IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 20, 2021, accepted June 1, 2021, date of publication June 4, 2021, date of current version June 14, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3086531

SIR_1R_2: Characterizing Malware Propagation in WSNs With Second Immunization

XIAOTONG YE, SISI XIE, AND SHIGEN SHEN, (Member, IEEE)
Department of Computer Science and Engineering, Shaoxing University, Shaoxing 312000, China
Corresponding author: Shigen Shen (shigens@usx.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61772018.

ABSTRACT As an infrastructure of Internet of Things, WSNs (Wireless Sensor Networks) play a more and more important role. However, WSNs are vulnerable to malware and malware can destroy their data security and integrity, which motivates us to explore the role of malware propagation in WSNs. First, according to the actual propagation characteristics of malware in the WSNs and the process of the density change of all node types, we propose an epidemiology-based malware propagation model in consideration of a secondary immune mechanism. Then we set up differential equations to describe the propagation model. By solving differential equations, we can obtain two kinds of equilibrium points indicating that the density of all node types tends to be stable in the WSNs. One is to achieve an equilibrium where only susceptible nodes exist in the WSNs. The other is that malware always exists in the WSNs. Moreover, we prove the local and global stability of these two equilibrium points. Eventually, we analyze the influence and effect of the secondary immunity, forgetting mechanism and containment mechanism on malware propagation in the WSNs, and validate the proposed model through simulations.

INDEX TERMS wireless sensor networks, malware propagation, secondary immunization, epidemiology, equilibrium point.

I. INTRODUCTION

WSNs (Wireless Sensor Networks) [1], [2] have been utilized in many domains, for examples, monitoring temperature, pressure and humidity in the environment, detecting and monitoring animals and automobiles [3], [4], establishing wireless communication links in a wireless body sensor network [5]. These WSNs are self-organized networks that consist of thousands of sensor nodes (SNs) [6]. Generally, SNs are able to sense and collect information from the very harsh environments, and to return information according to some requests from users [7]. However, SNs have easily become attack targets of malware because of their resource constraints and weak defense capability [8], [9].

In fact, malware that was developed by external actors has seriously threatened the security of WSNs [10], [11]. It can disrupt or deny the normal operation of WSNs [12]–[14] after it attacks the WSNs successfully. Some studies have shown the harmfulness of malware on SNs. For example, an attacker may endanger an SN by its physical interfaces or tamper with the hardware itself so that malware can introduce wrong measurements to WSNs [15]. Besides, malware can attack an SN and propagate itself throughout the WSNs by infecting neighbor SNs with communications.

Therefore, the research of malware has become an issue that cannot be ignored in the field of WSNs security. In addition, it is very important to detect and defend malware accurately and effectively. Although SNs deployed in WSNs can update the software through a specific protocol without manual operation, it is impossible to completely avoid the WSNs being attacked by malware because these protocols are likely to open a door for attackers to propagate malware [16], [17]. In order to understand the propagation process of WSNs malware, epidemic models [18], [19] have been suggested as a viable approach.

Epidemic theory from epidemiology can be broadly employed to formulate malware propagation due to a strong similarity in the propagation process of biological viruses and WSNs malware [20]. Generally, typical states such as *Susceptible*, *Infectious*, and *Recovered* are combined to construct traditional deterministic epidemic models including SI (Susceptible-Infectious) and SIR (*Susceptible-Infectious-Recovered*) [21]. But there are some limitations when these general epidemic models are employed to formulate the

The associate editor coordinating the review of this manuscript and approving it for publication was Noor Zaman.

propagation process of WSNs malware. First, the infectious SN is unconscious of malware propagation and cannot terminate malware propagation. Second, the forgetting mechanism is not involved. When a period of time passes, the infectious SN may forget those SNs which have been infected. Third, it is not considered secondary immunity, or even multiple immunity.

We take secondary immunization into account that SNs in WSNs have a certain ability to resist malware and become basic immune SNs after being infected for a period of time, resulting in our epidemic model called SIR$_1$R$_2$. This is motivated by the fact that the recovered SNs may not be able to withstand the second malware attack, because other hidden vulnerabilities of SNs may be attacked by malware again. It can be found that the same SN can get stronger immunity after being attacked twice by malware than the case it recovers from the first attack. In other words, the SN is transformed into a basic immune SN after recovering from the first attack, and the SN can obtain a preliminary immune ability. Only after the SN survives under the second attack launched by malware, the SN will get the complete immune ability.

To perform this work, our methods include epidemic theory, stability theory of differential equations, the next-generation matrix method, Routh-Hurwitz stability theory, and Lyapunov functions. We employ epidemic theory to formulate our model SIR$_1$R$_2$. We achieve the equilibrium points of our epidemic model by stability theory of differential equations. We further compute the basic reproduction number using the next-generation matrix method. We also prove the locally and globally asymptotically stable points of our model with Routh-Hurwitz stability theory and rational Lyapunov functions, respectively.

Our contributions mainly lie as follows:

(1) We propose a novel epidemic model, SIR$_1$R$_2$, considering the secondary immunization based on the forgetting and containment mechanisms. This model accurately describes dynamic states of malware propagation in WSNs. We further build a corresponding mathematical model.

(2) According to the propagation model proposed, we establish the corresponding differential equations and obtain the equilibrium points. We further obtain the basic reproduction number to determine the propagation threshold of WSNs malware by solving the equations. Then we use the Routh-Hurwitz criterion to judge the local stability of equilibrium points through the eigenvalue equations of the corresponding Jacobian matrix. We also prove the global stability of equilibrium points by setting up rational Lyapunov functions.

(3) We conduct numerical simulations to verify the stability of the equilibrium points. Moreover, we qualitatively analyze the effects of secondary immunization on malware propagation in WSNs according to the parameters of the model.

We arrange the rest of this paper as follows. Related work and some WSNs malware propagation problems are summarized in Section II. Then, we set up a WSNs malware propagation model based on a secondary immunization mechanism in Section III. We verify the dependability of the propagation model through theoretic analyses in Section IV. Through simulation experiments, we show the effect of secondary immunization parameters on malware's propagation in WSNs in Section V. Finally, we draw our conclusions and give the future work.

II. RELATED WORK

Recently, there are many researchers who have done studies of epidemic propagation. We pick some representative models from those as the basis for our study of WSNs malware propagation. The most fundamental epidemic model is called SI, where any node can only change from the susceptible to the infectious. Afterwards, two classic models are formulated to model the propagation process of malware. The first model for dynamic propagation is the two-state SIS (Susceptible-Infectious-Susceptible) model [22], [23]. Here, nodes exist only in *healthy* or *infectious*. The susceptible nodes can be changed into infectious nodes, and malware can be removed from the infectious nodes and make them turn into the susceptible state again in that model. The second model is the SIR model, which can be described as the densities of susceptible, infectious, and recovered nodes. Furthermore, according to the simple states but different transformation rules, the SIRS model [24], [25] is also available.

Based on the above models, there are some models introducing other states according to characteristics of WSNs. Khanh [26] proposed an SIQR model by adding a new state called *Quarantine*, where a node effected by the detection program can be immediately labeled as a worm-node or be released after being quarantined for a period of time. Keshri and Mishra [27] presented an SEIR model, which shows the transmission dynamics of WSNs malware propagation with latency and immunity delays. Shen *et al.* [28] extended the traditional SIR model by adding the state *D* (Dead) in consideration of losing its functionality because of electricity exhaustion or malware attack. Moreover, some works have referred to the SEIR model which involves the state *E* (Exposed). Shen *et al.* [29] also proposed an SNIRD model including states *N* (iNsidious) and *D* (Dysfunctional), where *N* denotes the case that malware may prevent itself from being captured by the IDS and SNs in the state *N* have no intention to infect other neighbor SNs even if they have been infected. Sharma and Gupta [30] proposed another SEIR model based on cellular automata. López *et al.* [31] extended the SIR model to describe the propagation of random jamming attacks. Zhang *et al.* [32] presented an SAIS (Susceptible-Alert-infectious-Susceptible) model to evaluate the effectiveness of different alerting strategies. Acarali *et al.* [33] built a botnet propagation model called IoT-SIS for WSNs-based IoT networks, which reflects IoT-specific characteristics. Zhang and Xu [34] set up an SICD (Susceptible-Infectious-Cured-Dead) model with two particular non-cooperative states, which characterizes the D2D malware propagation process. Xia *et al.* [35] proposed an IDEPSR model for analyzing malware propagation in

TABLE 1. Individual characteristics and stability of WSNs malware propagation models.

Contributors	Model	Characteristics	Stability	
			Malware-free equilibrium	Endemic equilibrium
Wang et al. [10]	EiSIRS	SNs sleep and work interleaving	n/a	n/a
Shakya et al. [19]	SIR	Spatial correlation	Locally and globally asymptotically stable	Locally asymptotically stable
Ojha et al. [20]	SIQRS	SNs communication radius, SNs density	Locally and globally asymptotically stable	Locally asymptotically stable
Khanh [26]	SIQR	Malware quarantine	Locally and globally asymptotically stable	Locally and globally asymptotically stable
Keshri and Mishra [27]	SEIR	Time delay in exposed period and temporary immunity period	Locally and globally asymptotically stable	Locally asymptotically stable
Shen et al. [28]	HSIRD	Heterogeneous SN communication connectivity	Locally asymptotically stable	Locally asymptotically stable
Shen et al. [29]	SNIRD	Heterogeneous SN communication connectivity, malware hiding, and dysfunctional SN	n/a	n/a
Liu et al. [38]	SILS	Removal, charging, and reinfection of SNs	Locally and globally asymptotically stable	Locally and globally asymptotically stable
Mishra and Keshri [41]	SEIRS-V	Spatial and temporal dynamics	Locally and globally asymptotically stable	n/a
Shen et al. [42]	VCQPS	Heterogeneous and mobile SNs	Locally and globally asymptotically stable	n/a
Ojha et al. [43]	SEIQRV	Malware quarantine and vaccination	Locally and globally asymptotically stable	n/a
Zhang et al. [48]	SEIRD	Cellular Automaton-based analyses	Locally asymptotically stable	n/a
Zhu et al. [50]	SIR	Discrete time delay	Locally asymptotically stable	Locally asymptotically stable
Singh et al. [55]	SEIRV	SNs communication radius, SNs density	Locally and globally asymptotically stable	Locally asymptotically stable
This work	SIR_1R_2	SNs secondary immunization	Locally and globally asymptotically stable	Locally and globally asymptotically stable

city IoT, which reflects social features including the propagation and identification abilities of smart devices. Hernandez *et al.* [36] introduced an SCIRAS model for simulating the propagation process of zero-day malware, considering states *Susceptible*, *Carrier*, *Infectious*, *Recovered*, *Attacked*, and *Susceptible*. Li *et al.* [37] proposed a DDSEIR model to analyze CPS malware propagation based on states *Disseminate*, *Discriminate*, *Spread*, *Exposed*, *Ignorant*, and *Recover*. Liu *et al.* [38] presented an SILS model to disclose the epidemic process in wireless rechargeable sensor networks, which consists of states *Susceptible*, *Infectious*, *Low-energy*, and *Susceptible*. Muthukrishnan *et al.* [39] gave a WSNs node-based epidemic SITPS model including states *Susceptible*, *Infectious*, *Traced*, *Patched*, and *Susceptible*. Other typical models consist of an SEIRS-V [40] model introducing *V* (Vaccination) into the SEIR model, an SEIRS-V model considering the factor of software diversity [41], a VCQPS model reflecting both the heterogeneity and mobility of SNs [42], an epidemic SEIQRV model aggregating quarantine and vaccination techniques [43], a general SEIR model with vaccination-based sliding control [44], an SIC model reflecting countermeasure and network topology [45], an SIQVD model based on time delay and changeable infection probability [46], an SIR-based containment model with mobile social IoT [47], an SEIRD model with Cellular Automaton [48], as well as an SEIRS-V model considering the impact of mobile devices [49].

The improvement of the basic model can not only add specific states and introduce different influencing factors, but also affect malware propagation by introducing different influencing factors. To study dynamic behaviors, Zhu *et al.* [50] introduced discrete delay time and presented a novel malware propagation model with reaction-diffusion equations for MWSNs (mobile wireless sensor networks). Shen *et al.* [51] applied a continuous-time Markov chain to assess the reliability of clustered WSNs under malware diffusion. Moreover, Shen *et al.* [52] forecasted the malware propagation process by a developed non-zero-sum game. Xu *et al.* [53] introduced a Win-Stay, Lose-Likely-Shift approach into a Prisoner's Dilemma (PD) game framework because of some selfish nodes refusing cooperation in the WSNs. Farooq and Zhu [54] proposed an analytical model for exploring the D2D malware propagation. To clearly compare individual characteristics of WSNs malware propagation models herein, we make tabulation discussions listed in Table 1.

However, there are still some WSNs malware propagation problems to be solved. One is how to describe the scene that an SN can only gain most immunity after the first infection, but not completely resist the unknown malware. The other is how to express the immunity increment after the number of infectious SNs increases. Herein, we try to solve both two problems by supplementing a complete immune state to the traditional SIR model, taking

into account the forgetting and containment mechanisms in WSNs.

III. BUILDING A MALWARE PROPAGATION MODEL CONSIDERING SECONDARY IMMUNIZATION

We set up a state transition diagram of WSNs malware propagation considering secondary immunity. For this aim, we supplement a new type of an SN which has stronger immunity against malware called completely recovered state based on the original SIR model. Consequently, we construct a novel epidemic model SIR$_1$R$_2$, where all SNs are belonged to be in one of four possible states:

1) Susceptible state (S): The SNs in state S have not been contaminated by WSNs malware and they are defenseless to WSNs malware.
2) Infectious state (I): The SNs in state I have been contaminated by WSNs malware and these SNs may successfully contaminate some SNs in state S.
3) Basically recovered state (R_1): The SNs in state R_1 are cleaned off malware for the first time, and have a basic ability to resist malware and may be contaminated again.
4) Completely recovered state (R_2): The SNs in state R_2 are transformed from SNs in R_1, which is to reflect the fact that SNs will have stronger immunity against malware after being contaminated and recovered again.

Next, we illustrate our WSNs malware propagation model, SIR$_1$R$_2$, as described in Fig. 1. Susceptible SNs are contaminated by malware due to mutual communication, and they will be transformed into infectious SNs which can propagate the malware and infect other SNs. Generally, we cure infectious SNs by patching security programs and they are able to build up their basic resistance to the known malware. Infectious SNs can be naturally changed into basically recovered SNs based on the stimulus from malware under the influence of the containment mechanism. If basically recovered SNs do not have sufficient immunity, they may be infected by the same kind of malware again. Thus, these SNs' states will be changed from R_1 into R_2 after being infected and recovered from the same malware again. With time going by, any infectious SNs may be changed into susceptible SNs due to the existence of unknown malware. In addition, we may patch SNs so that susceptible SNs may have immunity to specific malware. This stimulus causes susceptible SNs to be changed to recovered ones directly.

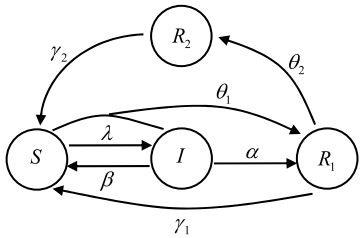

FIGURE 1. Node state transition diagram.

According to characteristics of SNs and propagation characteristics of malware in the WSNs under the secondary immune mechanism, we introduce $S(t)$, $I(t)$, $R_1(t)$, and $R_2(t)$ at time t to be the density of SNs in states S, I, R_1, and R_2, respectively. We can easily achieve

$$S(t) + I(t) + R_1(t) + R_2(t) = 1. \tag{1}$$

To make the WSNs work meaningfully, we impose an infectious SN in the WSNs at least and no recovered SNs. Moreover, the number of all the remaining susceptible SNs in the WSNs should obviously be much larger than 1. Thus, we can achieve

$$\begin{cases} S(t) \approx 1 \\ I(t) \approx 0 \\ R_1(t) = 0 \\ R_2(t) = 0 \end{cases} \tag{2}$$

Because the transformation probabilities of all kinds of SNs should be in [0, 1], we can obtain

$$\begin{cases} 0 \le \alpha, \beta, \lambda, \gamma_1, \theta_1, \gamma_2, \theta_2 \le 1 \\ \gamma_2 < \gamma_1 \\ \theta_2 < \theta_1 \end{cases} \tag{3}$$

Then, we can formulate the WSNs malware propagation model by a system including a group of differential equations as

$$\begin{cases} \dfrac{dS(t)}{dt} = -(\lambda + \theta_1)S(t)I(t) + \beta I(t) + \gamma_1 R_1(t) + \gamma_2 R_2(t) \\ \dfrac{dI(t)}{dt} = \lambda S(t)I(t) - \alpha I(t) - \beta I(t) \\ \dfrac{dR_1(t)}{dt} = \alpha I(t) + \theta_1 S(t)I(t) - \gamma_1 R_1(t) - \theta_2 R_1(t) \\ \dfrac{dR_2(t)}{dt} = -\gamma_2 R_2(t) + \theta_2 R_1(t) \end{cases} \tag{4}$$

IV. ANALYZING STABILITY OF OUR MODEL WITH SECONDARY IMMUNE

A. EQUILIBRIUM POINTS

Here, we adopt the method of letting the differential equations in system (4) be zero, in order to attain equilibrium points of our WSNs malware propagation model. After calculation, we can achieve two equilibria for tuple $< S, I, R_1, R_2 >$. Then we can determine the threshold of our model to indicate whether WSNs malware will propagate steadily or vanish gradually.

For convenience of description, we represent the densities of SNs in I, S, R_1, and R_2 be x_1, x_2, x_3, and x_4, respectively. In this manner we set

$$\mathbf{x} = [x_1 \quad x_2 \quad x_3 \quad x_4]^{\mathrm{T}}. \tag{5}$$

We define the function $F_i(\mathbf{x})$ as the speed of i-th type of SNs being changed into infectious ones. $V_i^+(\mathbf{x})$ and $V_i^-(\mathbf{x})$

represent the rates of i-th type of SN increment and decrement. Let

$$V_i(\mathbf{x}) = V_i^-(\mathbf{x}) - V_i^+(\mathbf{x}). \tag{6}$$

According to (4), we can obtain

$$F_i(\mathbf{x}) = \begin{cases} \lambda SI & i = 1 \\ 0 & i = 2, 3, 4 \end{cases} \tag{7}$$

We set

$$\mathbf{F} = [F_1(\mathbf{x}) \quad F_2(\mathbf{x}) \quad F_3(\mathbf{x}) \quad F_4(\mathbf{x})]^{\mathrm{T}}, \tag{8}$$

then obtain

$$\mathbf{F} = [\lambda SI \quad 0 \quad 0 \quad 0]^{\mathrm{T}}. \tag{9}$$

We set

$$\mathbf{V} = [\, V_1(\mathbf{x}) \quad V_2(\mathbf{x}) \; V_3(\mathbf{x}) \quad V_4(\mathbf{x}) \,]^{\mathrm{T}}, \tag{10}$$

where $V_1(\mathbf{x})$ denotes the rate of infectious SNs being changed into other SN types, and $V_2(\mathbf{x})$, $V_3(\mathbf{x})$, and $V_4(\mathbf{x})$ denote the density change rates of susceptible SNs, basic recovered SNs, and completely recovered SNs in the WSNs, respectively. According to (4), (6) and (10), we can obtain

$$\mathbf{V} = \begin{bmatrix} \beta I + \alpha I \\ (\lambda + \theta_1)SI - \gamma_1 R_1 - \gamma_2 R_2 - \beta I \\ -\alpha I + \gamma_1 R_1 + \theta_2 R_1 - \theta_1 SI \\ \gamma_2 R_2 - \theta_2 R_1 \end{bmatrix}. \tag{11}$$

We define $\dot{x}_i$ as the change rate of i-th type in the WSNs. Then, we obtain

$$\dot{x}_i = F_i(\mathbf{x}) - V_i(\mathbf{x}). \tag{12}$$

When the density of all SN types does not change, meaning that all change rates are 0, malware propagation in the WSNs reaches an equilibrium state. We thus obtain

$$\begin{cases} \dot{x}_1 = \lambda S(t)I(t) - \alpha I(t) - \beta I(t) = 0 \\ \dot{x}_2 = -(\lambda + \theta_1)S(t)I(t) + \beta I(t) + \gamma_1 R_1(t) + \gamma_2 R_2(t) = 0 \\ \dot{x}_3 = \alpha I(t) + \theta_1 S(t)I(t) - \gamma_1 R_1(t) - \theta_2 R_1(t) = 0 \\ \dot{x}_4 = -\gamma_2 R_2(t) + \theta_2 R_1(t) = 0 \end{cases} \tag{13}$$

By solving (13), we can get two equilibrium points $\mathbf{Y}_1 = [\, S_1 \; I_1 \; R_{11} \; R_{12} \,]^{\mathrm{T}}$ and $\mathbf{Y}_2 = [\, S_2 \; I_2 \; R_{21} \; R_{22} \,]^{\mathrm{T}}$ where

$$\mathbf{Y}_1 = [1 \quad 0 \quad 0 \quad 0]^{\mathrm{T}} \tag{14}$$

and

$$\mathbf{Y}_2 = \begin{bmatrix} \dfrac{\alpha + \beta}{\lambda} \\ \dfrac{(\lambda - \alpha - \beta)(\lambda\alpha + \theta_1\alpha + \theta_1\beta)\gamma_2}{(\gamma_2 + \theta_2)(\lambda\alpha + \theta_1\alpha + \theta_1\beta) + \lambda\gamma_2(\gamma_1 + \theta_1)} \\ \dfrac{(\lambda - \alpha - \beta)(\lambda\alpha + \theta_1\alpha + \theta_1\beta)\gamma_2^2}{\lambda(\gamma_2 + \theta_2)(\lambda\alpha + \theta_1\alpha + \theta_1\beta) + \lambda^2\gamma_2(\gamma_1 + \theta_1)} \\ \dfrac{\theta_2(\lambda - \alpha - \beta)(\lambda - \alpha - \beta)\gamma_2}{\lambda(\gamma_2 + \theta_2)(\lambda\alpha + \theta_1\alpha + \theta_1\beta) + \lambda^2\gamma_2(\gamma_1 + \theta)} \end{bmatrix}. \tag{15}$$

According to (14) and (15), we get a malware-free equilibrium that no malware in the WSNs will exist when the WSNs reaches the equilibrium point $\mathbf{Y}_1$. At that time, there are only susceptible SNs. We also get a malware-endemic equilibrium $\mathbf{Y}_2$. In other words, when the WSNs reaches the equilibrium point $\mathbf{Y}_2$, malware propagates steadily in the network, at the same time, the density of all SN types in the WSNs keeps dynamic equilibrium.

B. BASIC REPRODUCTION NUMBER

Generally, the next-generation matrix method can be applied to obtain the basic reproduction number $\rho(fv^{-1})$, which is in fact "the spectral radius of the next-generation matrix" [56]. Here, f and v denote the advent and transition rates of infectious SNs at malware-free equilibrium $\mathbf{Y}_1$, respectively. According to (7), (14), and (15), we can get

$$\begin{cases} f = \left.\dfrac{\partial F_1(\mathbf{x})}{\partial I}\right|_{\mathbf{Y}_1} = \lambda \\ v = \left.\dfrac{\partial V_1(\mathbf{x})}{\partial I}\right|_{\mathbf{Y}_1} = \alpha + \beta \end{cases} \tag{16}$$

The basic reproduction number $\rho(fv^{-1})$ can then be achieved by

$$\rho(fv^{-1}) = \frac{\lambda}{\alpha + \beta}. \tag{17}$$

In (17) $\rho(fv^{-1})$ is generally regarded as R_0, which reflects the number of infectious SNs within an average disease cycle of $1/r$ (r is the cure rate) when all of them are susceptible. The threshold 1 is used to determine whether the malware will be dead or not. If $R_0 > 1$, the specific malware will continue to propagate in the WSNs, and the density of malware will increase continuously. Until a certain value is reached, the density of infectious SNs will stabilize, and the density of all kinds of SNs will be in a dynamic equilibrium state. When $0 < R_0 < 1$ exists, the malware cannot survive in the WSNs, and the malware will gradually disappear in the WSNs at last.

C. STABILITY ANALYSIS OF EQUILIBRIUM POINTS

Theorem 1: When $R_0 < 1$, $\mathbf{Y}_1$ is the locally asymptotically stable point.

Proof: The Jacobian matrix of (4) is

$$\mathbf{J} = \begin{bmatrix} -(\lambda + \theta_1)I & -(\lambda + \theta_1)S + \beta & \gamma_1 & \gamma_2 \\ \lambda I & \lambda S - \alpha - \beta & 0 & 0 \\ \theta_1 I & \alpha - \theta_1 S & -\gamma_1 - \theta_2 & 0 \\ 0 & 0 & \theta_2 & -\gamma_2 \end{bmatrix}. \tag{18}$$

For $S(t) = 1 - I(t) - R_1(t) - R_2(t)$, the Jacobian matrix of (4) for the malware-infected WSNs can be changed into

$$\mathbf{J}_1 = \begin{bmatrix} \lambda S - \alpha - \beta & 0 & 0 \\ \alpha - \theta_1 S & -\gamma_1 - \theta_2 & 0 \\ 0 & \theta_2 & -\gamma_2 \end{bmatrix}. \tag{19}$$

At the equilibrium point $\mathbf{Y}_1$, we get

$$\mathbf{J}_1(\mathbf{Y}_1) = \begin{bmatrix} \lambda-\alpha-\beta & 0 & 0 \\ \alpha-\theta_1 & -\gamma_1-\theta_2 & 0 \\ 0 & \theta_2 & -\gamma_2 \end{bmatrix}. \tag{20}$$

Let ϑ be the eigenvalue of (20), we get the characteristic polynomial as

$$\vartheta^3 + m_1\vartheta^2 + m_2\vartheta + m_3 = 0, \tag{21}$$

where

$$\begin{cases} m_1 = \gamma_2+\theta_1+\alpha+\beta-\lambda \\ m_2 = (\alpha+\beta-\lambda)(\gamma_1+\theta_2)+(\alpha+\beta-\lambda+\gamma_1+\theta_2)\gamma_2 \\ m_3 = (\alpha+\beta-\lambda)(\gamma_1+\theta_2)\gamma_2 \end{cases} \tag{22}$$

From $R_0 = \frac{\lambda}{\alpha+\beta} < 1$, we can get

$$\alpha+\beta-\lambda > 0. \tag{23}$$

Moreover, from (3), we know $0 \le \gamma, \theta \le 1$ and

$$\begin{aligned}(\gamma_2+\theta_1+\alpha+\beta-\lambda)(\alpha+\beta-\lambda)(\gamma_1+\theta_2) \\ > (\alpha+\beta-\lambda)(\gamma_1+\theta_2)\gamma_2.\end{aligned} \tag{24}$$

Therefore, it is obvious that

$$\begin{cases} m_1 > 0 \\ m_2 > 0 \\ m_2 \cdot m_1 > m_3 \end{cases} \tag{25}$$

According to the criterion of Routh-Hurwitz stability [55], when $R_0 < 1$, $\mathbf{Y}_1$ is locally asymptotically stable. We complete the proof. □

Theorem 2: When $R_0 > 1$, $\mathbf{Y}_2$ is the locally asymptotically stable point.

Proof: According to (18) and $\frac{dR_2(t)}{dt} = -\gamma_2 R_2 + \theta_2 R_1 = 0$, the Jacobian matrix of (4) for the malware-infected WSNs can be changed into

$$\mathbf{J}_2 = \begin{bmatrix} -(\lambda+\theta_1)I & -(\lambda+\theta_1)S+\beta & \gamma_1 \\ \lambda I & \lambda S-\alpha-\beta & 0 \\ \theta_1 I & \alpha-\theta_1 S & -\gamma_1-\theta_2 \end{bmatrix}, \tag{26}$$

and the Jacobian matrix $\mathbf{J}_2$ at equilibrium point $\mathbf{Y}_2$ is

$$\mathbf{J}_2(\mathbf{Y}_2) = \begin{bmatrix} -(\lambda+\theta_1)I & -(\lambda+\theta_1)\dfrac{\alpha+\beta}{\lambda}+\beta & \gamma_1 \\ \lambda I & 0 & 0 \\ \theta_1 I & \alpha-\theta_1\dfrac{\alpha+\beta}{\lambda} & -\gamma_1-\theta_2 \end{bmatrix}, \tag{27}$$

where

$$I = \frac{(\lambda-\alpha-\beta)(\lambda\alpha+\theta_1\alpha+\theta_1\beta)\gamma_2}{(\gamma_2+\theta_2)(\lambda\alpha+\theta_1\alpha+\theta_1\beta)+\lambda\gamma_2(\gamma_1+\theta_1)}.$$

Let $\tilde{\vartheta}$ be the eigenvalue of (27), the characteristic polynomial is

$$\tilde{\vartheta}^3 + \tilde{m}_1\tilde{\vartheta}^2 + \tilde{m}_2\tilde{\vartheta} + \tilde{m}_3 = 0, \tag{28}$$

where

$$\begin{cases} \tilde{m}_1 = \lambda I+\theta_1 I+\gamma_2 \\ \tilde{m}_2 = I(\alpha\lambda+\alpha\theta_1+\beta\theta_1+\gamma_2\lambda+\gamma_2\theta_1) \\ \tilde{m}_3 = I\gamma_2(\alpha\lambda+\alpha\theta_1+\beta\theta_1). \end{cases} \tag{29}$$

According to $0 \le \alpha, \beta, \lambda, \gamma_1, \theta_1, \gamma_2, \theta_2 \le 1$ and $0 < I < 1$, it is obvious that $\tilde{m}_1 > 0$ and $\tilde{m}_3 > 0$ can be obtained. Further, we can get $\tilde{m}_3 < \tilde{m}_2$ and $\tilde{m}_3 < \tilde{m}_1$.

In summary, we get

$$\begin{cases} \tilde{m}_1 > 0 \\ \tilde{m}_3 > 0 \\ \tilde{m}_2 \cdot \tilde{m}_1 > \tilde{m}_3 \end{cases} \tag{30}$$

According to the criterion of Routh-Hurwitz stability, it can be obtained that $\tilde{m}_1 \cdot \tilde{m}_2 > \tilde{m}_3$ is valid. This completes the proof. □

Theorem 3: The equilibrium point $\mathbf{Y}_1$ is the globally asymptotically stable point when $R_0 < 1$.

Proof: We set up a Lyapunov function $L_1(t)$ as

$$L_1(t) = I(t), \tag{31}$$

whose derivative is

$$\begin{aligned}\frac{dL_1(t)}{dt} &= \frac{dI(t)}{dt} = \lambda SI - \alpha I - \beta I \\ &\le (\lambda-\alpha-\beta)I.\end{aligned} \tag{32}$$

When $R_0 < 1$, we can easily achieve $\lambda-\alpha-\beta < 0$ from (17). Thus,

$$\frac{dL_1(t)}{dt} = 0 \tag{33}$$

if and only if $I = 0$, which means

$$\lim_{t\to\infty} I(t) = 0. \tag{34}$$

We further achieve

$$\lim_{t\to\infty} S(t) = 1, \tag{35}$$

$$\lim_{t\to\infty} R_1(t) = 0, \tag{36}$$

and

$$\lim_{t\to\infty} R_2(t) = 0 \tag{37}$$

by substituting (34) into our model system (4). Consequently, $\mathbf{Y}_1$ is globally attractive. Joined by the conclusion that $\mathbf{Y}_1$ is locally asymptotically stable from Theorem 1, $\mathbf{Y}_1$ is the globally asymptotically stable point when $R_0 < 1$. This completes the proof. □

Theorem 4: The equilibrium point $\mathbf{Y}_2$ is the globally asymptotically stable point when $R_0 > 1$.

Proof: In this case we set up a Lyapunov function $L_2(t)$ as

$$L_2(t) = \frac{1}{2}\zeta_1(R_0-1)(S-S_2)^2 + \zeta_2(I-I_2-I_2\ln I), \tag{38}$$

where ζ_1 and ζ_2 are parameters. We then achieve the derivative of $L_2(t)$ as

$$\begin{aligned}
&\frac{dL_2(t)}{dt} \\
&= \zeta_1(R_0-1)(S-S_2)\frac{dS}{dt} + \zeta_2(1-\frac{I_2}{I})\frac{dI}{dt} \\
&= -\zeta_1(R_0-1)(S-S_2)^2(\lambda+\theta_1)I \\
&\quad +(S-S_2)(\zeta_1(R_0-1)(\beta I+\gamma_1 R_1+\gamma_2 R_2-(\lambda+\theta_1)S_2 I) \\
&\quad +\zeta_2\lambda(I-I_2)) \\
&\triangleq -\zeta_1(R_0-1)(S-S_2)^2(\lambda+\theta_1)I+(S-S_2)\Lambda. \qquad (39)
\end{aligned}$$

Let $\Lambda = 0$ by adjusting ζ_1 and ζ_2, thus

$$\frac{dL_2(t)}{dt} = -\zeta_1(R_0-1)(S-S_2)^2(\lambda+\theta_1)I \le 0 \qquad (40)$$

for any $\zeta_1 > 0$. When $R_0 > 1$,

$$\frac{dL_2(t)}{dt} = 0 \qquad (41)$$

if and only if $S = S_2$, which means

$$\lim_{t\to\infty} S(t) = S_2. \qquad (42)$$

We further achieve

$$\lim_{t\to\infty} I(t) = I_2, \qquad (43)$$

$$\lim_{t\to\infty} R_1(t) = R_{21}, \qquad (44)$$

and

$$\lim_{t\to\infty} R_2(t) = R_{22} \qquad (45)$$

by substituting (42) into our model system (4). Consequently, $\mathbf{Y}_2$ is globally attractive. Joined by the conclusion that $\mathbf{Y}_2$ is locally asymptotically stable from Theorem 2, $\mathbf{Y}_2$ is the globally asymptotically stable point when $R_0 > 1$. This completes the proof. □

Therefore, in the case of $\mathbf{Y}_1$ from Theorems 1 and 3, no matter how many infectious SNs appear in the WSNs, when the density of all kinds of SNs in the network stabilizes, the infectious SNs will disappear and malware can no longer propagate in the WSNs. On the other hand, when $R_0 > 1$, the equilibrium point $\mathbf{Y}_1$ is unstable, because if $R_0 > 1$ meaning $\frac{\lambda}{\alpha+\beta} > 1$, then $m_2 > 0$ in (21). According to the Routh-Hurwitz stability criterion [55], it can be concluded that $\mathbf{Y}_1$ is unstable. So as long as one SN in the WSNs is infected by malware, malware will propagate throughout the WSNs and will not disappear.

From Theorems 2 and 4, it can be concluded that if there are infectious SNs in the WSNs satisfying $R_0 > 1$, the WSNs will achieve the dynamic equilibrium at $\mathbf{Y}_2$, that is, the density of four SN types will keep a dynamic equilibrium, which also shows that malware will not be eliminated in the WSNs.

V. VALIDATING OUR MALWARE PROPAGATION MODEL WITH SECONDARY IMMUNITY

Here, we will use numerical simulation experiments to analyze the influence and effect of the secondary immunity, forgetting mechanism and containment mechanism on WSNs malware propagation, and validate the proposed model SIR$_1$R$_2$ through simulations. Besides, we will thoroughly analyze the correctness and stability of our model. In the experiments, we set $\gamma_2 = \gamma_1^2$ and $\theta_2 = \theta_1^2$. As for the function of secondary immunity, we set the initial densities of all kinds of SNs in the WSNs as $S(0) = 0.6$, $I(0) = 0.1$, $R_1(0) = 0.3$, and $R_2(0) = 0$, respectively, because completely recovered SNs cannot exist without secondary immunity.

A. VALIDATION FOR MODEL SIR$_1$ R$_2$

1) STABILITY VALIDATION FOR THE MALWARE-FREE EQUILIBRIUM

Figs. 2 and 3 respectively study the propagation process of malware in the WSNs with secondary immunity where the basic production numbers are different. To this end, we set the initial densities of all kinds of SNs in the WSNs as $S(0) = 0.6$,

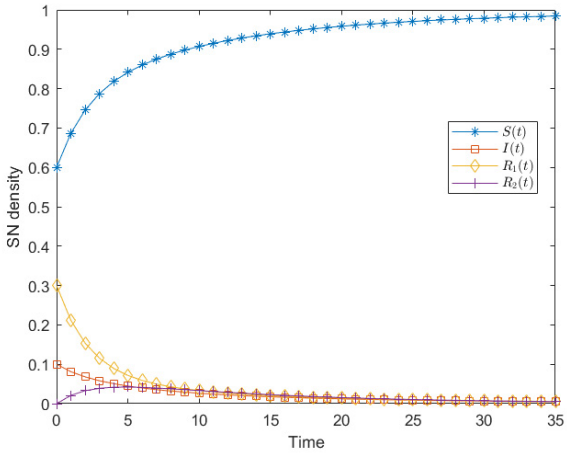

FIGURE 2. Different SN densities in the model SIR$_1$R$_2$ where $R_0 = 0.9$.

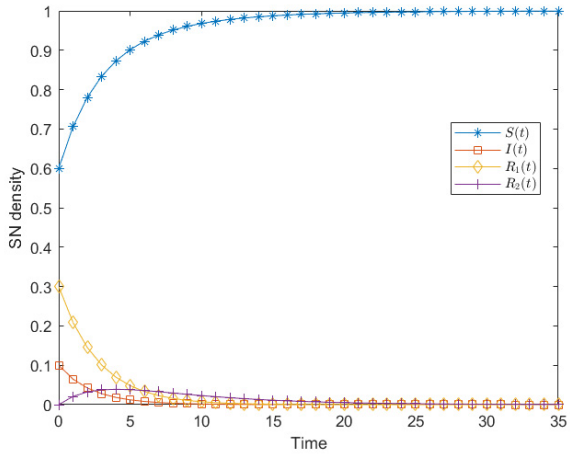

FIGURE 3. Different SN densities in the model SIR$_1$R$_2$ where $R_0 = 0.2$.

$I(0) = 0.1$, $R_1(0) = 0.17$, and $R_2(0) = 0.13$. Moreover, we set $\alpha = 0.2$, $\beta = 0.3$, $\lambda = 0.45$, $\theta_1 = 0.3$, $\gamma_1 = 0.4$, $\theta_2 = 0.09$, and $\gamma_2 = 0.16$ in Fig. 2, where the basic production number $R_0 = 0.9$. On the other hand, we set $\alpha = 0.2$, $\beta = 0.3$, $\lambda = 0.1$, $\theta_1 = 0.3$, $\gamma_1 = 0.4$, $\theta_2 = 0.01$, and $\gamma_2 = 0.16$ in Fig. 3, where $R_0 = 0.2$. It is obvious that R_0 in the two cases are both less than 1, which satisfies the condition of Theorems 1 and 3. By observing the simulation results, we see that malware finally disappears in the WSNs. That is, the densities of the infectious SNs and the two types of recovered SNs are 0, and the density of the susceptible SNs is 1. The results reflect that the propagation equilibrium point is (1, 0, 0, 0), which validates stability for the malware-free equilibrium in the model with secondary immunization.

From the comparison between Fig. 2 and Fig. 3, in the case of $R_0 < 1$, the closer R_0 is to 0, the faster the malware in the WSNs will die out and reach the malware-free equilibrium. For example, when $t = 20$, the density of the SNs reaches (1, 0, 0, 0) in Fig. 3; but in Fig. 2, this state can only be reached in the future.

2) STABILITY VALIDATION FOR THE MALWARE-ENDEMIC EQUILIBRIUM

Here, we validate stability for the malware-endemic equilibrium of our model, as depicted in Figs. 4 and 5. We set $\alpha = 0.3$, $\beta = 0.3$, $\lambda = 0.9$, $\theta_1 = 0.3$, $\gamma_1 = 0.3$, $\theta_2 = 0.09$, and $\gamma_2 = 0.09$ in Fig. 4, where $R_0 = 1.5$. From Fig. 4, the equilibrium point is about (0.661, 0.097, 0.125, 0.117). On the other hand, in Fig. 5, we set $\alpha = 0.3$, $\beta = 0.3$, $\lambda = 1.2$, $\theta_1 = 0.3$, $\gamma_1 = 0.3$, $\theta_2 = 0.09$, and $\gamma_2 = 0.16$, where $R_0 = 2.0$, and the equilibrium point is about (0.498, 0.153, 0.178, 0.171). Both two cases indicate $I(t) > 0$; therefore, when $R_0 > 1$, the malware will eventually propagate stably in the WSNs. From Figs. 4 and 5, it can be obtained that the closer R_0 is to 1, the faster the WSNs will reach the stable state. In addition, the slower WSNs will reach the stable state when R_0 is larger and farther away from 1.

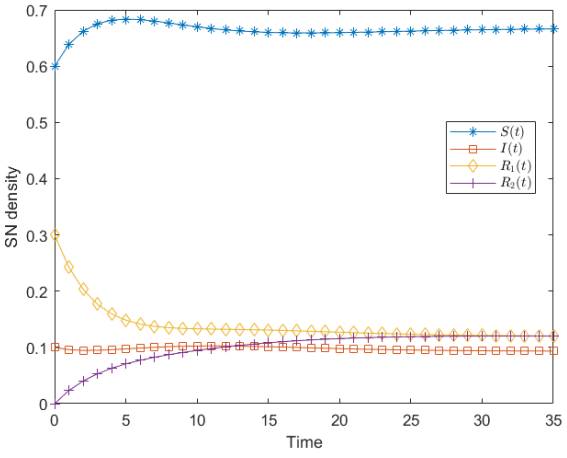

FIGURE 4. Different SN densities in the model SIR$_1$R$_2$ where $R_0 = 1.5$.

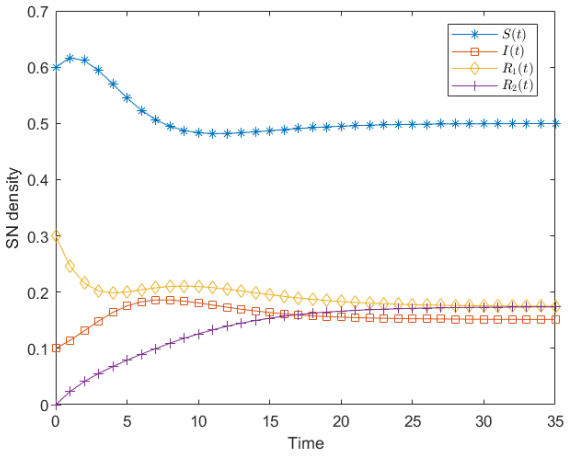

FIGURE 5. Different SN densities in the model SIR$_1$R$_2$ where $R_0 = 2.0$.

B. VALIDATION FOR THE EFFECT OF THE FORGETTING AND CONTAINMENT MECHANISM

First of all, Fig. 6 shows different cases of infectious SNs under different θ indicating the effect of the forgetting mechanism. It can be seen that under the condition $R_0 > 1$, when β increases, the density of the infectious SNs will be less at last. Moreover, under the condition of $R_0 < 1$, when β increases, the infectious SNs will die out faster. Therefore, it can be concluded that the larger the probability of forgetting mechanism is, the less the number of infectious SNs reaching to the dynamic equilibrium will be. The forgetting mechanism has restrained malware propagation in the WSNs.

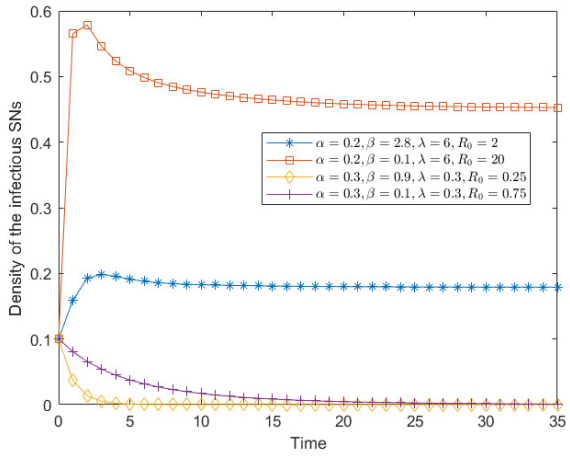

FIGURE 6. Effect of the forgetting mechanism in the model SIR$_1$R$_2$ under $\theta_1 = 0.3$, $\gamma_1 = 0.3$, $\theta_2 = 0.09$, and $\gamma_2 = 0.09$.

Then, we concentrate on the effect of the containment mechanism. From Fig. 7, when $R_0 > 1$ the density of the infectious SNs will be less in the case of larger α, on the contrary, the density of the infectious SNs will be larger. However, under the condition $R_0 < 1$, the density of the infectious SNs will tend to 0 faster and the WSNs will reach the equilibrium faster when α is larger. It can be concluded the

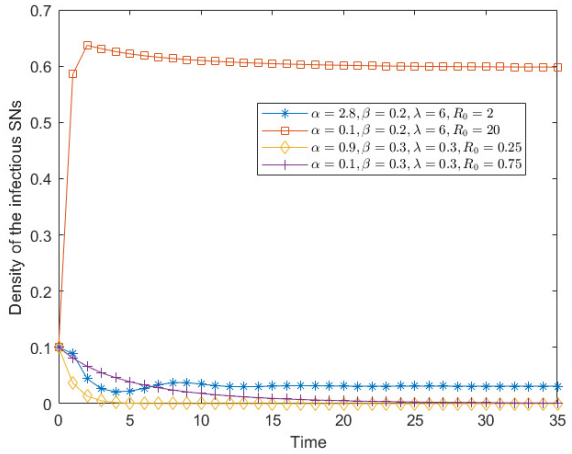

FIGURE 7. Effect of the containment mechanism in the model SIR_1R_2 under $\theta_1 = 0.3$, $\gamma_1 = 0.3$, $\theta_2 = 0.09$, and $\gamma_2 = 0.09$.

containment mechanism has restrained malware propagation in the WSNs.

C. COMPARISION WITH THE BASIC SIR MODEL

To show the effectiveness of our secondary immunity-based model SIR_1R_2, we compare it with the basic SIR model. Figs. 8–10 respectively study the density change process of various SNs in the WSNs over time, showing the WSNs malware propagation process under the function of secondary immunity.

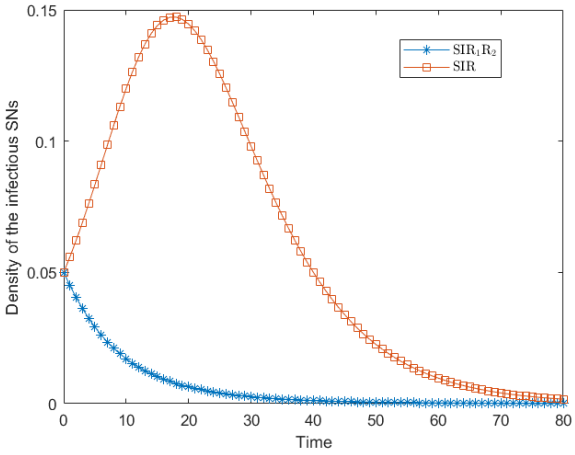

FIGURE 8. Comparison of changeable densities of infectious SNs in two models.

Without loss of generality, we set two models with the same parameter values. In addition, we choose $S(t)$, $I(t)$, $R(t)$ as contrast aspects, because they can reflect the effectiveness of malware diffusion models. We set $S(t) = 0.88$, $I(t) = 0.05$, and $R(t) = 0.07$ ($R_1(t) = 0.07$ and $R_2(t) = 0$ in the model SIR_1R_2) at beginning.

From Fig. 8, the density of infectious SNs in the proposed model SIR_1R_2 with secondary immunity drops and reaches

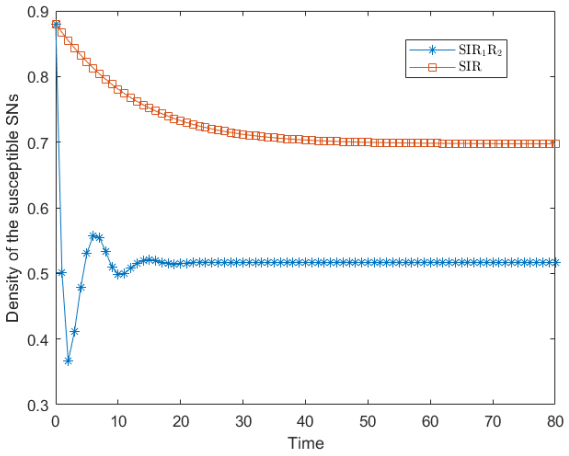

FIGURE 9. Comparison of changeable densities of susceptible SNs in two models.

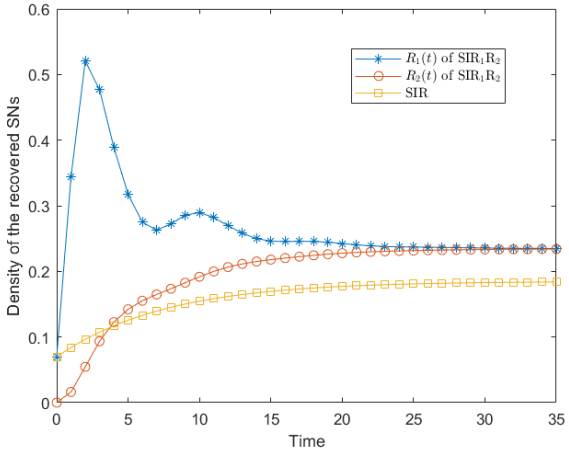

FIGURE 10. Comparison of changeable densities of recovered SNs in two models.

0 just spending about 40 units of time. However, it takes longer and longer for the infectious SNs to be died out in the SIR model. More specially, the density of infectious SNs changes to 0 at approximately 80 units of time in the SIR model.

According to Figs. 9 and 10, the proposed model SIR_1R_2 with secondary immunity is more effective than the basic SIR model in terms of reaching the equilibrium. When malware propagation in the WSNs reaches the equilibrium, there is a higher density of recovered SNs and a lower density of susceptible SNs in the proposed SIR model. Consequently, the defense capability of the entire WSNs becomes stronger.

VI. CONCLUSION

Based on the theory of infectious diseases, a novel epidemic model called SIR_1R_2 considering the secondary immunity mechanism was presented. We have achieved differential equations characterizing the dynamics of various SNs belonging to states *Susceptible*, *Infectious*, *basically recovered*, and

completely recovered. We have shown that no malware in the WSNs will exist when the WSNs reach the malware-free equilibrium, and that malware propagates steadily when the WSNs reach the endemic equilibrium point. As a result, the stability of our model with secondary immune have been analyzed based on the basic reproduction number obtained. In this manner, we have explained the malware propagation behaviors under different actual conditions.

From the view of a practical point, the theoretical results presented in this paper is of guiding significance to inhibit malware propagation in WSNs. Based on Theorems 1−4, the infectious SNs will disappear and malware can no longer propagate in the WSNs when $R_0 < 1$, whereas malware will propagate throughout the WSNs and will not disappear when $R_0 > 1$. In addition, secondary immunity has an impact on malware propagation in WSNs in despite of $R_0 > 1$ or $R_0 < 1$. Further, when $R_0 < 1$, the malware propagation in the WSNs will decelerate if the value of R_0 is approaching 1, while the propagation will accelerate if the value of R_0 is approaching 1 when $R_0 > 1$. On the other hand, in the case of $R_0 < 1$, malware disappears faster when θ becomes larger; however, in the case of $R_0 > 1$, the final density of malware will be less when θ becomes smaller. Moreover, we concentrate on the forgetting mechanism and containment mechanism. They both have a deterrent effect on malware propagation in WSNs.

Although we have solved the problem on how to characterize the WSNs malware propagation dynamics through the proposed model SIR$_1$R$_2$ with the secondary immunity, there still exists an interesting work on how to present optimal control strategies. The alternative methods may include SN immunity optimization, transformation probabilities optimization, and WSNs topology optimization and so on. We plan to do it in the future.

REFERENCES

[1] I. G. A. Poornima and B. Paramasivan, "Anomaly detection in wireless sensor network using machine learning algorithm," *Comput. Commun.*, vol. 151, pp. 331–337, Feb. 2020.

[2] S. Feng, S. Shen, L. Huang, A. C. Champion, S. Yu, C. Wu, and Y. Zhang, "Three-dimensional robot localization using cameras in wireless multimedia sensor networks," *J. Netw. Comput. Appl.*, vol. 146, Nov. 2019, Art. no. 102425.

[3] J. Liu, X. Wang, G. Yue, and S. Shen, "Data sharing in VANETs based on evolutionary fuzzy game," *Future Gener. Comput. Syst.*, vol. 81, pp. 141–155, Apr. 2018.

[4] H. Radhappa, L. Pan, J. X. Zheng, and S. Wen, "Practical overview of security issues in wireless sensor network applications," *Int. J. Comput. Appl.*, vol. 40, no. 4, pp. 202–213, Oct. 2018.

[5] S. Shen, K. Hu, L. Huang, H. Li, R. Han, and Q. Cao, "Optimal report strategies for WBANs using a cloud-assisted IDS," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 11, Nov. 2015, Art. no. 184239.

[6] W. Elsayed, M. Elhoseny, S. Sabbeh, and A. Riad, "Self-maintenance model for wireless sensor networks," *Comput. Electr. Eng.*, vol. 70, pp. 799–812, Aug. 2018.

[7] A. Belfkih, C. Duvallet, and B. Sadeg, "A survey on wireless sensor network databases," *Wireless Netw.*, vol. 25, no. 8, pp. 4921–4946, Nov. 2019.

[8] S. Shen, L. Huang, H. Zhou, S. Yu, E. Fan, and Q. Cao, "Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in fog-cloud-based IoT networks," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1043–1054, Apr. 2018.

[9] S. Shen, H. Li, R. Han, A. V. Vasilakos, Y. Wang, and Q. Cao, "Differential game-based strategies for preventing malware propagation in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1962–1973, Nov. 2014.

[10] X. Wang, Q. Li, and Y. Li, "EiSIRS: A formal model to analyze the dynamics of worm propagation in wireless sensor networks," *J. Combinat. Optim.*, vol. 20, no. 1, pp. 47–62, Jul. 2010.

[11] L. Xiao, Y. Li, X. Huang, and X. Du, "Cloud-based malware detection game for mobile devices with offloading," *IEEE Trans. Mobile Comput.*, vol. 16, no. 10, pp. 2742–2750, Oct. 2017.

[12] M. B. Bahador, M. Abadi, and A. Tajoddin, "HLMD: A signature-based approach to hardware-level behavioral malware detection and classification," *J. Supercomput.*, vol. 75, no. 8, pp. 5551–5582, Aug. 2019.

[13] J. Liu, S. Shen, G. Yue, R. Han, and H. Li, "A stochastic evolutionary coalition game model of secure and dependable virtual service in sensor-cloud," *Appl. Soft Comput.*, vol. 30, pp. 123–135, May 2015.

[14] J. Liu, J. Yu, and S. Shen, "Energy-efficient two-layer cooperative defense scheme to secure sensor-clouds," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 408–420, Feb. 2018.

[15] V. P. Illiano and E. C. Lupu, "Detecting malicious data injections in wireless sensor networks: A survey," *ACM Comput. Surveys*, vol. 48, no. 2, Nov. 2015, Art. no. 24.

[16] P. De, Y. Liu, and S. K. Das, "An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 8, no. 3, pp. 413–425, Mar. 2009.

[17] P. De, Y. Liu, and S. K. Das, "Deployment-aware modeling of node compromise spread in wireless sensor networks using epidemic theory," *ACM Trans. Sensor Netw.*, vol. 5, no. 3, pp. 1–33, May 2009.

[18] H. Zhou, S. Shen, and J. Liu, "Malware propagation model in wireless sensor networks under attack–defense confrontation," *Comput. Commun.*, vol. 162, pp. 51–58, Oct. 2020.

[19] R. K. Shakya, K. Rana, A. Gaurav, P. Mamoria, and P. K. Srivastava, "Stability analysis of epidemic modeling based on spatial correlation for wireless sensor networks," *Wireless Pers. Commun.*, vol. 108, no. 3, pp. 1363–1377, Oct. 2019.

[20] R. P. Ojha, G. Sanyal, P. K. Srivastava, and K. Sharma, "Design and analysis of modified SIQRS model for performance study of wireless sensor network," *Scalable Comput. Pract. Exper.*, vol. 18, no. 3, pp. 229–241, Sep. 2017.

[21] C. N. Angstmann, B. I. Henry, and A. V. McGann, "A fractional-order infectivity SIR model," *Phys. A, Stat. Mech. Appl.*, vol. 452, pp. 86–93, Jun. 2016.

[22] Q. Wu and X. Fu, "Immunization and epidemic threshold of an SIS model in complex networks," *Phys. A, Stat. Mech. Appl.*, vol. 444, pp. 576–581, Feb. 2016.

[23] S. Huang, "Global dynamics of a network-based WSIS model for mobile malware propagation over complex networks," *Phys. A, Stat. Mech. Appl.*, vol. 503, pp. 293–303, Aug. 2018.

[24] C.-H. Li, C.-C. Tsai, and S.-Y. Yang, "Analysis of epidemic spreading of an SIRS model in complex heterogeneous networks," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 4, pp. 1042–1054, Apr. 2014.

[25] L. Yang, M. Draief, and X. Yang, "Heterogeneous virus propagation in networks: A theoretical study," *Math. Methods Appl. Sci.*, vol. 40, no. 5, pp. 1396–1413, Mar. 2017.

[26] N. H. Khanh, "Dynamics of a worm propagation model with quarantine in wireless sensor networks," *Appl. Math. Inf. Sci.*, vol. 10, no. 5, pp. 1739–1746, Sep. 2016.

[27] N. Keshri and B. K. Mishra, "Two time-delay dynamic model on the transmission of malicious signals in wireless sensor network," *Chaos, Solitons Fractals*, vol. 68, pp. 151–158, Nov. 2014.

[28] S. Shen, H. Zhou, S. Feng, L. Huang, J. Liu, S. Yu, and Q. Cao, "HSIRD: A model for characterizing dynamics of malware diffusion in heterogeneous WSNs," *J. Netw. Comput. Appl.*, vol. 146, Nov. 2019, Art. no. 102420.

[29] S. Shen, H. Zhou, S. Feng, J. Liu, and Q. Cao, "SNIRD: Disclosing rules of malware spread in heterogeneous wireless sensor networks," *IEEE Access*, vol. 7, no. 1, pp. 92881–92892, Jul. 2019.

[30] N. Sharma and A. K. Gupta, "Impact of time delay on the dynamics of SEIR epidemic model using cellular automata," *Phys. A, Stat. Mech. Appl.*, vol. 471, pp. 114–125, Apr. 2017.

[31] M. López, A. Peinado, and A. Ortiz, "An extensive validation of a SIR epidemic model to study the propagation of jamming attacks against IoT wireless networks," *Comput. Netw.*, vol. 165, Dec. 2019, Art. no. 106945.

[32] T. Zhang, L.-X. Yang, X. Yang, Y. Wu, and Y. Y. Tang, "Dynamic malware containment under an epidemic model with alert," *Phys. A, Stat. Mech. Appl.*, vol. 470, pp. 249–260, Mar. 2017.
[33] D. Acarali, M. Rajarajan, N. Komninos, and B. B. Zarpelão, "Modelling the spread of botnet malware in IoT-based wireless sensor networks," *Secur. Commun. Netw.*, vol. 2019, Feb. 2019, Art. no. 3745619.
[34] L. Zhang and J. Xu, "Differential security game in heterogeneous device-to-device offloading network under epidemic risks," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 3, pp. 1852–1861, Jul. 2020.
[35] H. Xia, L. Li, X. Cheng, C. Liu, and T. Qiu, "A dynamic virus propagation model based on social attributes in city IoT," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8036–8048, Sep. 2020.
[36] J. D. H. Guillen, A. M. del Rey, and R. Casado-Vara, "Security countermeasures of a SCIRAS model for advanced malware propagation," *IEEE Access*, vol. 7, pp. 135472–135478, 2019.
[37] L. Li, J. Cui, R. Zhang, H. Xia, and X. Cheng, "Dynamics of complex networks: Malware propagation modeling and analysis in industrial Internet of Things," *IEEE Access*, vol. 8, pp. 64184–64192, 2020.
[38] G. Liu, B. Peng, and X. Zhong, "A novel epidemic model for wireless rechargeable sensor network security," *Sensors*, vol. 21, no. 1, Dec. 2020, Art. no. 123.
[39] S. Muthukrishnan, S. Muthukumar, and V. Chinnadurai, "Optimal control of malware spreading model with tracing and patching in wireless sensor networks," *Wireless Pers. Commun.*, vol. 117, no. 3, pp. 2061–2083, Apr. 2021.
[40] S. Hosseini and M. A. Azgomi, "A model for malware propagation in scale-free networks based on rumor spreading process," *Comput. Netw.*, vol. 108, pp. 97–107, Oct. 2016.
[41] B. K. Mishra and N. Keshri, "Mathematical model on the transmission of worms in wireless sensor network," *Appl. Math. Model.*, vol. 37, no. 6, pp. 4103–4111, Mar. 2013.
[42] S. Shen, H. Zhou, S. Feng, J. Liu, H. Zhang, and Q. Cao, "An epidemiology-based model for disclosing dynamics of malware propagation in heterogeneous and mobile WSNs," *IEEE Access*, vol. 8, pp. 43876–43887, 2020.
[43] R. P. Ojha, P. K. Srivastava, G. Sanyal, and N. Gupta, "Improved model for the stability analysis of wireless sensor network against malware attacks," *Wireless Pers. Commun.*, vol. 116, no. 3, pp. 2525–2548, Feb. 2021.
[44] H. Jiao and Q. Shen, "Dynamics analysis and vaccination-based sliding mode control of a more generalized SEIR epidemic model," *IEEE Access*, vol. 8, pp. 174507–174515, 2020.
[45] X. Zhang and C. Gan, "Global attractivity and optimal dynamic countermeasure of a virus propagation model in complex networks," *Phys. A, Stat. Mech. Appl.*, vol. 490, pp. 1004–1018, Jan. 2018.
[46] Y. Yao, Q. Fu, W. Yang, Y. Wang, and C. Sheng, "An epidemic model of computer worms with time delay and variable infection rate," *Secur. Commun. Netw.*, vol. 2018, pp. 1–11, Mar. 2018, Art. no. 9756982.
[47] Q. Xu, Z. Su, K. Zhang, and S. Yu, "Fast containment of infectious diseases with E-healthcare mobile social Internet of Things," *IEEE Internet Things J.*, early access, Feb. 26, 2021, doi: 10.1109/JIOT.2021.3062288.
[48] H. Zhang, S. Shen, Q. Cao, X. Wu, and S. Liu, "Modeling and analyzing malware diffusion in wireless sensor networks based on cellular automaton," *Int. J. Distrib. Sens. Netw.*, vol. 16, no. 11, pp. 1–9, Nov. 2020.
[49] S. Hosseini and M. A. Azgomi, "Dynamical analysis of a malware propagation model considering the impacts of mobile devices and software diversification," *Phys. A, Stat. Mech. Appl.*, vol. 526, Jul. 2019, Art. no. 120925.
[50] L. Zhu, H. Zhao, and X. Wang, "Stability and bifurcation analysis in a delayed reaction–diffusion malware propagation model," *Comput. Math. Appl.*, vol. 69, no. 8, pp. 852–875, Apr. 2015.
[51] S. Shen, L. Huang, J. Liu, A. Champion, S. Yu, and Q. Cao, "Reliability evaluation for clustered WSNs under malware propagation," *Sensors*, vol. 16, no. 6, Jun. 2016, Art. no. 855.
[52] S. Shen, H. Ma, E. Fan, K. Hu, S. Yu, J. Liu, and Q. Cao, "A non-cooperative non-zero-sum game-based dependability assessment of heterogeneous WSNs with malware diffusion," *J. Netw. Comput. Appl.*, vol. 91, pp. 26–35, Aug. 2017.
[53] H. Xu, D. Wang, S. Shen, Y. Shi, and Q. Cao, "An efficient approach for stimulating cooperation among nodes in wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 5, May 2016, Art. no. 2873439.
[54] M. J. Farooq and Q. Zhu, "Modeling, analysis, and mitigation of dynamic botnet formation in wireless IoT networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 9, pp. 2412–2426, Sep. 2019.
[55] A. Singh, A. K. Awasthi, K. Singh, and P. K. Srivastava, "Modeling and analysis of worm propagation in wireless sensor networks," *Wireless Pers. Commun.*, vol. 98, no. 3, pp. 2535–2551, Feb. 2018.
[56] P. van den Driessche and J. Watmough, "Reproduction numbers and subthreshold endemic equilibria for compartmental models of disease transmission," *Math. Biosci.*, vol. 180, nos. 1–2, pp. 29–48, Nov. 2002.

XIAOTONG YE received the B.S. degree in computer science and technology from Zhejiang Normal University, Jinhua, China, in 2001, and the M.S. degree in software engineering from Tongji University, Shanghai, China, in 2005.

He is currently a Lecturer with the Department of Computer Science and Engineering, Shaoxing University, Shaoxing, China. His current research interests include the Internet of Things, cyber security, cloud computing, and game theory.

SISI XIE received the B.E. degree in computer science and technology from Shaoxing University, Shaoxing, China, in 2019. Her current research interests include the Internet of Things and cyber security.

SHIGEN SHEN (Member, IEEE) received the B.S. degree in fundamental mathematics from Zhejiang Normal University, Jinhua, China, in 1995, the M.S. degree in computer science and technology from Zhejiang University, Hangzhou, China, in 2005, and the Ph.D. degree in pattern recognition and intelligent systems from Donghua University, Shanghai, China, in 2013.

He is currently a Professor with the Department of Computer Science and Engineering, Shaoxing University, Shaoxing, China. His current research interests include the Internet of Things, cyber security, cloud computing, and game theory.