = 10, \eta = 0.006, \delta = 0.0004$. For $t = 0$, the values of $(S(0), E(0), I(0), R(0), D(0)) = (10000, 1, 1, 0, 0)$ respectively. In this case, $R_0 = 4.084967$. As Fig. 7 illustrates, malware continues to exist on the network if $R0 > 1$. Additionally, Fig. 7 shows that at first, the number of sensor nodes rises to a maximum value, decreases, and stabilizes as time passes. Other sensor network parameters similarly affect the maximum number of sensor nodes in the corresponding states. It discovered that the number of dead nodes rises linearly as sensor nodes' energy runs out.
- **Case 2**: Consider $L = 600, e = 0.3, K = 4, \alpha = 0.02, \beta = 0.03,\ \rho = 0.13, \lambda = 0.00005, \mu = 0.0004, \gamma = 0.07, q = 10, \eta = 0.006, \delta = 0.0004$. For $t = 0$ the values of $(S(0), E(0), I(0), R(0), D(0)) = (10000, 1, 1, 0, 0)$ respectively. As shown in Fig. 8, the number of sensor nodes in various stages varies over time. It is discovered that, at first, node state changes occur pretty slowly. Nevertheless, as time passes and reaches its maximum value, the number of nodes in the exposed, infected, and recovery states begins to decrease and eventually reaches zero. Figure 8 illustrates how, as sensor nodes' energy runs out, the number of dead nodes rises linearly while susceptible nodes are stable. In this case, $R_0 = 0.951837$. It has been noted that the virus gets eliminated from the WSN if $R0 < 1$. Therefore, in worm-free equilibrium, the system will be asymptotically stable.

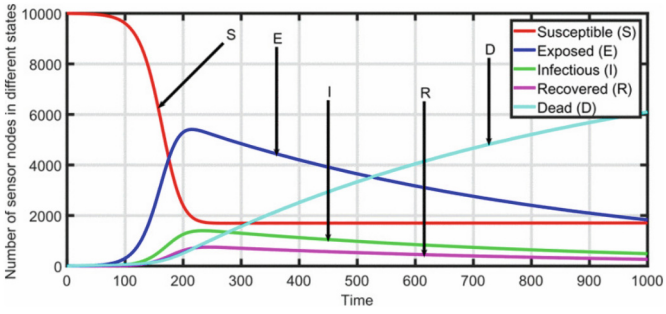

Fig. 7. The status of users in WSN when $R_0 > 1$ (case1) [32].

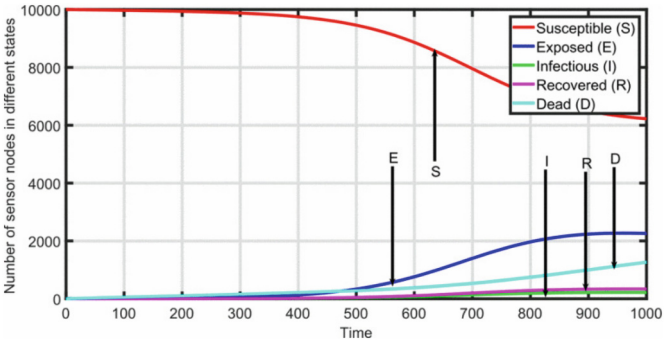

Fig. 8. The status of users in WSN when $R_0 < 1$ (case2) [32].

6 Conclusion

This work has provided an overview of the latest developments in research relative to malware propagation in WSN. This study analyzes epidemic models for the propagation of malware in WSNs. The majority of these systems are demonstrated to be based on ODE systems. As a result, neither individual characteristics nor the local interactions among the network parts are considered. Malware harms user computer systems by illegally acquiring personal and confidential information and compromising or turning off our security mechanisms. This study discussed the strategies that security researchers use to address these threats. The survey article explained several propagation techniques. This research analyzes the present status of global models used to simulate malware propagation in WSNs. Several models for WSNs have enhanced existing models of malware spread on the Internet by restricting the range of worm dissemination. Despite abundant studies and findings, numerous tasks still need to be accomplished.

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

References

1. Khan, S., Pathan, A.S.K., Alrajeh, N.A.: Wireless Sensor Networks: Current Status and Future Trends. CRC Press, Boca Raton (2013)
2. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Comput. Netw. **38**, 393–422 (2002)
3. Pathan, A.S.K., Lee, H.W., Hong, C.S.: Security in wireless sensor networks: issues and challenges. In: Proceedings of the 8th IEEE ICACT, vol. 2, pp. 1043–1048 (2006)
4. Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. Commun. ACM **47**, 53–57 (2004)

5. D'Angelo, G., Farsimadan, E., Ficco, M., Palmieri, F., Robustelli, A. Privacy-preserving malware detection in Android-based IoT devices through federated Markov chains. Future Gener. Comput. Syst. **148**, 93–105 (2023). https://doi.org/10.1016/j.future.2023.05.021
6. D'Angelo, G., Ficco, M., Palmieri, F.: Association rule-based malware classification using common subsequences of API calls. Appl. Soft Comput. **105**, 107234 (2021). https://doi.org/10.1016/j.asoc.2021.107234
7. D'Angelo, G., Farsimadan, E., Palmieri, F.: Recurrence plots-based network attack classification using CNN-autoencoders. In: Gervasi, O., et al. (eds.) ICCSA 2023. LNCS, vol. 14105, pp. 191–209. Springer, Heidelberg (2023). https://doi.org/10.1007/978-3-031-37108-0_13
8. Abu-Zaideh, S., Snober, M.A., Al-Haija, Q.A.: Smart boosted model for behavior-based malware analysis and detection. In: Joby, P.P., Balas, V.E., Palanisamy, R. (eds.) IoT Based Control Networks and Intelligent Systems. Lecture Notes in Networks and Systems, vol. 528, pp. 803–813. Springer, Singapore (2023). https://doi.org/10.1007/978-981-19-5845-8_58
9. Conti, M.: Secure Wireless Sensor Networks: Threats and Solutions. AIS, vol. 65. Springer, New York (2015). https://doi.org/10.1007/978-1-4939-3460-7
10. Feng, L., Song, L., Zhao, Q., Wang, H.: Modeling and stability analysis of worm propagation in wireless sensor network. Math. Prob. Eng. **2015**, Article ID 129598, 8 (2015). https://doi.org/10.1155/2015/129598
11. Hu, J., Song, Y.: The model of malware propagation in wireless sensor networks with regional detection mechanism. Commun. Comput. Inf. Sci. **501**, 651–662 (2015)
12. Sen, J.: A survey on wireless sensor network security. Int. J. Commun. Netw. Inf. Secur. **1**, 55–78 (2009)
13. Yang, Y., Zhu, S., Cao, G.: Improving sensor network immunity under worm attacks: a software diversity approach. In: Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 149–158 (2008)
14. Guo, W., Zhai, L., Guo, L., Shi, J.: Worm propagation control based on spatial correlation in wireless sensor network. In: Wang, H., Zou, L., Huang, G., He, J., Pang, C., Zhang, H.L., Zhao, D., Yi, Z. (eds.) APWeb 2012. LNCS, vol. 7234, pp. 68–77. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29426-6_10
15. Shengjun, W., Junhua, C.: Modeling the spread of worm epidemics in wireless sensor networks. In: 5th International Conference on Networking and Mobile Computing in Wireless Communications, pp. 1–4 (2009)
16. Queiruga-Dios, A., Hernández Encinas, A., Martín-Vaquero, J., Hernández Encinas, L.: Malware propagation models in wireless sensor networks: a review. In: Graña, M., López-Guede, J.M., Etxaniz, O., Herrero, Á., Quintián, H., Corchado, E. (eds.) SOCO/CISIS/ICEUTE -2016. AISC, vol. 527, pp. 648–657. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-47364-2_63
17. De, P., Das, S.K.: Epidemic Models, Algorithms, and Protocols in Wireless Sensor and Ad Hoc Networks. Wiley, New York (2008)
18. Shen, S., Li, H., Han, R., et al.: Differential game-based strategies for preventing malware propagation in wireless sensor networks. IEEE Trans. Inf. Forensic Secur. **9**(11), 1962–1973 (2014)
19. Zhu, L., Zhao, H.: Dynamical analysis and optimal control for a malware propagation model in an information network. Neurocomputing **149**, 1370–1386 (2015)
20. Fadel, E., et al.: A survey on wireless sensor networks for smart grid. Comput. Commun. **71**(1), 22–33 (2015)

21. Ojha, T., Misra, S., Raghuwanshi, N.S.: Wireless sensor networks for agriculture: the state-of-the-art in practice and future challenges. Comput. Electron. Agric. **118**, 66–84 (2015)
22. De, P., Liu, Y., Das, S.K.: An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks. IEEE Trans. Mob. Comput. **8**(3), 413–425 (2009)
23. De, P., Liu, Y., Das, S.K.: Deployment-aware modeling of node compromise spread in wireless sensor networks using epidemic theory. ACM Trans. Sensor Netw. **5**(3), 1–33 (2009)
24. Mishra, B.K., Keshri, N.: Mathematical model on the transmission of worms in Wireless Sensor Network. Appl. Math. Model. **37**(6), 4103–4111 (2013)
25. Ojha, R.P., Sanyal, G., Srivastava, P.K.: Pre-vaccination and quarantine approach for defense against worms propagation of malicious objects in wireless sensor networks. Int. J. Inf. Syst. Model. Des. (IJISMD) **9**(1), 01–20 (2018)
26. Haghighi, M.S., Wen, S., Xiang, Y., Quinn, B., Zhou, W.: On the race of worms and patches: modeling the spread of information in wireless sensor networks. IEEE Trans. Inf. Forensics Secur. **11**(12), 2854–2865 (2016)
27. Kermack, W.O., McKendrick, A.G.: A contribution to the mathematical theory of epidemics. Proc. R. Soc. London **115**, 700 (1927)
28. Khayam, S.A., Radha, H.: Using signal processing techniques to model worm propagation over wireless sensor networks. IEEE Signal Process. Maga. **23**(2), 164–169 (2006)
29. Zou, C.C., Towsley, D., Gong, W.: Modeling and simulation study of the propagation and defense of internet e-mail worms. IEEE Trans. Depend. Secure Comput. **4**, 105–118 (2007)
30. Kim, J., Radhakrishnan, S., Dhall, S.K.: Measurement and analysis of worm propagation on Internet network topology. In: Proceedings of IEEE International Conference on Computer Communications and Networks, Chicago, Illinois, USA, pp. 495–500 (2004)
31. Xiaoming, W., Yingshu, L.: An improved SIR model for analyzing the dynamics of worm propagation in wireless sensor networks. Chin. J. Electron. **18**(1), 8–12 (2009)
32. Biswal, S.R., Swain, S.K.: Model for study of malware propagation dynamics in wireless sensor network. In: 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, pp. 647–653 (2019). https://doi.org/10.1109/ICOEI.2019.8862736.
33. Srivastava, V., et al.: Generalized defensive modeling of malware propagation in WSNs using Atangana-Baleanu-Caputo (ABC) fractional derivative. IEEE Access **11**, 49042–49058 (2023). https://doi.org/10.1109/ACCESS.2023.3276351
34. 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
35. Shen, S., Zhou, H., Feng, S., Liu, J., Zhang, H., Cao, Q.: An epidemiology-based model for disclosing dynamics of malware propagation in heterogeneous and mobile WSNs. IEEE Access **8**, 43876–43887 (2020). https://doi.org/10.1109/ACCESS.2020.2977966
36. Zhang, H., Yang, S., Wu, G., Shen, S., Cao, Q.: Steady-state availability evaluation for heterogeneous edge computing-enabled WSNs with malware infections. Mobile Inf. Syst. **2022**, 1–16 (2022). https://doi.org/10.1155/2022/4743605