Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 3847016, 9 pages
https://doi.org/10.1155/2021/3847016

Corrigendum

Corrigendum to "Nodes Availability Analysis of NB-IoT Based Heterogeneous Wireless Sensor Networks under Malware Infection"

Xiaojun Wu,[1] **Qiying Cao**,[2] **Juan Jin**,[2] **Yuanjie Li**,[3] **and Hong Zhang**[2]

[1]*College of Information Science and Technology, Donghua University, Shanghai 201620, China*
[2]*College of Computer Science and Technology, Donghua University, Shanghai 201620, China*
[3]*School of Information Management, Shanghai Lixin University of Accounting and Finance, Shanghai 201620, China*

Correspondence should be addressed to Xiaojun Wu; wxj@dhu.edu.cn

Received 24 August 2020; Accepted 24 August 2020; Published 28 January 2021

In the article titled "Nodes Availability Analysis of NB-IoT Based Heterogeneous Wireless Sensor Networks Under Malware Infection" [1], there were errors that have been corrected in the revised version shown below.

(i) Related Works
(ii) Topology Structure of NBIOT-HWSNs
(iii) Malicious Program Propagation Mechanism in NBIOT-HWSNs
(iv) Node Availability Analysis of NBIOT-HWSN
(v) Numerical Simulation and Analysis
(vi) Conclusion
(vii) Acknowledgement Section
(viii) Figures 1, 2, 3, and 4 have been corrected
(ix) Tables 1 and 2 have been corrected.

The corrected article is as follows.

I. Introduction

The development of a new generation of mobile communication technologies has provided support conditions for the application of wireless sensor networks in more fields and has also boosted the development of wireless sensor networks in smart traffic, smart wearable, remote medical monitoring, smart meter development, and other industries. The Narrowband Internet of Things (NB-IoT) standard based on mobile cellular network commonly participated in and formulated by Huawei, ZTE, and other companies and many global enterprises shows itself in a variety of standards. The core of the standard protocol has passed the 3GPP standardized evaluation in 2016, and the mobile communication company has started the commercial application of NB-IoT. Because NB-IoT has the advantages of penetration coverage, large access capacity, and low energy consumption [1], it can be networked with WSNs, and some nodes become dual-mode convergence nodes of WSNs and NB-IoT, optimizing the network structure, reducing redundant data, and increasing efficiency.

Security issues around WSNs are important factors to be considered in topological design and operating maintenance. In the research and analysis of traditional WSNs security problems, because many nodes in the network are homogeneous, they have the same antiattack and antimalware capabilities. Therefore, the possibility of a network node being attacked by a malicious program is only relevant to the throughput of the information exchange behavior. The greater the probability of the connection of node, the greater the probability of being infected by a malicious program, and the greater the probability of being infected. After extensive application of NB-IoT to WSNs, the logical distance between nodes and application networks is quite different. The nodes in the hybrid network have heterogeneity. They have different degrees of nodes and vulnerability and thus constitute a Heterogeneous Wireless Sensor Networks [2] (HWSNs); here, we define it as NBIOT-HWSNs.

The availability of WSN nodes represent the probability with that the node can work normally in the network [3]. It is one of the important indexes for measuring the node performance. In actual calculations, it is usually expressed by the probability of the available state when the network reaches a steady state. For a node, its availability when it reaches a stable state is related to its own energy and the environment in which it is located. To assess the availability of the NBIOT-HWSN network, we must first analyze the availability of its constituent nodes. Therefore, how to evaluate the availability of nodes is one of the key issues in measuring the performance of NBIOT-HWSNs. In this paper, based on the previous research on the availability of heterogeneous wireless sensor network nodes, combined with the characteristics of NBIOT-HWSNS, by extending the classical epidemiological model and Markov chain, based on the node heterogeneity, the node state analysis method attacked by malicious programs is given, and the effects of the degree of nodes on the availability of nodes are studied. Firstly, by observing the relationship between the degree of nodes and the antiattack ability of nodes in the actual network, a heterogeneity model of the sensor node based on the difference in the degree of nodes is given, and the infection rate function is defined. Then, based on the classical epidemic model, a SIRLD state transition model is established. Based on the Markov chain, the dynamic equation of the transition between states of the heterogeneous sensor nodes is given. Finally, the formula for calculating the availability of heterogeneous nodes is given when the NBIOT-HWSNs reach the dynamic equilibrium state.

II. Related Works

Recently, researchers around the world have put forward some solutions to the security of wireless sensor networks from different perspectives and analyzed the influence of node heterogeneity and availability of heterogeneous wireless sensor networks on the prevention and treatment of viruses.

Research [4, 5] showed that WSNs are vulnerable to attacks, and malware can spread from nodes to nodes in WSNs. Likewise, Illiano and Lupu [4] found that embedded sensors are vulnerable to compromise by external actors through malware but also through their wireless and physical interfaces. Compromised sensors can be made to report false measurements with the aim at producing inappropriate and potentially dangerous responses. Such malicious data injections can be particularly difficult to detect if multiple sensors have been compromised as they could emulate plausible sensor behavior such as failures or detection of events where none occur. Gu et al. [5] found that memory fault attacks in sensors are not the same as in regular computers due to sensor's hardware and software architecture, a special mal-packet, which only carries specially crafted data, can exploit memory-related vulnerabilities and utilize existing application code in a sensor to propagate itself.

Research [6–10] studied different kinds of malicious program propagation models; these models are from the Epidemic Dynamics Theory, Cellular Automaton Theory, Queuing Theory, etc. The following are some impressive research models. Wang et al. [6] investigated the stability of information spreading over SNS, discovered the principles inherent in the spreading behavior, and then defined a SEIR-(Susceptible-Exposed-Infectious-Removed-) based model for the information spreading over SNS. Costa et al. [7] proposed a representation of the dynamics of epidemics through a compartmental SIR (Susceptible-Infected-Recovered) model, with the combined use of geo-referenced cellular automata and fuzzy systems. Qu and Wang [8] proposed a heterogeneous infection susceptible CSIS model in which the degree of infection is associated with the scale of the two nodes, and the effect of node heterogeneity on virus propagation in scale-free networks and random networks. Essouifi and Achahbar [9] studied the SIR-SIS (Susceptible-Infectious-Removed and SIS) hybrid model of computer viruses spreading in a two-dimension network and used the SIR model for node classes that required protection and security, and other models using SIS models. Mishra and Keshri [10] studied the characteristics of the worm attack behavior in the wireless sensor network and established a virus-processing model using the immune method of infectious diseases, and the simulation results showed that the security could be improved.

Some WSN reliability evaluation methods are used in published articles [11–14]. Shen et al. [11] proposed an effective method for estimating the steady availability of heterogeneous sensor networks for malicious program propagation in order to predict the available performance of heterogeneous sensor networks. Combined with the use of the complete information static game, Markov chain, and reliability theory into a method to evaluate the survivability of cluster heterogeneity sensor networks under malicious program propagation environment, Kabadurmus and Smith [12] proposed a new indicator that combines network reliability and network resiliency to assess network reliability. Arslan et al. [13] established the Markov model for effective data detection and fault tolerance of wireless sensor network nodes and conducted simulation analysis. Zhang and Dong [14] created an OBDD-based method for availability evaluation of WSN.

With the development of heterogeneous WSNs, some latest research [15–18] show their characters and new development. Fan et al. [15] studied the cross-layer protocol of heterogeneous sensor networks and discussed the development direction of cross-layer design of heterogeneous sensor networks. Karyotis et al. [16] demonstrated the developed model in various complex networks, showing how it can be exploited for analytically quantifying network reliability and further used for increasing the robustness of the network against generic malware attacks. Shen et al. [17] considered Heterogeneous Wireless Sensor Networks (HWSNs) with malware diffusion and a solution to assess their dependability in order to guarantee dependable operations on sending sensed data from sensor nodes (SNs) to a sink node. Kasraoui et al. [18] focused the IPv6 over Low power Wireless Personal Area Networks (6LoWPANs) which interconnects the Heterogeneous Wireless Sensor Networks (HWSNs) with the Internet. They also proposed a novel Cooperative Key Exchange System (CKES) by using the concept of Chinese Remainder Theorem (CRT).

III. Topology Structure of NBIOT-HWSNs

There are many methods for combining NB-IoT technology and WSNs. One of them is to use NB-IoT nodes and WSNs nodes to form a network according to their own characteristics to give full play to the characteristics of random deployment, flexible networking, and low cost of traditional WSNs nodes and the characteristics of wireless wide area access, low power consumption, long life cycle, and strong penetration capabilities of NB-IoT. Figure 1 shows a typical NBIOT-HWSN structure.

NBIOT-HWSNs nodes can be divided into two categories: one is the common sensor node that is randomly distributed inside or within the monitoring area. There are a large number of such nodes, and there is no great demand for processing capacity, storage capacity, and communication capability. It is often composed of inexpensive miniature sensors, which are mainly responsible for data acquisition and data transmission. The other is sink/cluster head nodes for data aggregation. The capabilities of these nodes are stronger than those of sensor nodes, and their impact on the entire NBIOT-HWSNs is also greater. The data that the sensor node monitors can be transmitted along other sensor nodes and finally aggregated to the aggregation node. For NBIOT-HWSNs, due to the large area to be deployed and the limited communication distance between nodes, it is usually necessary to deploy multiple sensor subnets. Each sensor subnet has its own aggregation/cluster head node, and the aggregation/cluster head nodes of this subnet are responsible for data transmission of the aggregation/cluster head nodes at the upper level.

In the NBIOT-HWSN, nodes at different hierarchical locations and different functions have different degrees of nodes. A node with a smaller degree of node has a single node function, and the supporting security mechanism is also simple. The probability of being controlled by a malicious program of a virus is larger, and a node with a larger degree of node is configured with a system access restriction, a security firewall, and other mechanisms when the network is designed to improve the ability to prevent attack and cracking and reduce the probability of successful attacks. If the degree of node is defined as k and its vulnerability function is defined as $d(k)$, then the greater the probability of a successful attack by a malicious program is, the greater the value of $d(k)$ is. In other words, $d(k)$ is a monotonically decreasing function whose specific form is determined by the environment, structure, etc. of the NBIOT-HWSNs.

In actual NBIOT-HWSNs, node vulnerability affects the nodes' resistance to malicious program's attack, and thereby, the node vulnerability function is used to represent the infection rate when a heterogeneous sensor node is attacked by a malicious program. For a heterogeneous sensor node i with the degree of node k, the probability of being infected by a malicious program can be defined as (1), where m is the normalization constant.

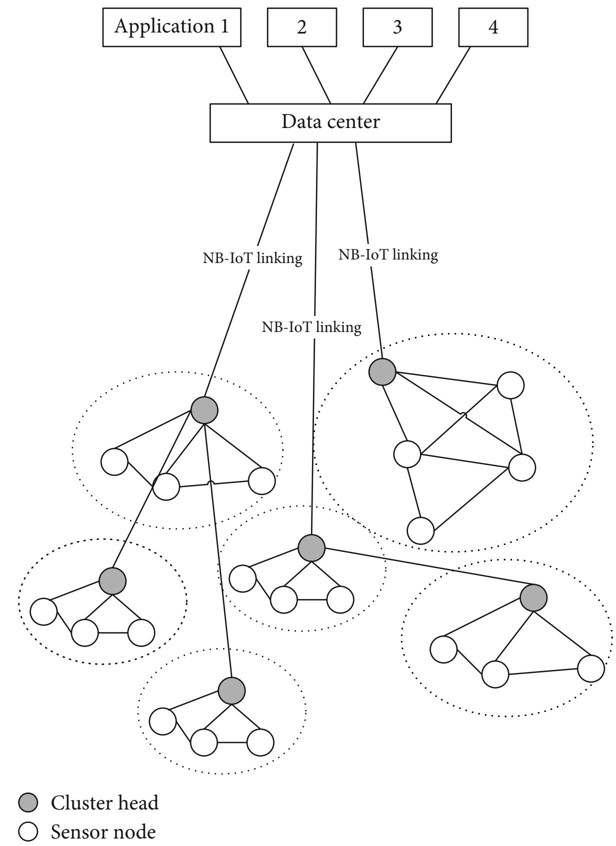

Figure 1: Schematic diagram of NBIOT-HWSNs.

$$\zeta_i(k) = m * d(k). \tag{1}$$

Assume that the degree of node in the NBIOT-HWSNs obeys the distributionPr $(K = k)$; the probability of the degree of node k is $P(k)$, the number of nodes in the NBIOT-HWSNs is N, and by the average of the two sides of the formula (1), the following can be obtained.

$$\bar{\zeta} = \frac{1}{N}\sum_{i\in N}\zeta_i(k) = m\sum_{k}\zeta_i(k)P(k) = m < d(k) > . \tag{2}$$

Therefore, the value of constant m is $m = \bar{\zeta}/<d(k)>$, and being substituted into (1), the following can be obtained:

$$\zeta_i(k) = \frac{\zeta d(k)}{<d(k)>}, \tag{3}$$

in which $<d(k)>$ is the mean value of the integral of $d(k)$, which is determined by the distribution function of the degree of node. $\bar{\zeta}$ refers to the node infection probability when the node vulnerability function $d(k) = 1$, that is, when the node vulnerability is the same. At this time, the infection probability of each node is the same, which are all $\bar{\zeta}$. When the structures of NBIOT-HWSNs are ready, $<d(k)>$ and $\bar{\zeta}$ are all constants.

IV. Malicious Program Propagation Mechanism in NBIOT-HWSNs

In NBIOT-HWSNs, malicious programs acquire their data and transmit it by infecting susceptible nodes. This mode of transmission is similar to the infectious disease transmission process. Therefore, this paper draws on the SIR and SIRD model in the classical epidemiological theory to describe the state changes of nodes in the process of infection of NBIOT-HWSN malicious programs and develops it to a new SIRLD model. Among them, the states of the sensor nodes are divided into susceptible state, infected state, recovered state, and dead state. Susceptible state refers to a state in which a NBIOT-HWSN node has security vulnerability but has not yet been infected by a malicious program and may be infected by a malicious program, abbreviated as state S, and the node in this state is a susceptible node. The infected state refers to a state in which a susceptible node is discovered and infected by a malicious program, controlled by a malicious program, and has the ability to infect, abbreviated as state I. The node in this state is an infection node; the recovered state refers to a state in which the security vulnerability of a node is found or security patches are installed after being infected with a malicious program and after it was cleared, abbreviated as state R. The node in this state is an immune node; the dead state refers to a state in which a node has failed due to a malicious program attack or energy exhaustion, abbreviated as state D. The node in this state is a dead node. With the development of solar energy, WSN node can be powered by solar battery, and then, the dead state nodes may recover after sunshine charging. A new state of "Lost Connection" abbreviated as state L is added to the cycle. The nodes in state L may go to state D after a set time or go back to their original state I, R, or S. The heterogeneous sensor node state transition model is shown in Figure 2.

For a heterogeneous sensing node i with the degree of node k, there are k neighboring nodes that communicate with it, which may attack node i, so that node i is converted from state S to state I. Therefore, the state of node i at time t is related to the state of node at time $t-1$ and the states of k neighboring nodes. Expressions like$p_i^S(t), p_i^I(t), p_i^R(t), p_i^L(t), p_i^D(t)$ are defined as the probabilities of node i at times of t in states of S, I, R, L, D separately, and $q_i^{xy}(t)$ represents the probability that the node transitions from the state x to the state y, in which $x, y \in \{S, I, R, L, D\}$. In the initial stage of establishment, necessary security patches have been installed in the node of any one HWSN to have resistance to existing malicious programs, so the initial state is R, i.e., $p_i^R(0) = 1$, $p_i^S(0) = p_i^I(0) = p_i^L(0) = p_i^D(0) = 0$.

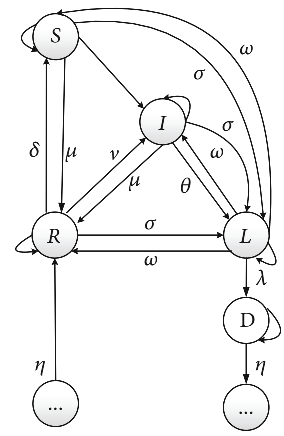

Figure 2: Node state transition diagram of NBIOT-HWSNs.

The Intrusion Detection System (IDS) in NBIOT-HWSNs can scan for malicious programs and install security patches for heterogeneous sensor nodes. When IDS finds a security hole in node i or node i has been infected by a malicious program, IDS can install a security patch for it to convert it from state S or state I to state R. Assume that the IDS detection rate and false alarm rate are μ and ν, respectively. A heterogeneous sensor node has the possibility of exhausting energy or being damaged by other reasons. Node i will change from state S to state L with rate θ. The node will continue to change to state D with rate λ if it cannot wake up with battery charging during a limit time; otherwise, it returns to former state with rate ω. During simulation, the probability of node changing to state L not caused by the damage of malicious program is defined as σ.

For any heterogeneous sensor node i, as the degree of node increases, the contact probability between node i and the infected node also increases. Therefore, the probability of being attacked by a malicious program increases. Define the probability of a neighboring node in state I attacking node i as ρ_I. When node i in state S at time t contacts with an unknown node, the probability of being successfully attacked by a malicious program can be expressed as $p_i^I(t)\rho_I\zeta_i(k)$; correspondingly, the probability of not being infected by a malicious program is $1 - p_i^I(t)\rho_I\zeta_i(k)$.

Further, node i may communicate with surrounding k neighboring nodes. If a certain neighboring node of node i is in state I, it is possible for the node to attack node i. As long as an infected node attacks it and the infection is successful, the node will change from state S to state I. Therefore, when node i contacts with k unknown nodes, the probability of node i being infected cannot be expressed as $(1 - p_i^I(t)\,\rho_I\zeta_i(k))^k$. In addition, the node may also be detected by the IDS, and the security patches are installed for it, that is, the state S transitions to the state R. It may also cause the death of node due to physical reasons, that is, state S transitions to the state L. Then, it will continue to the state D if it cannot wake up during a limit time. Therefore, the probability of a state transition for node i that is in state S at time t can be expressed as

$$\begin{cases} q_i^{SS}(t) = \left[1 - \zeta_i(k)\rho_I p_i^I(t-1)\right]^k - \mu - \sigma \\ q_i^{SI}(t) = 1 - \left[1 - \zeta_i(k)\rho_I p_i^I(t-1)\right]^k \\ q_i^{SR}(t) = \mu \\ q_i^{SL}(t) = \sigma - \omega \\ q_i^{SD}(t) = 0. \end{cases} \tag{4}$$

From Figure 2, we can see that when node i is in state I, it cannot be converted into state S, but it may be damaged by a malicious program to change from state I to state D. The probability of being damaged by a malicious program is defined as θ. When node i is detected by IDS, IDS will install a security patch for it to change from state I to state R. When node i is killed by a malicious program or the node is dead due to physical reasons, the node i will be converted from state I to state L. Therefore, the probability of the state transition for node i that is in state S at time t can be expressed as

$$\begin{cases} q_i^{\mathrm{IS}}(t) = 0 \\ q_i^{II}(t) = 1 - \mu - \theta - \sigma \\ q_i^{IR}(t) = \mu \\ q_i^{IL}(t) = \sigma + \theta - \omega \\ q_i^{ID}(t) = 0. \end{cases} \tag{5}$$

For node i in state R, when a malicious program finds a new security hole, it will make the heterogeneous sensor node have the possibility of being attacked, making it convert from state R to state S. This probability is defined as δ. The IDS may be misreported to mistake the node in state R as an infected node, making it convert from state R to state I. At the same time, node i also has the possibility of death due to physical reasons. From the above analysis, it can be concluded that the probability of the state transition for node i that is in state R at time t can be expressed as

$$\begin{cases} q_i^{\mathrm{RS}}(t) = \delta \\ q_i^{\mathrm{RI}}(t) = \nu \\ q_i^{\mathrm{RR}}(t) = 1 - \delta - \nu - \sigma \\ q_i^{\mathrm{RL}}(t) = \sigma - \omega \\ q_i^{\mathrm{RD}}(t) = 0. \end{cases} \tag{6}$$

For node i in state L, it is a temporary state of losing connections with all neighbor nodes from states S, R, and I because of all kinds of reasons like out of battery, physical damage, human's removal, and malicious attack. These kinds of nodes may recover from state L to its formal states like S, R, and I after sunshine charging battery or human moving back. It also may change to state D after a limit time if no possibility to recover. From the above analysis, it can be concluded that the probability of the state transition for a node i that is in state L at time t can be expressed as

$$\begin{cases} q_i^{\mathrm{LS}}(t) = \omega \\ q_i^{\mathrm{LI}}(t) = \omega \\ q_i^{\mathrm{LR}}(t) = \omega \\ q_i^{\mathrm{LL}}(t) = 1 - \omega - \lambda \\ q_i^{\mathrm{LD}}(t) = \lambda. \end{cases} \tag{7}$$

In order to guarantee the availability of NBIOT-HWSNs, it is necessary to put into new heterogeneous sensor nodes. In order to keep the number of nodes in the NBIOT-HWSNs stable, it is assumed that the user adds new healthy nodes to the HWSNs with a probability of η per unit time and clears the dead nodes with a probability of η, and the initial state of the new node is R. Therefore, the probability of the state transition for a node i that is in state D at time t can be expressed as

$$\begin{cases} q_i^{\mathrm{DS}}(t) = 0 \\ q_i^{\mathrm{DI}}(t) = 0 \\ q_i^{\mathrm{DL}}(t) = 0 \\ q_i^{\mathrm{DR}}(t) = \eta \\ q_i^{\mathrm{DD}}(t) = 1 - \eta. \end{cases} \tag{8}$$

From Figure 2, we can see that the nodes in the three states of S, R, and L at time t may be converted into state S at time t, and the nodes in the four states of S, I, R, and L may be converted to state I at time t, and the nodes in the four states of S, I, R, and L may be converted to state R at time t, and the nodes in the four states of S, I, R, and L may be converted to state L at time t. Only two states L and R have the possibilities to convert to state D at time t. Therefore, the probability of node i in each state at time t can be expressed as

$$\begin{cases} p_i^S(t) = \left(q_i^{SS}(t) - q_i^{SI}(t) - q_i^{SR}(t) - q_i^{SL}(t)\right)p_i^S(t-1) + q_i^{RS}(t)p_i^R(t-1) + q_i^{LS}(t)p_i^L(t-1) \\ p_i^I(t) = \left(q_i^{II}(t) - q_i^{IR}(t) - q_i^{IL}(t)\right)p_i^I(t-1) + q_i^{SI}(t)p_i^S(t-1) + q_i^{RI}(t)p_i^R(t-1) + q_i^{LI}(t)p_i^L(t-1) \\ p_i^R(t) = \left(q_i^{RR}(t) - q_i^{RI}(t) - q_i^{RS}(t) - q_i^{RL}(t)\right)p_i^R(t-1) + q_i^{IR}(t)p_i^I(t-1) + q_i^{SR}(t)p_i^S(t-1) + q_i^{LR}(t)p_i^L(t-1) \\ p_i^L(t) = \left(q_i^{LL}(t) - q_i^{LR}(t) - q_i^{LI}(t) - q_i^{LR}(t) - q_i^{LS}(t) - q_i^{LD}(t)\right)p_i^L(t-1) + q_i^{IL}(t)p_i^I(t-1) + q_i^{RL}(t)p_i^R(t-1) + q_i^{SL}(t)p_i^S(t-1) \\ p_i^D(t) = p_i^D(t-1) + q_i^{LD}(t)p_i^L(t-1). \end{cases} \tag{9}$$

Substituting (4)-(7) into (8), we can get the dynamic equation of the transition between each state of node i at time t.

$$\begin{cases} p_i^S(t) = p_i^S(t-1)\left\{\left[1-\zeta_i(k)\rho_I p_i^I(t-1)\right]^k - \mu - \sigma\right\} + p_i^R(t-1)\delta + p_i^L(t-1)\omega \\ p_i^S(0) = 0, \end{cases} \tag{10}$$

$$\begin{cases} p_i^I(t) = p_i^S(t-1)\left\{1-\left[1-\zeta_i(k)\rho_I p_i^I(t-1)\right]^k\right\} + p_i^I(t-1)(1-\mu-\theta-\sigma) + p_i^R(t-1)\nu + p_i^L(t-1)\omega \\ p_i^I(0) = 0, \end{cases} \tag{11}$$

$$\begin{cases} p_i^R(t) = p_i^S(t-1)\mu + p_i^I(t-1)\mu + p_i^R(t-1)(1-\delta-\nu-\sigma) + p_i^L(t-1)\omega + p_i^D(t-1)\eta \\ p_i^R(0) = 1, \end{cases} \tag{12}$$

$$\begin{cases} p_i^L(t) = p_i^S(t-1)\sigma + p_i^I(t-1)(\sigma+\theta-\omega) + p_i^R(t-1)(\sigma-\omega) - p_i^L(t-1)\lambda \\ p_i^D(0) = 0, \end{cases} \tag{13}$$

$$\begin{cases} p_i^D(t) = p_i^L(t-1)\lambda - p_i^D(t-1)\eta \\ p_i^D(0) = 0. \end{cases} \tag{14}$$

V. Node Availability Analysis of NBIOT-HWSN

According to reliability theory, the reliability of an NBIOT-HWSN node i at time t is called instantaneous availability, recorded as $\tau_i(k,t)$. After NBIOT-HWSNs run for a long period of time, that is, when t tends to infinity, the node reaches a stable state. At this time, the availability is called the steady-state availability (recorded as $D_i(k)$), so the node steady-state availability can be expressed as

$$D_i(k) = \lim_{t\to\infty} \tau_i(k,t). \tag{15}$$

The probabilities of heterogeneous sensor node i in each state when it reaches a stable state are defined as $P_S(k), P_I(k), P_R(k), P_L(k), P_D(k)$, and the following can be obtained:

$$P_S(k) + P_I(k) + P_R(k) + P_L(k) + P_D(k) = 1. \tag{16}$$

For ease of writing, define $\Delta(k) = \left[1-\zeta_i(k)\rho_I p_i^I(t-1)\right]^k$, and when node i reaches a stable state,

$$\begin{cases} P_i^S(k) = (\Delta(k)-\mu-\sigma)P_i^S(k) + \delta P_i^R(k) + \omega P_i^L(k) \\ P_i^I(k) = (1-\Delta(k))P_i^S(k) + (1-\mu-\theta-\sigma)P_i^I(k) + \nu P_i^R(k) + \omega P_i^L(k) \\ P_i^R(k) = \mu P_i^S(k) + \mu P_i^I(k) + (1-\delta-\nu-\sigma)P_i^R(k) + \omega P_i^L(k) + \eta P_i^D(k) \\ P_i^L(k) = \sigma P_i^S(k) + (\sigma+\theta-\omega)P_i^I(k) + (\sigma-\omega)P_i^R(k) - \lambda P_i^L(k) \\ P_i^D(k) = \lambda P_i^L(k) - \eta P_i^D(k). \end{cases} \tag{17}$$

By solving the system of equations from (17) and (16), state equations can be obtained. When a heterogeneous sensor node i is in state I, state L, or state D, it can be considered that the communication data sent by the node is unreliable or the node cannot send communication data, so both of these states are unavailable. Therefore, the steady-state availability of node i can be expressed as

$$D_i(k) = 1 - P_i^I(k) - P_i^L(k) - P_i^D(k). \tag{18}$$

VI. Numerical Simulation and Analysis

From (17) and (18), we can see that the steady-state availability of node i is related to a number of parameters, where the degree of node is only related to the node itself, μ and ν are related to IDS, and other parameters are related to the NBIOT-HWSN topological structure, deployment environment, and so on where the node is located.

VI.1. Effect of Distribution of the Degree of Node on Infection Probability of Nodes

When NBIOT-HWSNs belong to a scale-free network (SF network), a small number of nodes have a large number of connections, the degree of nodes is large, and a large number degrees of nodes are small, usually conforming to Zipf's law, where the degree of the node k obeys the power law distributionPr $(K=k) \sim k^{-\lambda}$, $k \in [k_{\min}, k_{\max}]$, where $k_{\min}$ is the minimum degree and $k_{\max}$ is the truncation of degree, and λ is an index describing the width of the distribution and meets $\lambda > 0$. In an actual network, the exponent λ is usually in the range of [2, 3]. Therefore, assuming the exponent $\lambda = 2, 2.5, 3$, minimum degree $k_{\min} = 1$, maximum degree $k_{\max} = 20$, and $<k>$ are about 4, the distribution of the degree of nodes for NBIOT-HWSNs can be obtained as shown in Table 1 and Figure 3.

Table 1: Distribution probability of the degree of node for NBIOT-HWSNs.

$P(k,\lambda)$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$	$k=9$	$k=10$	$k=11$	$k=12$	$\cdots$	$k=20$
$\lambda=2$	1.000	0.250	0.111	0.063	0.040	0.028	0.020	0.016	0.012	0.010	0.008	0.007	…	0.003
$\lambda=2.5$	1.000	0.177	0.064	0.031	0.018	0.011	0.008	0.006	0.004	0.003	0.002	0.002	…	0.001
$\lambda=3$	1.000	0.125	0.037	0.016	0.008	0.005	0.003	0.002	0.001	0.001	0.001	0.001	…	0.000

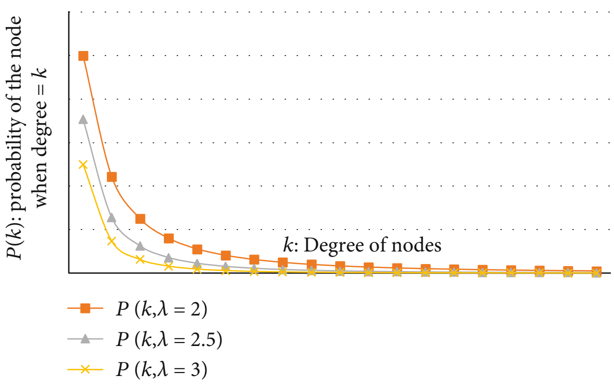

Figure 3: Distribution probability of the degree of node for NBIOT-HWSNs.

In the actual deployment of NB-IoT and WSN combination network, gateway nodes usually communicate with multiple nodes. Although the possibility of being attacked by malicious programs increases, these nodes often are deployed with more strict security measures, making the probability of being infected by malicious programs greatly reduced.

VI.2. Effect of Node Vulnerability Function on Node Infection Probability

Due to different security vulnerabilities and environments of NBIOT-HWSN nodes, the node vulnerability function may also be inconsistent. From the definition of the vulnerability function, the vulnerability function is a decreasing function, and $d(k) > 0$. In this experiment, four kinds of node vulnerability functions are considered: (1) $d(k)=1$, it means homogenous WSNs without difference between nodes; (2) $d(k)=1/k$, node vulnerability meets power function; (3) $d(k)=e^{-k/<k>}$, node vulnerability satisfies exponential function; (4) $d(k)=1-k/\max(k)$, the node vulnerability satisfies the linear function, where$\max(k)=40$. This experiment takes the average infection rate $\bar{\zeta}=0.2$ and adopts SF network. In the case of different vulnerability functions, the probability of node infection is shown in Table 2 and Figure 4. From Figure 4, we can see that when the node vulnerability meets the power function, the node infection rate is the most affected by the degree of node, followed by the exponential function, and then the linear function. When the degree of node is small, the infection rate of the node is not significantly different in the case of different vulnerability functions. For example, when $k=1$, the infection rates in the four cases were about 0.2, 0.2381, 0.2858, and 0.2023, respectively. When the degree of node is large, the infection rate of the nodes is quite different. For example, when $k=10$, the infection rates for the four cases were approximately 0.2, 0.0238, 0.0301, and 0.1556, respectively.

Table 2: Probability data of a node being successfully infected.

$\zeta_i(k)$	m	$k=1$	$k=5$	$k=10$	$k=15$	$k=20$
$d(k)=1$	1	0.2	0.2	0.2	0.2	0.2
$d(k)=1/k$	0.2381	0.2381	0.0476	0.0238	0.0159	0.0119
$d(k)=e^{-k/4}$	0.3670	0.2858	0.1051	0.0301	0.0086	0.0025
$d(k)=1-k/40$	0.2075	0.2023	0.1816	0.1556	0.1297	0.1038

VII. Discussion

For a heterogeneous sensor node in a NB-IoT and WSN combination network, the degree of the node mainly affects the availability of the equilibrium state in the following points:

(1) The degree of node determines the vulnerability of the node. The greater the degree of the node is, the stronger the node becomes, and the less vulnerable to infection by malicious programs

(2) The degree of the node determines the number of nodes it communicates with

(3) The greater the number of neighboring nodes that can communicate with it is, the larger the probability of contact with infected nodes, and therefore, the larger the probability of a node being infected by a malicious program is. These two aspects of influences have opposite effects of the node infection rate is opposite. Therefore, when the influence of (1) is greater than that of (2), the availability of nodes is positively correlated with the degree of nodes; otherwise, it is negatively correlated

(4) Simulation results show that when the degree of node is small and the node vulnerability function is a power function, the node availability is the highest; when the degree of node is large and the node vulnerability function satisfies the exponential function and the power function, the node availability is high. Therefore, when constructing a NBIOT-HWSN network, node protection is implemented according to the degree of node, so that when the node vulnerability function satisfies the power function, all nodes can maintain high availability, thus making the entire network more stable.

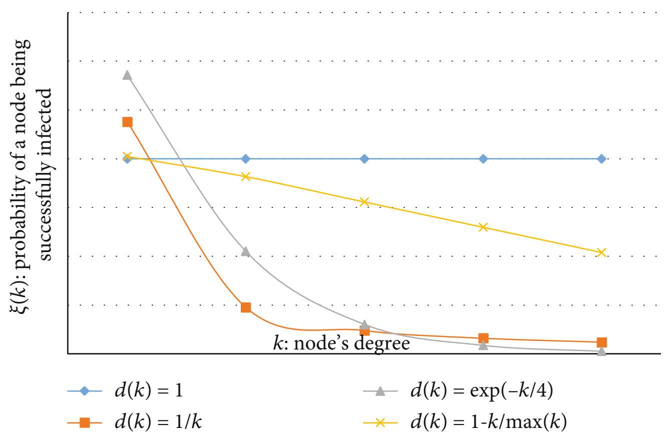

FIGURE 4: Probability of a node being successfully infected.

VIII. Conclusion

In this paper, based on node heterogeneity and the distribution of the degree of node, the influence of malicious program attack on NBIOT-HWSNs was analyzed, and node heterogeneity model SIRLD is established on the basis of model SIR and model SIRD. By referring to the epidemiological theory and Markov chain, the transition relations between the states of heterogeneous sensor nodes are described. The dynamic equations of node state transitions are given. Through the calculation, the calculation formula of node availability is obtained. The experimental results show the distribution of node infection rate under different degrees of nodes and different node vulnerability functions; it also finds out the effect of the degree of nodes under different degrees of vulnerability functions on the availability of nodes.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under grant No. 61772018. It is a part of my Ph.D. research in the field of WSNs. This work was advised by Professor Qiying Cao; MATLAB simulations are completed by Juan Jin and some other teammates. I express my hearty thanks for their help here.

References

(1) S. Oh and J. Shin, "An efficient small data transmission scheme in the 3GPP NB-IoT system," IEEE Communications Letters, vol. 21, no. 3, pp. 660–663, 2017.

(2) J. Sun, X. Zhang, and X. Dong, "Availability evaluation model for the heterogeneous system based on RBD," Journal of XIAN University, vol. 43, no. 3, pp. 190–196, 2016.

(3) C. Nie, X. Gao, and R. Dong, "Symbolic computation method of wireless sensor network reliability based on fault tree," Computer Engineering and Design, vol. 36, no. 6, pp. 1425–1431, 2015.

(4) V. Illiano and E. Lupu, "Detecting malicious data injections in wireless sensor networks: A survey," ACM Computing Surveys, vol. 48, no. 2, pp. 1–57, 2015.

(5) Q. Gu, C. Ferguson, and R. Noorani, "A study of self-propagating mal-packets in sensor networks: attacks and defenses," Computers & Security, vol. 30, no. 1, pp. 13–27, 2011.

(6) C. Wang, Y. Hu, C. Liu, Z. Liu, and J. Ma, "Stability analysis of information spreading on SNS based on refined SEIR model," China Communications, vol. 11, no. 11, pp. 24–33, 2014.

(7) W. Costa, L. Medeiros, and S. Sandri, "A fuzzy cellular automata for SIR compartmental models," Fuzzy Logic and Applications, vol. 8256, pp. 234–247, 2013.

(8) B. Qu and H. Wang, "SIS epidemic spreading with correlated heterogeneous infection rates," Physica A: Statistical Mechanics and its Applications, vol. 472, pp. 13–24, 2017.

(9) M. Essouifi and A. Achahbar, "A mixed SIR-SIS model to contain a virus spreading through networks with two degrees," International Journal of Modern Physics C, vol. 9, no. 28, 2017.

(10) B. K. Mishra and N. Keshri, "Model on the transmission of worms in wireless sensor network," Applied Mathematical Modelling, vol. 37, no. 6, pp. 4103–4111, 2013.

(11) S. Shen, L. Huang, E. Fan, K. Hu, J. Liu, and Q. Cao, "Survivability evaluation for WSNs under malware infection," Chinese Journal of Sensors and Actuators, vol. 29, no. 7, pp. 1083–1089, 2016.

(12) O. Kabadurmus and A. E. Smith, "Evaluating reliability/survivability of capacitated wireless networks," IEEE Transactions on Reliability, vol. 67, no. 1, pp. 26–40, 2018.

(13) M. Arslan, A. Joseph, and G. Ann, "Model on the transmission of worms in wireless sensor network,"

ACM Transactions on Embedded Computing Systems, vol. 14, no. 1, pp. 1539–9087, 2015.

(14) X. Zhang and R. Dong, "An OBDD-based method for availability evaluation of WSN," Journal of Guilin University of Electronic Technology, vol. 36, no. 3, pp. 210–214, 2016.

(15) J. Fan, J. Xie, Q. Tao, and Q. Fan, "Review on the cross -layer protocol of heterogeneous wireless sensor networks," Journal of Yunnan University (Natural Science), no. 4, pp. 235–244, 2011.

(16) V. Karyotis and S. Papavassiliou, "Macroscopic malware propagation dynamics for complex networks with churn," IEEE Communications Letters, vol. 19, no. 4, pp. 577–580, 2015.

(17) S. Shen, H. Ma, E. Fan et al., "A non-cooperative non-zero-sum game-based dependability assessment of heterogeneous WSNs with malware diffusion," Journal of Network and Computer Applications, vol. 91, pp. 26–35, 2017.

(18) M. Kasraoui, A. Cabani, and H. Chafouk, "Secure collaborative system in heterogenous wireless sensor networks," Journal of Applied Research and Technology, vol. 13, no. 2, pp. 342–350, 2015.

References

[1] X. Wu, Q. Cao, J. Jin, Y. Li, and H. Zhang, "Nodes availability analysis of NB-IoT based heterogeneous wireless sensor networks under malware infection," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 4392839, 9 pages, 2019.