IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 15, 2019, accepted July 1, 2019, date of publication July 8, 2019, date of current version July 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2927220

SNIRD: Disclosing Rules of Malware Spread in Heterogeneous Wireless Sensor Networks

SHIGEN SHEN[1], HAIPING ZHOU[1], SHENG FENG[1], JIANHUA LIU[1], (Member, IEEE), AND QIYING CAO[2]

[1]Department of Computer Science and Engineering, Shaoxing University, Shaoxing 312000, China
[2]College of Computer Science and Technology, Donghua University, Shanghai 201620, China

Corresponding authors: Shigen Shen (shigens@126.com) and Jianhua Liu (ljh_541@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61772018 and Grant 61572014, and in part by the Public Welfare Technology Research Project of Zhejiang Province under Grant LGG19F020007.

ABSTRACT Heterogeneous wireless sensor networks (WSNs) are widely deployed, owing to their good capabilities in terms of network stability, dependability, and survivability. However, they are prone to the spread of malware because of the limited computational capabilities of sensor nodes. To suppress the spread of malware, a malware spread model is urgently required to discover the rules of malware spread. In this paper, a heterogeneous susceptible-iNsidious-infectious-recovered-dysfunctional (SNIRD) model was proposed, which not only considers the communication connectivity of heterogeneous sensor nodes but also reflects the characteristics of malware hiding and dysfunctional sensor nodes. Then, the fraction evolution equations of heterogeneous sensor nodes in different states in discrete time were obtained. Furthermore, the existence of equilibria for the heterogeneous SNIRD model was proved, and the malware spread threshold was obtained, which indicates whether malware will spread or fade out. Finally, the heterogeneous SNIRD model was simulated and it was contrasted with the conventional SIS and SIR models to validate its effectiveness. The results construct a theoretical guideline for administrators to suppress the spread of malware in heterogeneous WSNs.

INDEX TERMS Heterogeneous wireless sensor networks, malware, epidemic theory, heterogeneity, equilibria, malware spread threshold.

I. INTRODUCTION

Currently, heterogeneous wireless sensor networks (WSNs) have become the most universal method to network sensor nodes and smart devices to construct smart Internet of Things [1], [2]. In contrast to homogeneous WSNs, where all the sensor nodes involved have the same capabilities including power, communication, and computation, heterogeneous WSNs allow for all types of sensor nodes with energy, link, and computational heterogeneities. Therefore, heterogeneous WSNs are more scalable and have better capabilities in terms of network stability, dependability, and survivability. They have been widely employed in areas such as smart cities, medical treatment, agriculture, factories, and so on [3]–[6].

Malware (short for malicious software) refers to any software intentionally designed by attackers to inflict damage on computer systems [7]–[15]. Malware is prone to spread in heterogeneous WSNs [16]–[20], because the sensor nodes have limited computational capabilities and high-strength security measures cannot be efficiently deployed. Once malware has broadly spread, it can interfere with the regular sensing processes, eavesdrop on data sensed by the nodes, and even destroy sensor nodes [21], [22]. These malicious behaviors do great damage to the service availability and data confidentiality of heterogeneous WSNs. To solve the problems associated with the spread of malware, the most important issue is to set up a malware spread model and thus disclose the rules of malware spread to suppress the malware infection.

Epidemic models are usually borrowed to formulate the spread of malware [23]–[25], owing to the fact that malware spread has similarities, especially with the spread processes of epidemic diseases. Conventional epidemic models include the SI, SIR, and SIS models, which are based on node state classification. The SI and SIS models classify all nodes into

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

two states *Susceptible* (S) and *Infectious* (I), whereas the SIR model has three states S, I and *Recovered* (R).

According to the behaviors of the heterogeneous sensor nodes, a heterogeneous epidemic model called the SNIRD model was put forward, which includes the states S, N (*iNsidious*), I, R, and D (*Dysfunctional*), by extending the conventional SIR model. The state N was introduced for cases where the malware may have hidden itself to avoid being detected by the sensor IDS (intrusion detection system). Moreover, a heterogeneous sensor node in state N is infected by malware but it doesn't infect other neighbor nodes, which is motivated by the exposed state of the SEIR model. On the other hand, the state D was supplemented for the motivation that a heterogeneous sensor node may become dysfunctional due to malware destruction, power exhaustion, or physical damage. Obviously, a heterogeneous sensor node in state D cannot infect others even if the node has been infectious. Further, the heterogeneity of heterogeneous sensor nodes was distinguished by their communication connectivity, which universally exists in heterogeneous WSNs and denotes the number of connections a heterogeneous sensor node has to other nodes. Next, the heterogeneous SNIRD model in discrete time was constituted, integrating the communication connectivity of the heterogeneous sensor nodes. Further, the equilibria of the heterogeneous SNIRD model was obtained and the malware spread threshold was computed as an indicator to guide administrators in taking security measures.

The contributions of this paper are summarized as follows.

First, a heterogeneous SNIRD model for heterogeneous WSNs was proposed. To our knowledge, this model is the first work to not only consider the communication connectivity of heterogeneous sensor nodes as a characteristic of their heterogeneity but also introduce the states N and D to reflect the characteristics of malware hiding and dysfunctional sensor nodes.

Second, the conversion quantity of all states of the heterogeneous SNIRD model was analyzed, and then fraction evolution equations for heterogeneous sensor nodes in different states were obtained as time evolves in a discrete manner. These equations can disclose the changeable quantities of all the heterogeneous sensor nodes in a heterogeneous WSN under the spread of malware.

Finally, the existence of the equilibria of the heterogeneous SNIRD model was proved. Further, the malware spread threshold was obtained by computing the basic reproduction number, which can indicate whether the malware will spread or fade out. Thus, a theoretical guideline for administrators was constructed to suppress the spread of malware in heterogeneous WSNs.

The rest of the paper was arranged as follows. Related work was surveyed in Section II, and the unsolved problems of current epidemic models for heterogeneous WSNs were addressed. In Section III, the state transitions of heterogeneous sensor nodes were analyzed. In Section IV, the heterogeneous SNIRD model was presented. Then, the existence of equilibria for the proposed model was proved in Section V, and the malware spread threshold was obtained. In Section VI, the heterogeneous SNIRD model was validated and the proposed model was compared with the conventional SIS and SIR models. Finally, the paper was summarized.

Notations used in this paper are listed in Table 1 for easy examination.

TABLE 1. Notations.

Notation	Description
K	Number of assemblages, each of which has the same communication connectivity.
S_k^t	Fraction of nodes in state S having the same communication connectivity (belonging to assemblage) k at time t.
N_k^t	Fraction of nodes in state N having the same communication connectivity (belonging to assemblage) k at time t.
I_k^t	Fraction of nodes in state I having the same communication connectivity (belonging to assemblage) k at time t.
R_k^t	Fraction of nodes in state R having the same communication connectivity (belonging to assemblage) k at time t.
D_k^t	Fraction of nodes in state D having the same communication connectivity (belonging to assemblage) k at time t.
φ	Initial fraction of nodes in state I belonging to assemblage k.
ω_k^t	Probability that a heterogeneous sensor node in state S belonging to assemblage k communicates with one of the infectious nodes.
$< m >$	Average communication connectivity of the heterogeneous WSN.
α_k	Probability of a heterogeneous sensor node having communication connectivity k.
δ_k	Infectious capability of a heterogeneous sensor node having communication connectivity k.
q_{ij}^k	Probability of heterogeneous sensor nodes in assemblage k converting from state i to j.
η	Fraction of added/discarded nodes.
Δ_1	Malware-free equilibrium meaning malware extermination.
Δ_2	Endemic equilibrium meaning malware spread.
γ	Basic reproduction number equaling the mean quantity of infectious sensor nodes added by the primary sensor nodes in state I.
$\rho(\cdot)$	Spectral radius of the next-generation matrix.
$\mathbf{A}$	Advent rate matrix of fresh heterogeneous sensor nodes in state I at equilibrium Δ_1.
$\mathbf{B}$	Transition rate matrix of a heterogeneous sensor node in state I at equilibrium Δ_1.
$\mathbb{G}(t)$	Heterogeneous WSN simulated at time t.

II. RELATED WORK

To date, there are some malware spread models for WSNs which are developed by extending the conventional epidemic models. An SEIRS-V model proposed in [26] adds states E (Exposed) and V (Vaccination), based on the SIR model, to disclose the dynamics of malware spread in WSNs. The SEIR model presented in [27] reflects latency and immunity delays. A geographical SI model, given in [28], considers the spatial and geometrical features of the sensor nodes. The SITR model in [29] adds the state T (Terminally Infected)

to the SIR model to characterize the sleeping mode of sensor nodes. An SIS-based passive dynamical system in [30] develops adaptive strategies, which can restrain the spread of multiple malware threats. With regard to malware spread in mobile WSNs, there are reaction diffusion equations [31], pulse differential equations [32], and delay reaction diffusion equations [33], all based on the SIR model. The SEIRV model in [34] and the improved SIRS model in [35] both reflect the deployed density and the communication radius of sensor nodes. A discrete-time absorbing Markov process used in the SIS model of [36] characterizes the spread of malware across nontrivial topologies of large networks. In addition, typical epidemic models for WSN malware spread include a stochastic SIS model [37], an SEIR model considering time delay [38], a developed SEIRS model with a changeable infection rate [39], and an SEIR model with a variable contact rate [40].

Some researchers have focused on the spread of malware in heterogeneous WSNs. Qu and Wang [41] considered the infection rate heterogeneity among nodes and employed the SIS model to analyze the influence with log-normal, gamma and newly designed distribution functions on the fraction of infected nodes, respectively. Nowzari *et al.* [42] proposed an epidemic model called the susceptible-exposed-infected-vigilant model, which analyzes the spread of malware over universal directed graphs with heterogeneous nodes. Eshghi *et al.* [43] presented a general epidemic framework, which can be employed in any node cluster with universal contact rates between any two nodes. Yang *et al.* [44] proposed a heterogeneous SIRS model, which considers the network topology heterogeneity.

However, there are still some problems with malware spread models for heterogeneous WSNs that need to be solved. One problem is how to simultaneously reflect three practical circumstances: the heterogeneity of sensor nodes, malware hiding and dysfunctional sensor nodes. The other problem is how to indicate whether malware will spread or fade out after solving the first problem. Herein, the first problem was addressed by adding states N and D to the traditional SIR model and employing a communication connectivity measure to reflect the sensor node heterogeneity. Then, the second problem was addressed by exploring the equilibria of the heterogeneous model and obtaining the malware spread threshold.

III. STATE TRANSITIONS OF A HETEROGENEOUS SENSOR NODE

In the heterogeneous SNIRD model, a heterogeneous sensor node in state S indicates that it has system bugs and is susceptible to infection by malware. N indicates that the heterogeneous sensor node has been infected and is controlled by malware, and that the resident malware is insidious to attack other heterogeneous sensor nodes. I indicates that the heterogeneous sensor node has been infected and controlled by malware, and that the resident malware can infect other heterogeneous sensor nodes by communicating with them.

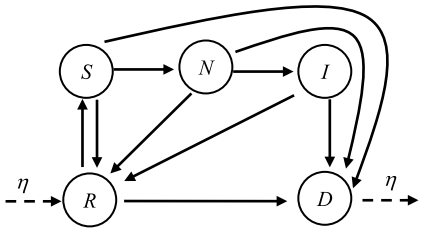

FIGURE 1. State conversion flow of a heterogeneous sensor node.

R indicates that the infected node has had the resident malware removed through the sensor IDS launched by administrators, and it is vaccinated against the given malware. D indicates that the heterogeneous sensor node is dysfunctional, because it may be physically damaged or intentionally destroyed by the resident malware. Note that malware resided in a heterogeneous sensor node of state N will not infect other heterogeneous sensor nodes, whereas the resident malware in a heterogeneous sensor node of state I can infect other heterogeneous sensor nodes.

Figure 1 illustrates the state conversion flow of a heterogeneous sensor node. In fact, these state conversions are implemented by the actions of the sensor IDS and the malware, which are controlled by administrators and adversaries, respectively. For a heterogeneous sensor node, it initially is in state R. Its state converts from state R to S, once malware scans the heterogeneous sensor node and finds its security vulnerabilities, and thus malware can inject itself into the heterogeneous sensor node. Then, its state converts from state S to N, once the malware continually attacks and successfully resides in the heterogeneous sensor node. The node state may be in state N over a long period of time, because the malware can be more easily detected by the sensor IDS if the malware is frequently launching attacks. Further, its state converts from state N to I, once the resident malware infects other heterogeneous sensor nodes. In general, administrators employ the sensor IDS to detect and remove the resident malware and patch the security programs of the susceptible nodes to immunize them from the given malware. These actions convert states S, N, and I to R. In addition, any heterogeneous sensor node may have software and hardware failures, energy exhaustion, or destruction incurred by malware. These cases convert states S, N, I, and R to D. These dysfunctional nodes are generally replaced by new nodes, because most heterogeneous sensor nodes cannot be repaired. The replacement makes these dysfunctional nodes convert from state D to R. At that time, note that the heterogeneous sensor nodes converting state D to R are no longer dysfunctional nodes and dashed arrows are employed in Fig. 1 to denote this conversion. More specifically, the incoming dashed arrow in Fig. 1 means that some new nodes are added to replace those dysfunctional nodes, whereas the outgoing dashed arrow means that those dysfunctional nodes are discarded.

In the heterogeneous SNIRD model, a heterogeneous sensor node initially is in state R, which is different from

conventional epidemic models where the initial state is S. This treatment is made for the following reason. Generally, a new heterogeneous sensor node is patched with the newest security programs. Therefore, the new node has the ability to defend the known malware. This characteristic is corresponding to state R. In fact, this paper is motivated by conventional epidemic models, but this paper flexibly deals with the initial state according to the characteristic of a new heterogeneous sensor node.

IV. HETEROGENEOUS SNIRD MODEL

In the proposed model, the heterogeneity of heterogeneous sensor nodes is based on their communication connectivity. As a result, all heterogeneous sensor nodes are divided into K assemblages, each of which has the same communication connectivity. Let $k \in \{1, 2, \cdots, K\}$ be the communication connectivity of assemblage k. S_k^t, N_k^t, I_k^t, R_k^t, and D_k^t are the fractions of assemblage k in states S, N, I, R, and D at time t, respectively. They obviously satisfy

$$S_k^t + N_k^t + I_k^t + R_k^t + D_k^t = 1 \tag{1}$$

at any time. As assumed in other epidemic models [43], let φ be the initial fraction of nodes in state I belonging to assemblage k, that is,

$$I_k^0 = \varphi, \quad 0 < \varphi < 1. \tag{2}$$

The initial fractions of nodes in states N, R, and D belonging to assemblage k are 0. That is,

$$N_k^0 = R_k^0 = D_k^0 = 0. \tag{3}$$

Thus, the initial fraction of nodes in state S belonging to assemblage k is achieved by

$$S_k^0 = 1 - \varphi. \tag{4}$$

At time t, the probability, ω_k^t, that a heterogeneous sensor node in state S belonging to assemblage k communicates with one of the infectious nodes is

$$\omega_k^t = \frac{1}{< m >} \sum_{k=1}^{K} \alpha_k \delta_k I_k^t, \tag{5}$$

where $< m >$ is the average communication connectivity of the heterogeneous WSN, and α_k and δ_k are the probability and the infectious capability of a heterogeneous sensor node having communication connectivity k, respectively. Inherently, these parameters are characterized by

$$\sum_{k=1}^{K} \alpha_k = 1 \tag{6}$$

and

$$< m >= \sum_{k=1}^{K} k\alpha_k. \tag{7}$$

As for the δ_k that can be applied to heterogeneous WSNs, researchers have presented typical formulas such as 1) $\delta_k = k$ [45]; 2) $\delta_k = C$ [46], where C is a constant; and 3) $\delta_k = \vartheta k^{\varsigma}/(1 + \xi k^{\varsigma})$ [47], with three parameters: ϑ, ς, and ξ.

Next, the conversion quantity of all the states is analyzed. Let q_{ij}^k be the probability of heterogeneous sensor nodes in assemblage k converting from $i \in \{S, N, I, R, D\}$ to $j \in \{S, N, I, R, D\}$. For heterogeneous sensor nodes with communication connectivity k in state S at time t, the quantity increment of converting from state R is the probability q_{RS}^k times the fraction R_k^t at time $t-1$, i.e., $q_{RS}^k R_k^{t-1}$. The quantity decrements of converting into states N, R, and D are the probability q_{SN}^k times the probability ω_k^t at time $t-1$ times the fraction S_k^t at time $t-1$, the probability q_{SR}^k times the fraction S_k^t at time $t-1$, and the probability q_{SD}^k times the fraction S_k^t at time $t-1$, i.e., $q_{SN}^k \omega_k^{t-1} S_k^{t-1}$, $q_{SR}^k S_k^{t-1}$, and $q_{SD}^k S_k^{t-1}$, respectively. Thus, when time evolves from $t-1$ to t, the fraction S_k^t is

$$S_k^t = S_k^{t-1} + q_{RS}^k R_k^{t-1} - q_{SN}^k \omega_k^{t-1} S_k^{t-1} - q_{SR}^k S_k^{t-1} - q_{SD}^k S_k^{t-1}. \tag{8}$$

After a similar analysis on the heterogeneous sensor nodes with communication connectivity k in other states, other fractions are obtained by

$$N_k^t = N_k^{t-1} + q_{SN}^k \omega_k^{t-1} S_k^{t-1} - q_{NR}^k N_k^{t-1} - q_{NI}^k N_k^{t-1} - q_{ND}^k N_k^{t-1}, \tag{9}$$

$$I_k^t = I_k^{t-1} + q_{NI}^k N_k^{t-1} - q_{IR}^k I_k^{t-1} - q_{ID}^k I_k^{t-1}, \tag{10}$$

$$R_k^t = R_k^{t-1} + \eta + q_{SR}^k S_k^{t-1} + q_{NR}^k N_k^{t-1} + q_{IR}^k I_k^{t-1} - q_{RS}^k R_k^{t-1} - q_{RD}^k R_k^{t-1}, \tag{11}$$

and

$$D_k^t = D_k^{t-1} + q_{SD}^k S_k^{t-1} + q_{ND}^k N_k^{t-1} + q_{ID}^k I_k^{t-1} + q_{RD}^k R_k^{t-1} - \eta. \tag{12}$$

Thus far, (8)–(12) constitute the heterogeneous SNIRD model in discrete time. Note that the fraction η is added to the fraction R_k^t in (11) and is conversely subtracted from the fraction D_k^t in (12), because some new heterogeneous sensor nodes have replaced those irreparably dysfunctional nodes so that the heterogeneous WSN can work normally.

V. ANALYSES OF THE HETEROGENEOUS SNIRD MODEL

A. EQUILIBRIUM

As an epidemic model, the equilibrium of the heterogeneous SNIRD model is required to obtain the malware spread threshold which will determine whether the malware in the heterogeneous WSN will spread or dissipate. Mathematically, the equilibrium of the heterogeneous SNIRD model is denoted by the value $(S_k^{\#}, N_k^{\#}, I_k^{\#}, R_k^{\#}, D_k^{\#})$ of $(S_k^t, N_k^t, I_k^t, R_k^t, D_k^t)$ at a given time $t^{\#}$, satisfying

$$\forall t > t^{\#}, (S_k^t, N_k^t, I_k^t, R_k^t, D_k^t) = (S_k^{\#}, N_k^{\#}, I_k^{\#}, R_k^{\#}, D_k^{\#}). \tag{13}$$

That is, $(S_k^t, N_k^t, I_k^t, R_k^t, D_k^t)$ stays constant for all $t > t^{\#}$. In this manner, the following theorem is obtained.

Theorem 1: There exist equilibria for the heterogeneous SNIRD model expressed in (8)–(12).

Proof: Once the heterogeneous SNIRD model approaches its equilibrium at time $t^{\#}$, $(S_k^t, N_k^t, I_k^t, R_k^t, D_k^t)$ stays constant for all $t > t^{\#}$. Thus, all fraction increments of $S_k^t - S_k^{t-1}$, $N_k^t - N_k^{t-1}$, $I_k^t - I_k^{t-1}$, $R_k^t - R_k^{t-1}$, and $D_k^t - D_k^{t-1}$ become 0 for all $t > t^{\#}$. That is

$$\begin{cases} q_{RS}^k R_k^{t-1} - q_{SN}^k \omega_k^{t-1} S_k^{t-1} - q_{SR}^k S_k^{t-1} - q_{SD}^k S_k^{t-1} = 0 \\ q_{SN}^k \omega_k^{t-1} S_k^{t-1} - q_{NR}^k N_k^{t-1} - q_{NI}^k N_k^{t-1} - q_{ND}^k N_k^{t-1} = 0 \\ q_{NI}^k N_k^{t-1} - q_{IR}^k I_k^{t-1} - q_{ID}^k I_k^{t-1} = 0 \\ \eta + q_{SR}^k S_k^{t-1} + q_{NR}^k N_k^{t-1} + q_{IR}^k I_k^{t-1} - q_{RS}^k R_k^{t-1} - q_{RD}^k R_k^{t-1} = 0 \\ q_{SD}^k S_k^{t-1} + q_{ND}^k N_k^{t-1} + q_{ID}^k I_k^{t-1} + q_{RD}^k R_k^{t-1} - \eta = 0 \end{cases} \tag{14}$$

After solving (14), two equilibria

$$\Delta_1(S_k^{MF}, N_k^{MF}, I_k^{MF}, R_k^{MF}, D_k^{MF})$$

and

$$\Delta_2(S_k^{ME}, N_k^{ME}, I_k^{ME}, R_k^{ME}, D_k^{ME})$$

are obtained, which means that $(S_k^t, N_k^t, I_k^t, R_k^t, D_k^t)$ will finally stay Δ_1 or Δ_2. Here,

$$S_k^{MF} = \frac{\eta q_{RS}^k}{q_{RS}^k q_{SD}^k + q_{RD}^k q_{SR}^k + q_{RD}^k q_{SD}^k}, \tag{15}$$

$$N_k^{MF} = 0, \tag{16}$$

$$I_k^{MF} = 0, \tag{17}$$

$$R_k^{MF} = \frac{\eta(q_{SR}^k + q_{SD}^k)}{q_{RS}^k q_{SD}^k + q_{RD}^k q_{SR}^k + q_{RD}^k q_{SD}^k}, \tag{18}$$

$$\begin{aligned} D_k^{MF} &= 1 - S_k^{MF} - N_k^{MF} - I_k^{MF} - R_k^{MF} \\ &= 1 - \frac{\eta(q_{SR}^k + q_{SD}^k + q_{RS}^k)}{q_{RS}^k q_{SD}^k + q_{RD}^k q_{SR}^k + q_{RD}^k q_{SD}^k}, \end{aligned} \tag{19}$$

$$S_k^{ME} = \frac{\psi_k}{q_{SN}^k q_{NI}^k \sigma_k}, \tag{20}$$

$$N_k^{ME} = \frac{q_{IR}^k + q_{ID}^k}{q_{NI}^k} I_k^{ME}, \tag{21}$$

$$I_k^{ME} = \frac{\eta q_{RS}^k q_{SN}^k q_{NI}^k \sigma_k - \psi_k(q_{RS}^k q_{SD}^k + q_{RD}^k q_{SR}^k + q_{RD}^k q_{SD}^k)}{q_{SN}^k \sigma_k (q_{RS}^k q_{ND}^k (q_{IR}^k + q_{ID}^k) + q_{RS}^k q_{NI}^k q_{ID}^k + q_{RD}^k \psi_k)}, \tag{22}$$

$$R_k^{ME} = \frac{\psi_k(q_{SR}^k + q_{SD}^k + q_{SN}^k \sigma_k I_k^{ME})}{q_{RS}^k q_{SN}^k q_{NI}^k \sigma_k}, \tag{23}$$

and

$$D_k^{ME} = 1 - S_k^{ME} - N_k^{ME} - I_k^{ME} - R_k^{ME}, \tag{24}$$

where

$$\psi_k = (q_{IR}^k + q_{ID}^k)(q_{NR}^k + q_{NI}^k + q_{ND}^k), \tag{25}$$

and

$$\sigma_k = \frac{1}{< m >} \sum_{k=1}^{K} \alpha_k \delta_k. \tag{26}$$

Thus, the proof is finished. □

In Theorem 1, the equilibrium Δ_1 is referred to a malware-free equilibrium, because the fraction I_k^{MF} is 0, which means malware extermination, after the heterogeneous SNIRD model reaches the equilibrium Δ_1. On the other hand, the equilibrium Δ_2 is named the endemic equilibrium, because the fraction I_k^{ME} is better than zero, which means that the malware still spreads after the heterogeneous SNIRD model reaches the equilibrium Δ_2. Obviously, the equilibrium Δ_1 is the target that an administrator pursues for managing the heterogeneous WSN, because the malware will be exterminated after the administrators continually adopt the security actions. Contrarily, the equilibrium Δ_2 should be avoided, because malware will continue to spread and a fraction I_k^{ME} of the heterogeneous sensor nodes will be infected and disrupt the normal operation of the heterogeneous WSN.

B. MALWARE SPREAD THRESHOLD

Here, the malware spread threshold of the heterogeneous SNIRD model is explored, which is an indicator that guides administrators in taking security measures. The threshold determines whether or not the malware can spread in the heterogeneous WSN, and thus it plays an important role in analyzing the dynamics of the heterogeneous SNIRD model. Mathematically, the threshold is obtained by the basic reproduction number γ, which equals the mean quantity of infectious sensor nodes added by the primary sensor nodes in state I.

Theorem 2: There exists a malware spread threshold for the heterogeneous SNIRD model.

Proof: Based on the next-generation matrix method [48], the malware spread threshold γ equals the spectral radius of the next-generation matrix. That is, $\gamma = \rho(\mathbf{A}\mathbf{B}^{-1})$, where $\rho(\cdot)$ is the spectral radius, $\mathbf{A}$ is the advent rate matrix of fresh heterogeneous sensor nodes in state I at equilibrium $\Delta_1(S_k^{MF}, N_k^{MF}, I_k^{MF}, R_k^{MF}, D_k^{MF})$, $\mathbf{B}$ is the transition rate matrix of a heterogeneous sensor node at equilibrium $\Delta_1(S_k^{MF}, N_k^{MF}, I_k^{MF}, R_k^{MF}, D_k^{MF})$, and $\mathbf{B}^{-1}$ is the inverse of matrix $\mathbf{B}$. From this method, states N and I are included to compute the malware spread threshold. To clearly describe the process of computing $\mathbf{A}$ and $\mathbf{B}$ according to their definitions, two temporary matrices $\tilde{\mathbf{A}}$ and $\tilde{\mathbf{B}}$ are introduced, where a_{11}, a_{21}, b_{11}, and b_{21} are used in computing $\mathbf{A}$ and $\mathbf{B}$. Let

$$\tilde{\mathbf{A}} = \begin{bmatrix} a_{11} \\ a_{21} \end{bmatrix} = \begin{bmatrix} q_{SN}^k \omega_k^{t-1} S_k^{t-1} \\ 0 \end{bmatrix}, \tag{27}$$

and

$$\tilde{\mathbf{B}} = \begin{bmatrix} b_{11} \\ b_{21} \end{bmatrix} = \begin{bmatrix} (q_{NR}^k + q_{NI}^k + q_{ND}^k) N_k^{t-1} \\ -q_{NI}^k N_k^{t-1} + (q_{IR}^k + q_{ID}^k) I_k^{t-1} \end{bmatrix}, \tag{28}$$

satisfying

$$\tilde{\mathbf{A}} - \tilde{\mathbf{B}} = \begin{bmatrix} N_k^t - N_k^{t-1} \\ I_k^t - I_k^{t-1} \end{bmatrix}. \tag{29}$$

Thus, the advent rate matrix is

$$\mathbf{A} = \begin{bmatrix} \frac{\partial a_{11}}{\partial N_k^{t-1}} & \frac{\partial a_{11}}{\partial I_k^{t-1}} \\ \frac{\partial a_{21}}{\partial N_k^{t-1}} & \frac{\partial a_{21}}{\partial I_k^{t-1}} \end{bmatrix}_{\Delta_1} = \begin{bmatrix} 0 & q_{SN}^k \sigma_k S_k^{MF} \\ 0 & 0 \end{bmatrix}, \quad (30)$$

and the transition rate matrix is

$$\mathbf{B} = \begin{bmatrix} \frac{\partial b_{11}}{\partial N_k^{t-1}} & \frac{\partial b_{11}}{\partial I_k^{t-1}} \\ \frac{\partial b_{21}}{\partial N_k^{t-1}} & \frac{\partial b_{21}}{\partial I_k^{t-1}} \end{bmatrix}_{\Delta_1} = \begin{bmatrix} q_{NR}^k + q_{NI}^k + q_{ND}^k & 0 \\ -q_{NI}^k & q_{IR}^k + q_{ID}^k \end{bmatrix}. \quad (31)$$

Further, the malware spread threshold γ is obtained as

$$\gamma = \rho(\mathbf{A}\mathbf{B}^{-1}) = \frac{q_{NI}^k q_{SN}^k \sigma_k S_k^{MF}}{(q_{NR}^k + q_{NI}^k + q_{ND}^k)(q_{IR}^k + q_{ID}^k)}. \quad (32)$$

Thus, the proof is finished. □

The malware spread threshold obtained from Theorem 2 has a practical meaning in terms of guidelines. If the threshold is less than one, which means that each heterogeneous sensor node in state I will infect less than one fresh node among all the heterogeneous sensor nodes in state S, then $\Delta_1(S_k^{MF}, N_k^{MF}, I_k^{MF}, R_k^{MF}, D_k^{MF})$ will be stable. That is, malware will fade from the heterogeneous WSN. On the other hand, if the threshold is better than one, which means that each heterogeneous sensor node in state I will infect more than one fresh susceptible node, then $\Delta_2(S_k^{ME}, N_k^{ME}, I_k^{ME}, R_k^{ME}, D_k^{ME})$ will be stable. That is, the spread of malware will persist at the level value I_k^{ME}. In conclusion, administrators should try to control the parameters in (32) and ensure that the threshold is less than one, in order to suppress the spread of malware in the heterogeneous WSN.

VI. SIMULATION OF THE HETEROGENEOUS SNIRD MODEL

In this section, the heterogeneous SNIRD model is simulated with MATLAB R2018a. Further, the model is validated when the malware spread threshold γ is less than one and better than one, respectively. The proposed model is also contrasted with the conventional SIS and SIR models.

A. SIMULATION PARAMETERS AND ALGORITHM

During the simulation, the heterogeneous WSN contain 1,500 heterogeneous sensor nodes. The interval time of the heterogeneous WSN evolving from the current stage to the next one is 1 d. The topology of the heterogeneous WSN and the related parameter values which are deployed are described in [49], as scale-free networks and heterogeneous WSNs [50], [51] have similar characteristics. Here, the minimum communication connectivity, the maximum communication connectivity, and the average communication connectivity $< m >$ are set at 2, 20 (i.e., $K = 20$), and 4, respectively. Moreover, the probability q_{SN}^k indicating the malware spread probability, which is closely related to the communication connectivity of a heterogeneous sensor node, is set as $q_{SN}^k = \beta k$, where $\beta = 0.01$.

Let

$$\mathbb{G}(t) = [(s_1^t, d_1), (s_2^t, d_2), \cdots, (s_{1500}^t, d_{1500})] \quad (33)$$

be the heterogeneous WSN simulated at time t. Here, s_i^t stores the state of the i-th heterogeneous sensor node at time t; d_i stores the communication connectivity of the i-th heterogeneous sensor node, which is randomly set to an integer between 2 and 20, referring to [49], and satisfies the condition that the average value of all the d_i values is 4.

Next, the simulation algorithm is described in detail. First, the heterogeneous WSN simulated is initialized based on the given parameter values. After the artificial malware randomly infects heterogeneous sensor nodes, the numbers of heterogeneous sensor nodes having communication connection $k \in \{1, 2, \ldots, K\}$ in states S, N, I, R, and D are counted and stored. Correspondingly, their fractions can be computed. Then, the artificial malware randomly communicates with other nodes and the administrator randomly distributes security patches. According to the heterogeneous SNIRD model proposed in Section IV, all fractions of nodes belonging to different states are computed and stored at every discrete time. Eventually, if all differences of different fractions between two adjacent discrete time are less than a small enough value, then the heterogeneous WSN simulated reaches stable and the final fractions of nodes belonging to different states can be obtained.

B. VALIDATION FOR THE HETEROGENEOUS SNIRD MODEL WHEN $\gamma < 1$

In this instance, the infectious capability δ_k is set as $\delta_k = \vartheta k^{\varsigma}/(1 + \xi k^{\varsigma})$ [47], where $\vartheta = 5$, $\varsigma = 0.5$, and $\xi = 1$. Therefore, the average value of $q_{SN}^k \sigma_k$ is ∼0.1383. Considering the characteristics of heterogeneous WSNs, the probabilities are set as shown in Table 2. Under these circumstances, the malware spread threshold is less than one from (32).

Figs. 2–6 present the changeable fractions of heterogeneous sensor nodes in states S, N, I, R, and D, respectively, when $\gamma < 1$. From Fig. 2, the fractions of heterogeneous sensor nodes in state S remain at ∼90%, ∼80%, ∼70%, ∼60%, and ∼50%, in the first ∼12 d, as the initial fraction, φ, of the heterogeneous sensor nodes in state I evolves from 0.1 to 0.5 with a step size of 0.1. These fractions then gradually decrease to ∼48.69%, which is nearly equal to S_k^{MF} from (15) after ∼90 d. Fig. 3 shows that the fractions of insidious nodes all remain at 0 in the first ∼12 d when φ evolves. These fractions then gradually increase to their maximum values, ∼1.63%, ∼2.84%, ∼3.67%, ∼4.14%, and ∼4.3% for $\varphi = 0.1$, $\varphi = 0.2$, $\varphi = 0.3$, $\varphi = 0.4$, and $\varphi = 0.5$, respectively. Eventually, all of these fractions converge to 0, which is equal to N_k^{MF} from (16). Fig. 4 shows that the fractions of infectious nodes remain ∼10%, ∼20%, ∼30%, ∼40%, and ∼50% in the first ∼12 d for $\varphi = 0.1$, $\varphi = 0.2$, $\varphi = 0.3$, $\varphi = 0.4$, and $\varphi = 0.5$, respectively. All of them gradually decrease to 0, which

Algorithm 1: Simulation Algorithm to Validate the Heterogeneous SNIRD Model

$t \leftarrow 0$;
Initialize $G(t) = [(s_1^t, d_1), (s_2^t, d_2), \cdots, (s_{1500}^t, d_{1500})]$;
The artificial malware randomly infects $\varphi \times 1500$ heterogeneous sensor nodes;
Count the numbers of heterogeneous sensor nodes having communication connection $k \in \{1, 2, \ldots, K\}$ in states S, N, I, R, and D, and store them into S_k^t, N_k^t, I_k^t, R_k^t, and D_k^t, respectively;
$\tilde{S}_k(t) \leftarrow S_k^t/1500$;
$\tilde{N}_k(t) \leftarrow N_k^t/1500$;
$\tilde{I}_k(t) \leftarrow I_k^t/1500$;
$\tilde{R}_k(t) \leftarrow R_k^t/1500$;
$\tilde{D}_k(t) \leftarrow D_k^t/1500$;
do while T
The heterogeneous sensor nodes in state I randomly communicate with other nodes;
Convert the state of a heterogeneous sensor node in state S into N with the probability $q_{SN}^k \omega_k^{t-1}$ if the heterogeneous sensor node received a packet from an infectious node;
Convert the state of a heterogeneous sensor node in state N into I with the transition probability q_{NI}^k;
The administrator randomly distributes security patches;
Convert the state of heterogeneous sensor nodes in states S, N, and I into R with the probabilities q_{SR}^k, q_{NR}^k, and q_{IR}^k, respectively;
Convert the state of a heterogeneous sensor node in state R into S with the probability q_{RS}^k to simulate the actual scenario in which the malware produces new varieties;
Convert the state of heterogeneous sensor nodes in states S, N, I, and R into D with the probabilities q_{SD}^k, q_{ND}^k, q_{ID}^k, and q_{RD}^k, respectively;
Convert $\eta \times 1500$ heterogeneous sensor nodes in state D into R to simulate the actual scenario in which dysfunctional nodes are replaced by new nodes;
Count the numbers of heterogeneous sensor nodes having communication connection $k \in \{1, 2, \ldots, K\}$ in states S, N, I, R, and D, and store them into S_k^{t+1}, N_k^{t+1}, I_k^{t+1}, R_k^{t+1}, and D_k^{t+1}, respectively;
$\tilde{S}_k(t+1) \leftarrow S_k^{t+1}/1500$;
$\tilde{N}_k(t+1) \leftarrow N_k^{t+1}/1500$;
$\tilde{I}_k(t+1) \leftarrow I_k^{t+1}/1500$;
$\tilde{R}_k(t+1) \leftarrow R_k^{t+1}/1500$;
$\tilde{D}_k(t+1) \leftarrow D_k^{t+1}/1500$;
if $|\tilde{S}_k(t+1) - \tilde{S}_k(t)| < \tau$ **and** $|\tilde{N}_k(t+1) - \tilde{N}_k(t)| < \tau$ **and** $|\tilde{I}_k(t+1) - \tilde{I}_k(t)| < \tau$ **and** $|\tilde{R}_k(t+1) - \tilde{R}_k(t)| < \tau$ **and** $|\tilde{D}_k(t+1) - \tilde{D}_k(t)| < \tau$ //τ is a small enough value
  exit do;
endif
$t \leftarrow t + 1$;
enddo
return $G(t)$ and the arrays $\tilde{S}_k$, $\tilde{N}_k$, $\tilde{I}_k$, $\tilde{R}_k$, and $\tilde{D}_k$;

TABLE 2. Experimental parameters.

Parameter	Description	Value
η	Fraction of added/discarded nodes	0.01
q_{RS}^k	Probability of nodes in assemblage k converting from state R to S	0.25
q_{SN}^k	Probability of nodes in assemblage k converting from state S to N	0.4
q_{NI}^k	Probability of nodes in assemblage k converting from state N to I	0.2
q_{SD}^k	Probability of nodes in assemblage k converting from state S to D	0.0125
q_{IR}^k	Probability of nodes in assemblage k converting from state I to R	0.1
q_{SR}^k	Probability of nodes in assemblage k converting from state S to R	0.15
q_{ID}^k	Probability of nodes in assemblage k converting from state I to D	0.05
q_{NR}^k	Probability of nodes in assemblage k converting from state N to R	0.1
q_{RD}^k	Probability of nodes in assemblage k converting from state R to D	0.0125
q_{ND}^k	Probability of nodes in assemblage k converting from state N to D	0.0125

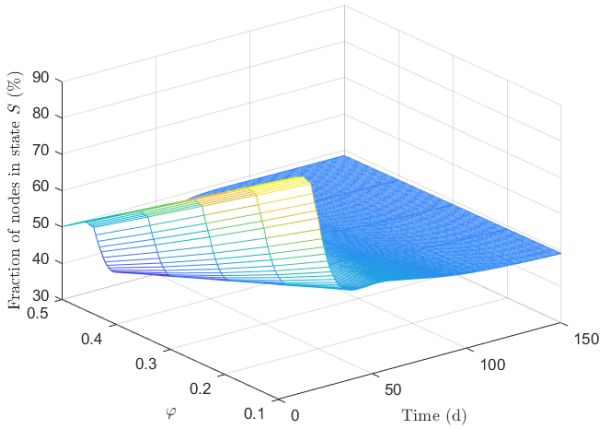

FIGURE 2. Fraction of heterogeneous sensor nodes in state S in terms of φ and time when $\gamma < 1$.

is equal to I_k^{MF} from (17). Fig. 5 shows that the fractions of the recovered nodes all remain at 0 in the first ∼12 d, then gradually increase and eventually stabilize at ∼31.63%, which is nearly equal to R_k^{MF} from (18). Fig. 6 shows that the fraction trends of the dysfunctional nodes are similar to those of recovered nodes. However, these fractions shown in Fig. 6 eventually stabilize at ∼19.68%, which is nearly equal to D_k^{MF} from (19).

Based on the above analyses, fractions of heterogeneous sensor nodes in states S, N, I, R, and D closely converge to S_k^{MF}, N_k^{MF}, I_k^{MF}, R_k^{MF}, and D_k^{MF}, respectively, regardless of the different fractions of initial infectious nodes. Experimental results have validated that the heterogeneous SNIRD model has a stable point $\Delta_1(S_k^{MF}, N_k^{MF}, I_k^{MF}, R_k^{MF}, D_k^{MF})$ if the malware spread threshold is less than one. Particularly,

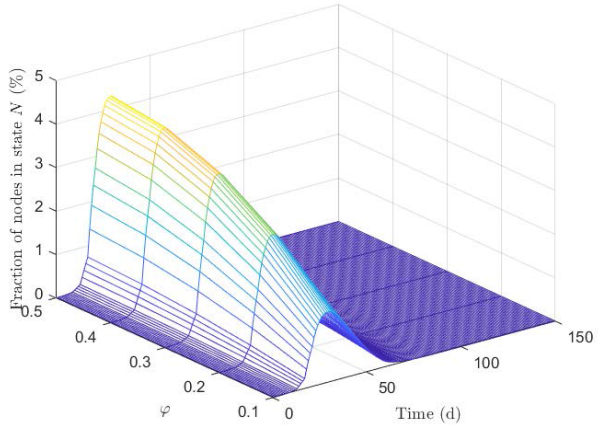

FIGURE 3. Fraction of heterogeneous sensor nodes in state *N* in terms of φ and time when $\gamma < 1$.

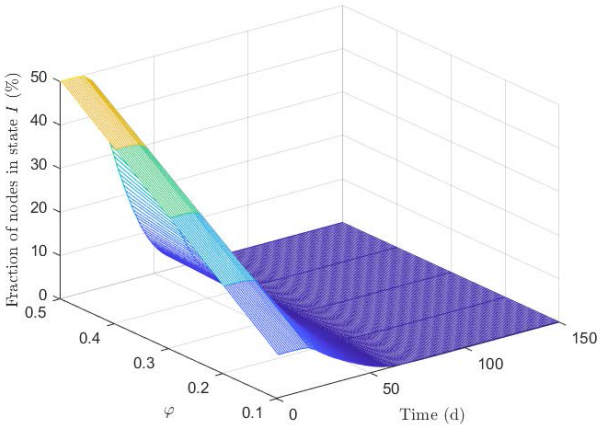

FIGURE 4. Fraction of heterogeneous sensor nodes in state *I* in terms of φ and time when $\gamma < 1$.

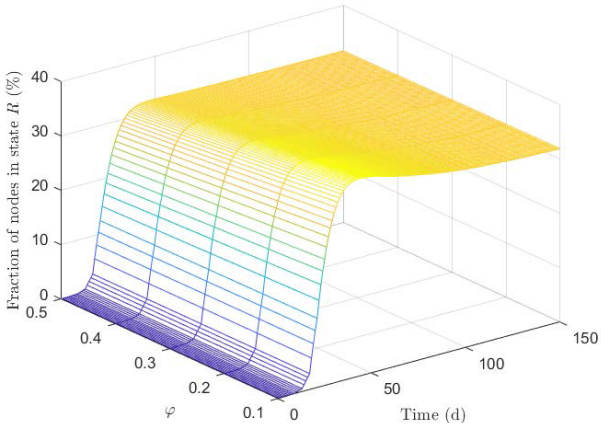

FIGURE 5. Fraction of heterogeneous sensor nodes in state *R* in terms of φ and time when $\gamma < 1$.

the experiments reflect that the fraction of infectious nodes finally converges to 0, meaning that the malware in the heterogeneous WSN will dissipate via the current security strategies adopted by the network administrators. Therefore, administrators should try to control parameters in (32) and ensure

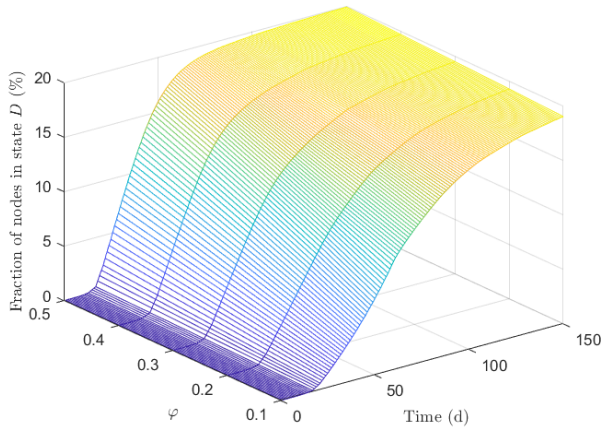

FIGURE 6. Fraction of heterogeneous sensor nodes in state *D* in terms of φ and time when $\gamma < 1$.

that the malware spread threshold is less than one in order to suppress the malware spread in heterogeneous WSNs.

C. VALIDATION FOR THE HETEROGENEOUS SNIRD MODEL WHEN $\gamma > 1$

In this instance, the heterogeneous WSN parameters are set as those presented in Section VI.B, except for $\vartheta = 10$ [49]. Therefore, the average value of $q_{SN}^k \sigma_k$ is ∼0.2766. Considering the characteristics of heterogeneous WSNs, the other parameters are set differently from those presented in Section VI.B: $q_{RS}^k = 0.1$, $q_{NI}^k = 0.5$, and $q_{IR}^k = 0.05$. Thus, the malware spread threshold $\gamma \approx 1.6740 > 1$ from (32).

Figs. 7–11 respectively illustrate the changeable fractions of heterogeneous sensor nodes in states S, N, I, R, and D when $\gamma > 1$. From these figures, the final fractions of heterogeneous sensor nodes in states S, N, I, R, and D when $\gamma > 1$ are ∼40.11%, ∼1.11%, ∼5.63%, ∼13.71%, ∼39.45%, respectively, which are nearly equal to S_k^{ME}, N_k^{ME}, I_k^{ME}, R_k^{ME} and D_k^{ME} from (20), (21), (22), (23), and (24), respectively. Thus, the heterogeneous SNIRD model with the stable point $\Delta_2(S_k^{ME}, N_k^{ME}, I_k^{ME}, R_k^{ME}, D_k^{ME})$, if the malware spread threshold is better than one, is validated. Note that the fraction of infectious nodes is not equal to 0, meaning that the malware will spread in heterogeneous WSNs. Further, the spread of malware makes more nodes become dysfunctional; therefore, the fraction of dysfunctional nodes is notably greater than that in the case $\gamma < 1$. Obviously, a practical guideline is that administrators should try to control parameters in (32) by adopting security strategies and ensure that the malware spread threshold is not better than one, so that the heterogeneous WSN can work normally.

D. COMPARISON WITH CONVENTIONAL MODELS

In this section, the effectiveness of the heterogeneous SNIRD model is validated by comparing with the conventional SIS and SIR models. The same two cases are still considered as those in Sections VI.B and VI.C. All models are implemented with the same parameters in the same case. The changeable

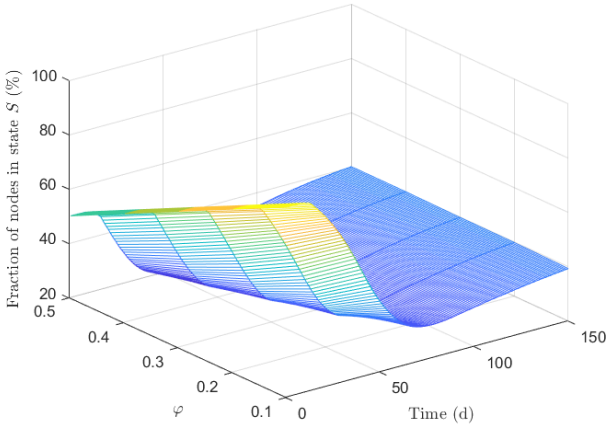

FIGURE 7. Fraction of heterogeneous sensor nodes in state *S* in terms of φ and time when $\gamma > 1$.

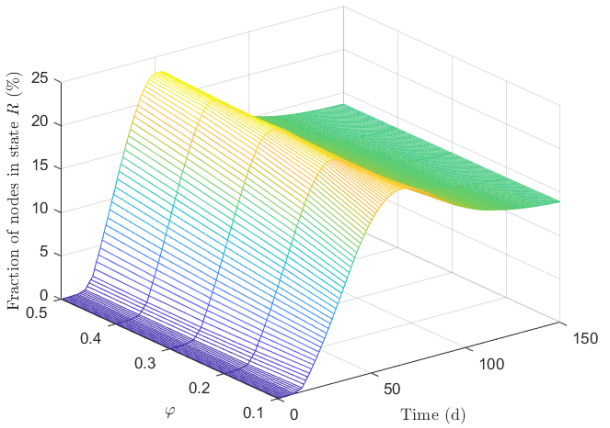

FIGURE 10. Fraction of heterogeneous sensor nodes in state *R* in terms of φ and time when $\gamma > 1$.

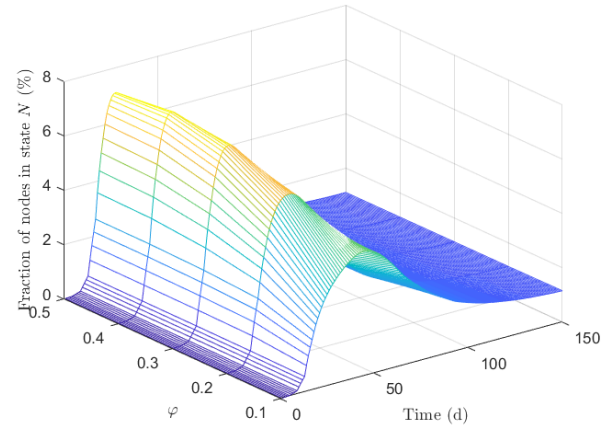

FIGURE 8. Fraction of heterogeneous sensor nodes in state *N* in terms of φ and time when $\gamma > 1$.

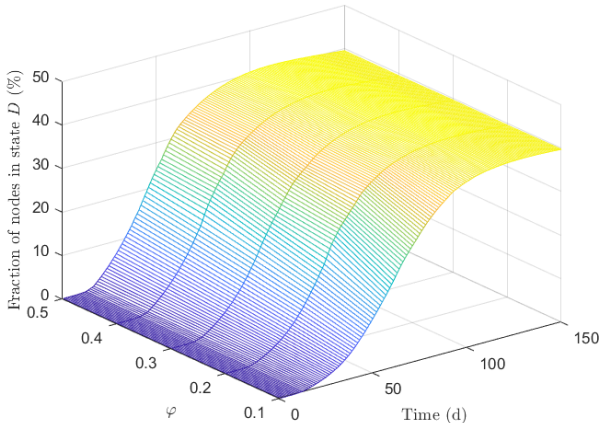

FIGURE 11. Fraction of heterogeneous sensor nodes in state *D* in terms of φ and time when $\gamma > 1$.

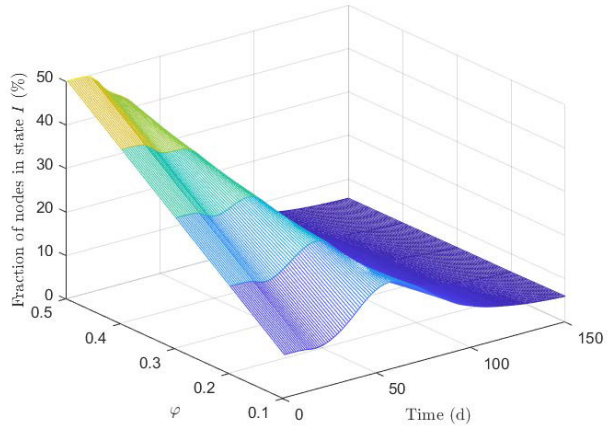

FIGURE 9. Fraction of heterogeneous sensor nodes in state *I* in terms of φ and time when $\gamma > 1$.

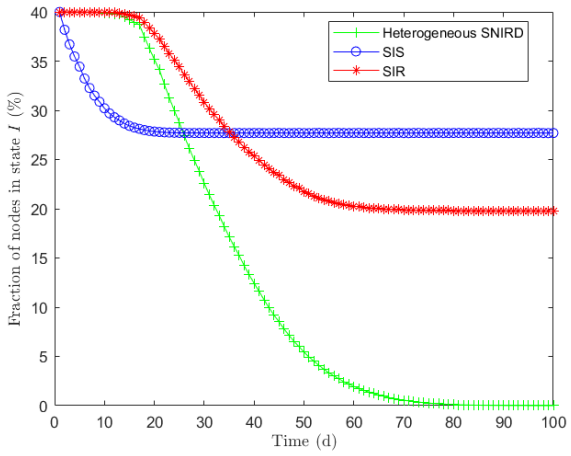

FIGURE 12. Infectious node fraction comparison among the heterogeneous SNIRD, SIS, and SIR models, when $\gamma < 1$.

fraction of heterogeneous sensor nodes in state *I* is selected as the comparison object, because this fraction of infectious nodes determines the effectiveness of the epidemic malware models.

Figs. 12 and 13, where the initial fraction of infectious nodes is set at 40%, show the comparisons among the three epidemic models under cases $\gamma < 1$ and $\gamma > 1$, respectively. From Fig. 12, the fractions of the heterogeneous sensor nodes

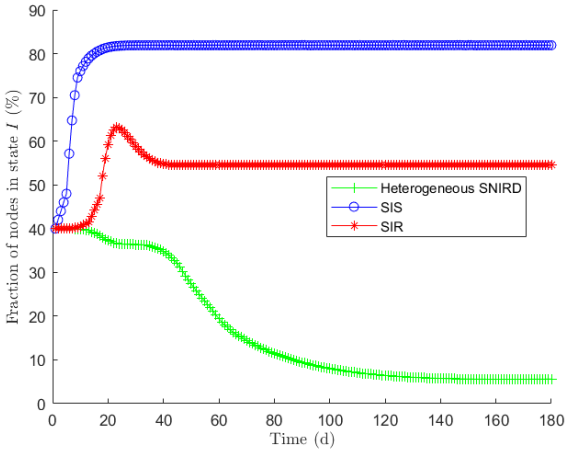

FIGURE 13. Infectious node fraction comparison among the heterogeneous SNIRD, SIS, and SIR models, when $\gamma > 1$.

in state I belonging to the SIS and SIR models converge to ∼27.7% and ∼20.2% after ∼26 d and ∼61 d, respectively. The fraction of infectious nodes in the heterogeneous SNIRD model has a similar trend to the SIR model in the beginning ∼16 d. Afterwards, it obviously decreases quicker than that of the SIR model. In addition, it is greater than that of the SIS model in the beginning ∼26 d. However, this infectious fraction converges to 0 after ∼80 d, which shows the effectiveness of the heterogeneous SNIRD model from the view of achieving the final equilibrium. Fig. 13 shows that the fractions of infectious nodes belonging to the SIS and SIR models converge to ∼81.9% and ∼54.61% after ∼28 d and ∼52 d, respectively. Different from the increasing trend of the infectious fractions in the SIS and SIR models, the infectious fraction belonging to the heterogeneous SNIRD model gradually decreases and finally converges to ∼5.63% after ∼150 d. According to the above analyses, the heterogeneous SNIRD model is obviously the most efficient one for the suppression of malware in heterogeneous WSNs.

In fact, the SIS and SIR models cannot reflect the actual case of a heterogeneous sensor node being dysfunctional due to physical deterioration, energy exhaustion, or malware attacks. Moreover, the SIS model cannot reflect the case that an infected node is cured and becomes immune to known malware threats by patching security programs. Therefore, the heterogeneous SNIRD model is more appropriate for heterogeneous WSNs.

VII. CONCLUSION

Motivated by the spread of malware in heterogeneous WSNs, a heterogeneous SNIRD model was proposed, which considers states of insidious sensor nodes infected by malware and dysfunctional nodes, as well as the communication connectivity heterogeneity of nodes. Fraction evolution equations were obtained, which can discover the changeable quantities of all the heterogeneous sensor nodes in heterogeneous WSNs under the spread of malware. It was proved that the equilibria of the heterogeneous SNIRD model exist, and the malware spread threshold was obtained, which can indicate whether the malware will spread or dissipate. In this manner, a theoretical guideline was constructed to enable administrators to suppress the spread of malware in heterogeneous WSNs.

In the heterogeneous SNIRD model, nodes in state D are dysfunctional and cannot be repaired. However, a given node can be repaired from a given infection but new threats exist for it. This consideration will produce different fractions R_k^t and D_k^t when time evolves from $t-1$ to t, leading to a different SNIRD model. It is interesting and can be considered as the future work.

In addition, adding the proof of the stability of equilibria points will make the heterogeneous SNIRD model be more mathematically rigorous. Based on these theoretical results, one can further obtain the optimal strategies to control the malware spread in the heterogeneous WSNs. These works also constitute the future directions.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[2] T. Qiu, N. Chen, K. Li, M. Atiquzzaman, and W. Zhao, "How can heterogeneous Internet of Things build our future: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2011–2027, 3rd Quart., 2018,

[3] J. Wang, Y. Gao, W. Liu, A. K. Sangaiah, and H.-J. Kim, "An improved routing schema with special clustering using PSO algorithm for heterogeneous wireless sensor network," *Sensors*, vol. 19, no. 3, Feb. 2019, Art. no. 671.

[4] S. He, K. Xie, W. Chen, D. Zhang, and J. Wen, "Energy-aware routing for SWIPT in multi-hop energy-constrained wireless network," *IEEE Access*, vol. 6, pp. 17996–18008, 2018.

[5] J. Wang, C. Ju, Y. Gao, A. K. Sangaiah, and G.-J. Kim, "A PSO based energy efficient coverage control algorithm for wireless sensor networks," *Comput., Mater. Continua*, vol. 56, no. 3, pp. 433–446, Jan. 2018.

[6] S. He, K. Xie, K. Xie, C. Xu, and J. Wang, "Interference-aware multisource transmission in multiradio and multichannel wireless network," *IEEE Syst. J.*, to be published. doi: 10.1109/JSYST.2019.2910409.

[7] 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.

[8] S. Yu, G. Wang, and W. Zhou, "Modeling malicious activities in cyber space," *IEEE Netw.*, vol. 29, no. 6, pp. 83–87, Nov./Dec. 2015.

[9] S. Yu, G. Gu, A. Barnawi, S. Guo, and I. Stojmenovic, "Malware propagation in large-scale networks," *IEEE Trans. Knowl. Data Eng.*, vol. 27, no. 1, pp. 170–179, Jan. 2015.

[10] 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.

[11] 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.

[12] 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.

[13] 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, Nov. 2015, Art. no. 184239.

[14] J. Liu, M. Xu, X. Wang, S. Shen, and M. Li, "A Markov detection tree-based centralized scheme to automatically identify malicious webpages on cloud platforms," *IEEE Access*, vol. 6, pp. 74025–74038, Nov. 2018.

[15] S. Sharmeen, S. Huda, J. H. Abawajy, W. N. Ismail, and M. M. Hassan, "Malware threats and detection for industrial mobile-IoT networks," *IEEE Access*, vol. 6, pp. 15941–15957, Mar. 2018.

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

[17] Q. Gu, C. Ferguson, and R. Noorani, "A study of self-propagating malpackets in sensor networks: Attacks and defenses," *Comput. Secur.*, vol. 30, no. 1, pp. 13–27, Jan. 2011.

[18] 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.

[19] S. Shen, L. Huang, J. Liu, A. C. Champion, S. Yu, and Q. Cao, "Reliability evaluation for clustered WSNs under malware propagation," *Sensors*, vol. 16, no. 6, Jun. 2016, Art. no. 855.

[20] 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.

[21] N. R. Zema, E. Natalizio, G. Ruggeri, M. Poss, and A. Molinaro, "MeDrone: On the use of a medical drone to heal a sensor network infected by a malicious epidemic," *Ad Hoc Netw.*, vol. 50, pp. 115–127, Nov. 2016.

[22] T. Wang, Q. Wu, S. Wen, Y. Cai, H. Tian, Y. Chen, and B. Wang, "Propagation modeling and defending of a mobile sensor worm in wireless sensor and actuator networks," *Sensors*, vol. 17, no. 1, Jan. 2017, Art. no. 139.

[23] G. Theodorakopoulos, J.-Y. Le Boudec, and J. S. Baras, "Selfish response to epidemic propagation," *IEEE Trans. Autom. Control*, vol. 58, no. 2, pp. 363–376, Feb. 2013.

[24] P.-Y. Chen, C.-C. Lin, S.-M. Cheng, H.-C. Hsiao, and C.-Y. Huang, "Decapitation via digital epidemics: A bio-inspired transmissive attack," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 75–81, Jun. 2016.

[25] A. Mahboubi, S. Camtepe, and H. Morarji, "A study on formal methods to generalize heterogeneous mobile malware propagation and their impacts," *IEEE Access*, vol. 5, pp. 27740–27756, Dec. 2017.

[26] 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.

[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] M. S. Haghighi, S. Wen, Y. Xiang, B. Quinn, and W. Zhou, "On the race of worms and patches: Modeling the spread of information in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2854–2865, Dec. 2016.

[29] R. K. Upadhyay and S. Kumari, "Bifurcation analysis of an e-epidemic model in wireless sensor network," *Int. J. Comput. Math.*, vol. 95, no. 9, pp. 1775–1805, Sep. 2018.

[30] P. Lee, A. Clark, B. Alomair, L. Bushnell, and R. Poovendran, "Adaptive mitigation of multi-virus propagation: A passivity-based approach," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 583–596, Mar. 2018.

[31] X. Wang, Z. He, X. Zhao, C. Lin, Y. Pan, and Z. Cai, "Reaction-diffusion modeling of malware propagation in mobile wireless sensor networks," *Sci. China-Inf. Sci.*, vol. 56, no. 9, pp. 1–18, Sep. 2013.

[32] X. Wang, Z. He, and L. Zhang, "A pulse immunization model for inhibiting malware propagation in mobile wireless sensor networks," *Chin. J. Electron.*, vol. 23, no. 4, pp. 810–815, Oct. 2014.

[33] L. Zhu, H. Zhao, and X. Wang, "Bifurcation analysis of a delay reaction–diffusion malware propagation model with feedback control," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 22, nos. 1–3, pp. 747–768, May 2015.

[34] 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.

[35] L. Feng, L. Song, Q. Zhao, and H. Wang, "Modeling and stability analysis of worm propagation in wireless sensor network," *Math. Problems Eng.*, vol. 2015, Aug. 2015, Art. no. 129598.

[36] X. Wang, W. Ni, K. Zheng, and R. P. Liu, "Virus propagation modeling and convergence analysis in large-scale networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 10, pp. 2241–2254, Nov. 2016.

[37] S. Xu, W. Lu, and Z. Zhan, "A stochastic model of multivirus dynamics," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 1, pp. 30–45, Jan. 2012.

[38] H. Kang, Y. Yu, B. Bao, X. Fu, and M. Sun, "Spreading dynamics of an SEIR model with delay on scale-free networks," *IEEE Trans. Netw. Sci. Eng.*, to be published. doi: 10.1109/TNSE.2018.2860988.

[39] J. D. H. Guillén, A. M. del Rey, and L. H. Encinas, "Study of the stability of a SEIRS model for computer worm propagation," *Physica A, Stat. Mech. Appl.*, vol. 479, pp. 411–421, Aug. 2017.

[40] D. Tian, C. Liu, Z. Sheng, M. Chen, and Y. Wang, "Analytical model of spread of epidemics in open finite regions," *IEEE Access*, vol. 5, pp. 9673–9681, Apr. 2017.

[41] B. Qu and H. Wang, "SIS epidemic spreading with heterogeneous infection rates," *IEEE Trans. Netw. Sci. Eng.*, vol. 4, no. 3, pp. 177–186, Jul./Sep. 2017.

[42] C. Nowzari, V. M. Preciado, and G. J. Pappas, "Optimal resource allocation for control of networked epidemic models," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 2, pp. 159–169, Jun. 2017.

[43] S. Eshghi, M. H. R. Khouzani, S. Sarkar, and S. S. Venkatesh, "Optimal patching in clustered malware epidemics," *IEEE/ACM Trans. Netw.*, vol. 24, no. 1, pp. 283–298, Feb. 2016.

[44] 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, 2017.

[45] L. Wang and G.-Z. Dai, "Global stability of virus spreading in complex heterogeneous networks," *SIAM J. Appl. Math.*, vol. 68, no. 5, pp. 1495–1502, 2008.

[46] J. Liu and T. Zhang, "Epidemic spreading of an SEIRS model in scale-free networks," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, no. 8, pp. 3375–3384, Aug. 2011.

[47] G. Zhu, X. Fu, and G. Chen, "Global attractivity of a network-based epidemic SIS model with nonlinear infectivity," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 6, pp. 2588–2594, Jun. 2012.

[48] P. van den Driessche and J. Watmough, "Reproduction numbers and subthreshold endemic equilibria for compartmental models of disease transmission," *Math. Biosci.*, vol. 180, no. 12, pp. 29–48, Nov./Dec. 2002.

[49] 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.

[50] T. Qiu, A. Zhao, F. Xia, W. Si, and D. O. Wu, "ROSE: Robustness strategy for scale-free wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 25, no. 5, pp. 2944–2959, Oct. 2017.

[51] H. Peng, S. Si, M. K. Awad, N. Zhang, H. Zhao, and X. S. Shen, "Toward energy-efficient and robust large-scale WSNs: A scale-free network approach," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 4035–4047, Dec. 2016.

SHIGEN SHEN 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.

HAIPING ZHOU received the B.S. degree in food science and engineering from Nanchang University, Nanchang, China, in 2001, and the M.S. degree in theoretical physics and the Ph.D. degree in microelectronics and solid-state electronics from Guizhou University, Guiyang, China, in 2006 and 2009, respectively.

He is currently a Professor with the Department of Computer Science and Engineering, Shaoxing University, Shaoxing, China. His current research interests include complex networks and recommendation algorithm.

SHENG FENG received the B.S. in computing from the University of Greenwich, London, U.K., in 2004, and the M.S. degree in software engineering and the Ph.D. degree in pattern recognition and intelligent system from Northeastern University, Shenyang, China, in 2013 and 2017, respectively.

He is currently a Lecturer with the Department of Computer Science and Engineering, Shaoxing University, Shaoxing, China. His research interests include intelligent robot, computer vision, and wireless sensor networks.

JIANHUA LIU received the B.S. degree in computer science and technology from Xinyang Normal University, Xinyang, China, in 2004, the M.S. degree in computer application technology from Shanghai Normal University, Shanghai, China, in 2008, and the Ph.D. degree in computer application technology from Shanghai University, Shanghai, in 2012.

He was a Visiting Scholar with the State University of New York, Buffalo, in 2014. He is currently an Associate Professor with the Department of Computer Science and Engineering, Shaoxing University, Shaoxing, China. His research interests include distributed computing, wireless communications, multimedia networking, and wireless sensor networks.

QIYING CAO received the B.S. degree from Harbin Engineering University, Harbin, China, in 1982, and the M.S. and Ph.D. degrees from Jiangsu University, Zhenjiang, China, in 1993 and 1998, respectively.

From 1999 to 2001, he was a Postdoctoral Researcher with the Chunlan Research Institute, Taizhou, China. He is currently a Professor with the College of Computer Science and Technology, Donghua University, Shanghai, China. His current research interests include pervasive computing and intelligent information processing.