Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 4392839, 9 pages
https://doi.org/10.1155/2019/4392839

Research Article

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 26 June 2018; Revised 31 October 2018; Accepted 11 December 2018; Published 3 January 2019

Academic Editor: Juan F. Valenzuela-Valdés

The Narrowband Internet of Things (NB-IoT) is a main stream technology based on mobile communication system. The combination of NB-IoT and WSNs can active the application of WSNs. In order to evaluate the influence of node heterogeneity on malware propagation in NB-IoT based Heterogeneous Wireless Sensor Networks, we propose a node heterogeneity model based on node distribution and vulnerability differences, which can be used to analyze the availability of nodes. We then establish the node state transition model by epidemic theory and Markov chain. Further, we obtain the dynamic equations of the transition between nodes and the calculation formula of node availability. The simulation result is 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-HWSNs 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.

1. Introduction

The development of a new generation of mobile 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 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 WSN, 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 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 is, the greater the probability of being infected by a malicious program is, and the greater the probability of being infected is. After extensive application of NB-IoT to WSNs, the logical distance between node and application network is quite different. The nodes in the hybrid network have heterogeneity. They have different degrees of node and vulnerability and constitute a Heterogeneous Wireless Sensor Networks [2] (HWSNs); here I define it as NBIOT-HWSNs.

The availability of WSNs node represents 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-HWSNs 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 was given and the effects of the degree of node on the availability of nodes are studied. Firstly, by observing the relationship between the degree of node and the antiattack ability of the node in the actual network, a heterogeneity model of the sensor node based on the difference in the degree of node was given, and the infection rate function is defined. Then, based on the classical epidemic model, a SIRD state transition model was established. Based on the Markov chain, the dynamic equation of the transition between states of the heterogeneous sensor nodes was given. Finally, the formula for calculating the availability of heterogeneous nodes is given when the NBIOT-HWSN reach the dynamic equilibrium state.

2. 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.

Researches [4, 5] showed that WSNs are vulnerable by attacks, and malware can spread from nodes to nodes in WSNs. Like ILLIANO V.P, LUPU E.C [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 of 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. Q. Gu, F. Christopher, and N. Rizwan [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 and can exploit memory-related vulnerabilities and utilize existing application code in a sensor to propagate itself.

Researches [6–10] studied different kinds of malicious program propagation models; these models are from: Epidemic Dynamics Theory, Cellular Automaton Theory, Queuing Theory, etc. The following are some impressive research models. C. WANG et al. [6] investigated the stability of information spreading over SNS, discovered the principles inherent in the spreading behavior, and the defined a SEIR- (Susceptible-Exposed-Infectious-Removed-) based model for the information spreading over SNS. W. 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. B. Qu et al. [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. M. Essouifi et al. [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. B. Mishra et al. [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 WSNs reliability evaluation methods are used in published articles [11–14]. S. 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 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, O. Kabadurmus et al. [12] proposed a new indicator that combines network reliability and network resiliency to assess network reliability. M. Arslan et al. [13] established the Markov model for effective data detection and fault tolerance of wireless sensor network nodes and conducted simulation analysis. X. Zhang et al. [14] created an OBDD-based method for availability evaluation of WSN.

With the development of heterogeneous WSNs, some latest researches [15–18] show their characters and new development. J. 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. V. 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. S. Shen [17] considered Heterogeneous Wireless Sensor Networks (HWSNs) with malware diffusion and find a solution to assess their dependability in order to guarantee dependable operations on sending sensed data from sensor nodes (SNs) to a sink node. M. Kasraoui [18] focused on the IPv6 over Low

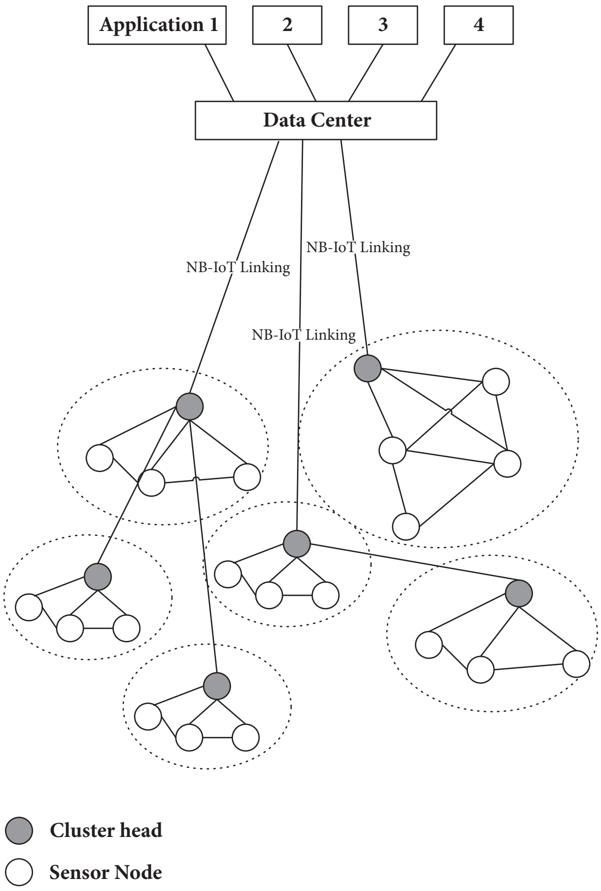


Figure 1: Schematic diagram of NBIOT-HWSNs.

power Wireless Personal Area Networks (6LoWPANs) which interconnects the Heterogeneous Wireless Sensor Networks (HWSNs) with Internet. They also proposed a novel Cooperative Key Exchange System (CKES) by using the concept of Chinese Remainder Theorem (CRT).

3. 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 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 and long life cycle, and strong penetration capabilities of NB-IoT. Figure 1 shows a typical NBIOT-HWSNs 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-HWSNs, 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 node's resistance to malicious program's attack; 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 c is the normalization constant.

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

Assume that the degree of node in the NBIOT-HWSNs obeys the distribution $\Pr(K = k)$, 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:

$$\overline{\zeta} = \frac{1}{N}\sum_{i\in N}\zeta_i(k) = c\sum_{k}\zeta_i(k)P(k) = c\langle d(k)\rangle \tag{2}$$

Therefore, the value of constant c is $c = \overline{\zeta}/\langle d(k)\rangle$ and being substituted into formula (1), it can be obtained:

$$\zeta_i(k) = \frac{\overline{\zeta} d(k)}{\langle d(k)\rangle} \tag{3}$$

in which $\langle d(k)\rangle$ is the mean value of the integral of $d(k)$, which is determined by the distribution function of the degree of node. $\overline{\zeta}$ 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

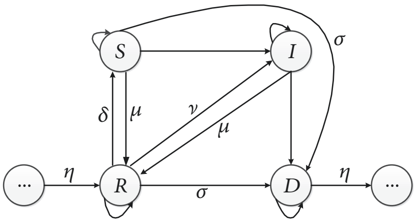


Figure 2: Node state transition diagram of NBIOT-HWSNs.

probability of each node is the same, which are all $\overline{\zeta}$. When the structure of NBIOT-HWSNs is ready, $\langle d(k) \rangle$ and $\overline{\zeta}$ are all constants.

4. 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 SIRD model in the classical epidemiological theory to describe the state changes of nodes in the process of infection of NBIOT-HWSNs malicious programs. Among them, the states of the sensor node are divided into susceptible state, infected state, recovered state, and dead state. Susceptible state refers to a state in which a NBIOT-HWSNs node has a 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 is 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. 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. $p_i^S(t)$, $p_i^I(t)$, $p_i^R(t)$, $p_i^D(t)$ are defined as the probabilities of node i at times of S, I, R, D, and $q_i^{xy}(t)$ represents the probability that the node transitions from the state x to the state y, in which $x, y \in \{S, I, R, D\}$. 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. $p_i^R(0) = 1$, $p_i^S(0) = p_i^I(0) = p_i^D(0)$.

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 andν, 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 D, and the probability of dead node 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 D. Therefore, the probability of a state transition for node i that is in state S at time of t can be expressed as

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

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 D. Therefore, the probability of the state transition for a node i that is in state S at time t can be expressed as

$$\begin{aligned} q_i^{IS}(t) &= 0 \\ q_i^{II}(t) &= 1 - \mu - \theta - \sigma \end{aligned}$$

$$\begin{aligned} q_i^{IR}(t) &= \mu \\ q_i^{ID}(t) &= \sigma + \theta \end{aligned} \tag{5}$$

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 a node i that is in state R at time t can be expressed as

$$\begin{aligned} q_i^{RS}(t) &= \delta \\ q_i^{RI}(t) &= \nu \\ q_i^{RR}(t) &= 1 - \delta - \nu - \sigma \\ q_i^{RD}(t) &= \sigma \end{aligned} \tag{6}$$

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; 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

$$\begin{aligned} q_i^{DS}(t) &= 0 \\ q_i^{DI}(t) &= 0 \\ q_i^{DR}(t) &= \eta \\ q_i^{DD}(t) &= 1 - \eta \end{aligned} \tag{7}$$

From Figure 2, we can see that the nodes in the two states of S and R at time t-1 may be converted into state S at time t, the nodes in the three states of S, I, and R may be converted to state I at time t, the nodes in the four states of S, I, R and D may be converted to state R at time t, and the nodes in the four states of S, I, R, and D may be converted to state D at time t. Therefore, the probability of node i in each state of at time t can be expressed as

$$\begin{aligned} p_i^S(t) &= \left(q_i^{SS}(t) - q_i^{SI}(t) - q_i^{SR}(t) - q_i^{SD}(t)\right) p_i^S(t-1) \\ &\quad + q_i^{RS}(t)\, p_i^R(t-1) \\ p_i^I(t) &= \left(q_i^{II}(t) - q_i^{IR}(t) - q_i^{ID}(t)\right) p_i^I(t-1) \\ &\quad + q_i^{SI}(t)\, p_i^S(t-1) + q_i^{RI}(t)\, p_i^R(t-1) \\ p_i^R(t) &= \left(q_i^{RR}(t) - q_i^{RI}(t) - q_i^{RS}(t) - q_i^{RD}(t)\right) p_i^R(t-1) \\ &\quad + q_i^{IR}(t)\, p_i^I(t-1) + q_i^{SR}(t)\, p_i^S(t-1) \\ &\quad + q_i^{DR}(t)\, p_i^D(t-1) \\ p_i^D(t) &= \left(q_i^{DD}(t) - q_i^{DR}(t)\right) p_i^D(t-1) + q_i^{ID}(t)\, p_i^I(t-1) \\ &\quad + q_i^{RD}(t)\, p_i^R(t-1) + q_i^{SD}(t)\, p_i^S(t-1) \end{aligned} \tag{8}$$

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

5. Node Availability Analysis of NBIOT-HWSN

According to reliability theory, the reliability of an NBIOT-HWSNs node i at time t is called instantaneous availability, recorded as $\tau_i(k,t)$. After NBIOT-HWSNs runs 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 $\widetilde{\tau_i(k)}$), so the node steady-state availability can be expressed as

$$\widetilde{\tau_i(k)} = \lim_{t \longrightarrow \infty} \tau_i(k,t) \tag{9}$$

The probabilities of heterogeneous sensing node i in each state when it reaches a stable state are defined as $\chi_S(k), \chi_I(k), \chi_R(k), \chi_D(k)$; the following can be obtained:

$$\chi_S(k) + \chi_I(k) + \chi_R(k) + \chi_D(k) = 1 \tag{10}$$

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

$$\begin{aligned} \chi_i^S(k) &= \left(\Delta(k) - \mu - \sigma\right)\chi_i^S(k) + \delta\chi_i^R(k) \\ \chi_i^I(k) &= \left(1 - \Delta(k)\right)\chi_i^S(k) + \left(1 - \mu - \theta - \sigma\right)\chi_i^I(k) \\ &\quad + \nu\chi_i^R(k) \\ \chi_i^R(k) &= \mu\chi_i^S(k) + \mu\chi_i^I(k) + \left(1 - \delta - \nu - \sigma\right)\chi_i^R(k) \\ &\quad + \eta\chi_i^D(k) \\ \chi_i^D(k) &= \sigma\chi_i^S(k) + \left(\sigma + \theta\right)\chi_i^I(k) + \sigma\chi_i^R(k) \\ &\quad + \left(1 - \eta\right)\chi_i^D(k) \end{aligned} \tag{11}$$

By solving the system of equations from (10) and (11), states equation can be obtained. When a heterogeneous sensing node i is in state I 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

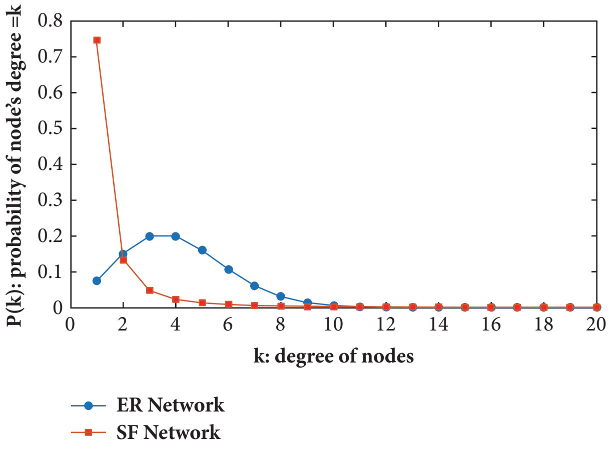


Figure 3: Distribution probability of the degree of node for NBIOT-HWSNs belonging to ER network and SF network, respectively.

states are unavailable. Therefore, the steady-state availability of node i can be expressed as

$$\widetilde{\tau_i(k)} = 1 - \chi_i^I(k) - \chi_i^D(k) \tag{12}$$

6. Numerical Simulation and Analysis

From (10) and (11) we can see that the steady-state availability of node i is related to a number of parameters, where the degree of node k is only related to the node itself, μ and ν are related to IDS, and other parameters are related to the NBIOT-HWSNs topological structure, deployment environment, and so on where the node is located.

6.1. Effect of Distribution of the Degree of Node on Infection Probability of Nodes. When NBIOT-HWSNs belong to the traditional stochastic network (ER network), the connections between nodes are set randomly, and most nodes have the same degree of nodes, where the degree of node k obeys the binomial distribution $\Pr(K = k) = C_n^k p^k (1-p)^{N-k}$. When the value of N is large enough, it can be regarded as obeying the Poisson distribution $\Pr(K = k) = e^{-E[K]}E(K)^k/k!$, and when taking the number of heterogeneous nodes $N = 10^4$ in the NBIOT-HWSNs and the average degree $E(K) = 4$, the probability distribution of the degree of nodes can be obtained as shown in Figure 3.

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 distribution $\Pr(K = k) \sim k^{-\lambda}$, $k \in [k_{\min}, k_{\max}]$, where $k_{\min}$ is the minimum degree, $k_{\max}$ 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 $\lambda = 2.5$, minimum degree $k_{\min} = 1$, maximum degree $k_{\max} = 50$, and $\langle k \rangle$ are about 4, the distribution of the degree of nodes for NBIOT-HWSNs can be obtained as shown in Figure 3.

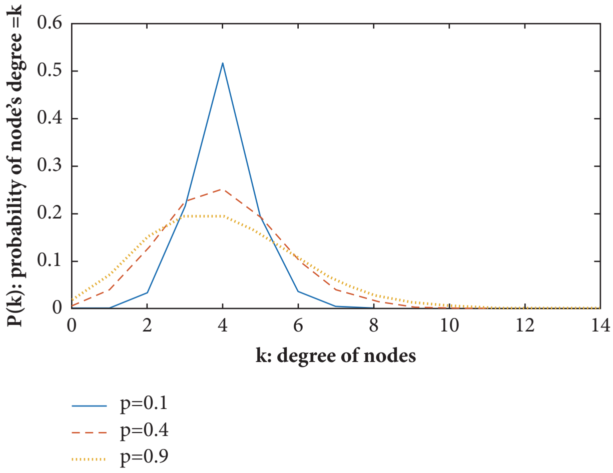


Figure 4: Distribution probability of the degree of nodes for different degree of reconnection probability when NBIOT-HWSNs belong to WS network.

Table 1: Effect data of node distribution on node infection rate.

	k=1	k=5	k=10	k=30	k=50
Random Network	0.607	0.123	0.085	0.023	0.010
Scale free Network	0.238	0.045	0.034	0.012	0.006

When NBIOT-HWSNs belong to a small-world network (WS network), the nodes use the reconnection probability p to reconnect each edge on the basis of the connection of the regular network, so that the network maintains the clustering of the regular network and greatly reduces the average path length in the regular network. The distribution of the degree of nodes k is related to the probability of reconnection p. When p=1, all nodes in the network are connected randomly, that is, random networks. When $N = 10^4$ and $\langle k \rangle$ is 4, the connection between nodes in the small-world network is simulated, the distribution probability of the degree of node for NBIOT-HWSNs under different reconnection probability as shown in Figure 4.

In the actual deployment of NBIOT-HWSNs, 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. This experiment takes the node vulnerability functions $d(k) = 1/k$, $\overline{\zeta} = 0.2$, and the influence of different network distributions on the node infection rate is shown in Table 1 and Figure 5. When the average infection rate of the entire NBIOT-HWSNs is the same, for nodes with the same degree, the probability of a node in a scale-free network being successfully infected is generally smaller than that of a random network, especially for a node with a smaller degree of node. For example, in an ER network, a node with a degree of 1 has an infection rate of about 0.606748, and in an SF network it is only about 0.238124.

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

	k=5	k=10	k=20	k=30	k=50
d(k)=1	0.2	0.2	0.2	0.2	0.2
d(k)=1/k	0.0495	0.0238	0.0231	0.015	0.011
$d(k) = e^{-k/\langle k\rangle}$	0.0610	0.0286	0.0275	0.018	0.012
$d(k) = 1 - k/\max(k)$	0.185	0.166	0.125	0.075	0

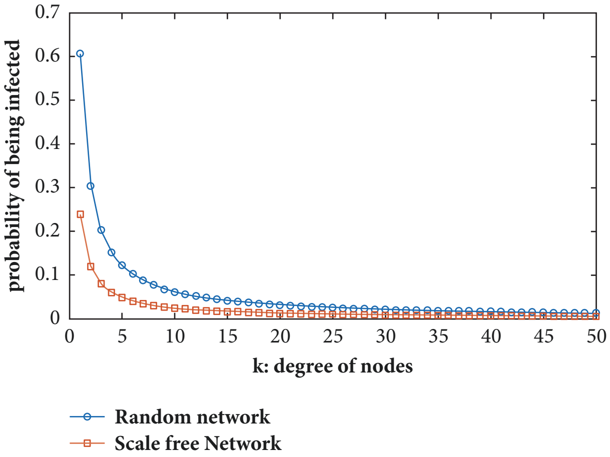


Figure 5: Effect of node distribution on node infection rate.

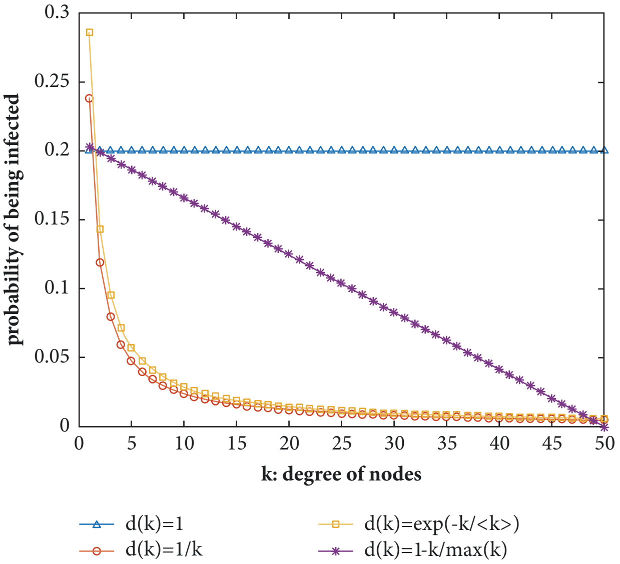


Figure 6: Probability of a node being successfully infected.

6.2. Effect of Node Vulnerability Function on Node Infection Probability. Due to different security vulnerabilities and environments of NBIOT-HWSNs 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) $d(k) = e^{-k/\langle k\rangle}$, node vulnerability satisfies exponential function; (4) $d(k) = 1 - k/\max(k)$, the node vulnerability satisfies the linear function, where $\max(k) = 50$. This experiment takes the average infection rate $\overline{\zeta} = 0.2$ and adopts SF network. In the case of different vulnerability functions, the probability of node infection is shown in Table 2 and Figure 6. From Figure 6, 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 0.2033, 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, 0.0286, and 0.166, respectively.

6.3. Influence of the Degree of Nodes of Heterogeneous Sensor on Its Availability. For a heterogeneous sensing node i, the degree of the node mainly affects the availability of the equilibrium state in two aspects:

(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 is;

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

The greater the number of neighboring nodes that can communicate with it is, the larger the probability of contact with infected nodes is, and therefore, the larger the probability of a node being infected by a malicious program is. These two aspects of influences have opposite effect of the node infection rate. 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. Table 3 and Figure 7 show the relationship between the degree of node and node availability in the case of the four vulnerability functions proposed in VI(B). Experimental 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

Table 3: Nodes' availability data of NBIOT-HWSNs.

	k=5	k=10	k=20	k=30	k=50
d(k)=1	0.397	0.388	0.372	0.356	0.33
d(k)=1/k	0.403	0.403	0.403	0.403	0.403
$d(k) = e^{-k/\langle k\rangle}$	0.395	0.399	0.405	0.406	0.406
$d(k) = 1 - k/\max(k)$	0.398	0.391	0.384	0.384	0.406

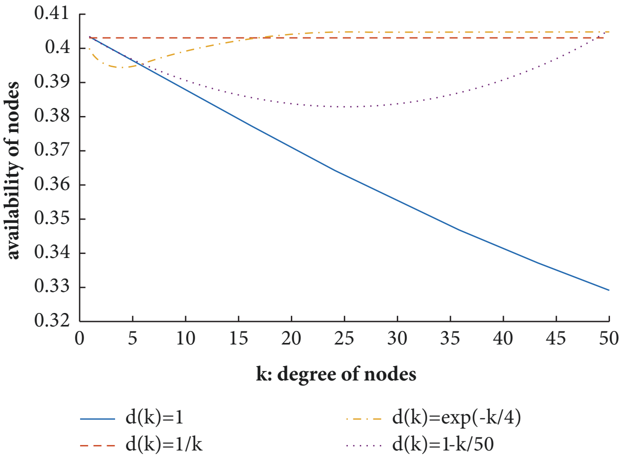


Figure 7: Nodes' availability of NBIOT-HWSNs.

the exponential function and the power function, the node availability is high. Therefore, when constructing a NBIOT-HWSNs 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.

7. 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 is established. 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 degree of vulnerability functions on the availability of nodes.

Data Availability

The authors declare that the data and experiments in this paper are available.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is a part of my Ph.D. research in the field of WSNs. This work was advised by Professor Qiyingcao; Matlab simulations are completed by Juanjin 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.

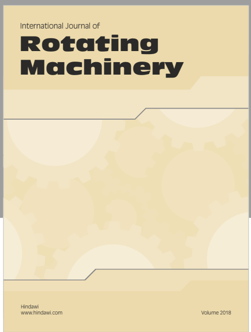
[16] V. Karyotis and S. Papavassiliou, “Macroscopic malware propagation dynamics for complex networks with churn,” *IEEE Communications Letters*, vol. 19, no. 4, pp. 577–580, 2015.

[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.

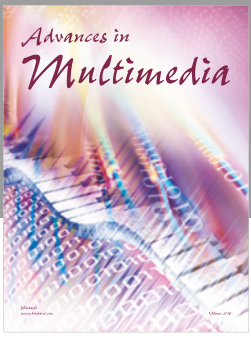
[18] M. Kasraoui, A. Cabani, and H. Chafouk, “Secure collaborative system in heterogenous wireless sensor networks,” *Journal of Applied Research and Technology*, vol. 13, no. 2, pp. 342–350, 2015.

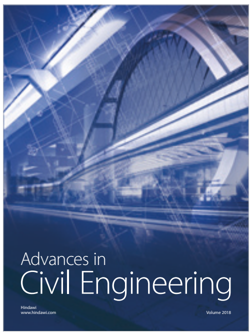
Journal of
Engineering

The Scientific World Journal

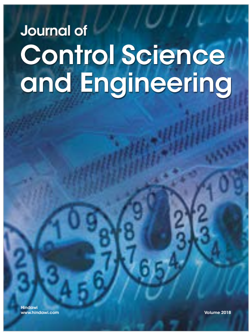

International Journal of
Rotating Machinery

Journal of
Sensors

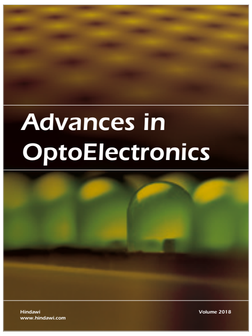

Advances in
Multimedia


Advances in
Civil Engineering

Journal of
Robotics

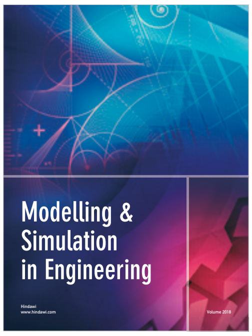

Journal of
Control Science and Engineering

Journal of
Electrical and Computer Engineering

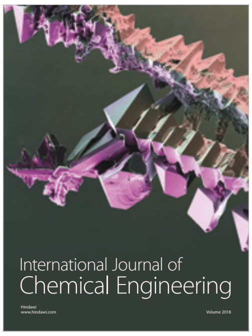

Advances in
OptoElectronics

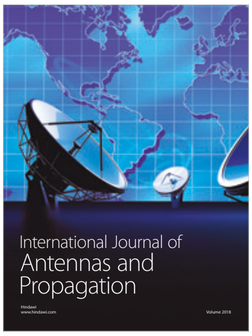
VLSI Design

International Journal of
Navigation and Observation

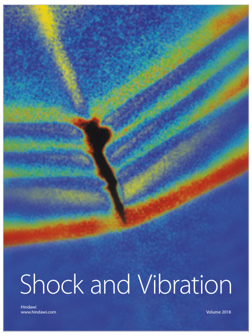

Modelling & Simulation in Engineering

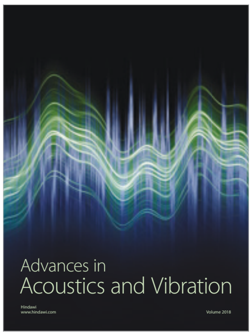
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration