Hindawi
Security and Communication Networks
Volume 2020, Article ID 6513920, 11 pages
https://doi.org/10.1155/2020/6513920

Research Article

Virus Propagation in Wireless Sensor Networks with Media Access Control Mechanism

Lurong Jiang, Qiaoyu Xu, Hangyi Pan, Yanyun Dai, and Jijun Tong

School of Information Science and Technology, Zhejiang Sci-Tech University, Hangzhou 310018, China

Correspondence should be addressed to Jijun Tong; jijuntong@zstu.edu.cn

Received 10 February 2020; Revised 20 September 2020; Accepted 24 October 2020; Published 21 November 2020

Academic Editor: Cristina Alcaraz

In wireless sensor networks, network security against virus propagation is one of the challenges with the applications. In severe cases, the network system may become paralyzed. In order to study the process of virus propagation in wireless sensor networks with the media access control mechanism, this paper uses the susceptible-infectious-removed (SIR) model to analyze the spreading process. It provides a theoretical basis for the development of virus immune mechanisms to solve network virus attack hidden dangers. The research shows that the media access control (MAC) mechanism in the wireless sensor network can inhibit the process of virus propagation, reduce the network virus propagating speed, and decrease the scale of infected nodes. The listen/sleep duty cycle of this mechanism will affect the suppression effect of virus propagation. The smaller the listen/sleep duty cycle, the stronger the suppression effect. Energy consumption has a peak value under specific infection probability. Meanwhile, it is also found that the spreading scale of the virus in wireless sensor networks can be effectively inhibited by the MAC mechanism.

1. Introduction

Viruses and cyber-attacks frequently exposed to computer networks have caused significant losses to human society. A network virus refers to a group of computer instructions or programs that can damage data or destroy device functions and spread through computer networks such as the Internet or wireless communication networks [1]. Different from the so-called viruses in biology, a network virus is created artificially and implanted malignantly but does not occur naturally. A network virus can self-replicate and self-transmit without human intervention, can trigger and lurk, and at the same time can have strong destructive ability and great harm [2]. For example, the worm known as the "beauty killer" once caused a world-renowned Internet paralysis event [3]. The Chernobyl virus (also known as CIH or Spacefiller) damages the essential input and output system of the computer by infecting the executable file of the system, making the machine unable to start usually [4]. Wireless sensor networks, which are composed of a large number of low power consumption sensor nodes through wireless communication technology, are a kind of computer networks [5] and are also threatened by network virus. Some researchers have found that the topology of wireless sensor networks is relatively complex and vulnerable to virus attack [6], because wireless sensor networks are constrained by space, energy, channel bandwidth, and other conditions [7]. Furthermore, the resources and power of the nodes in the wireless sensor networks are limited. Once a large number of nodes are infected, it is easy to become invalid due to the exhaustion of resources or energy. The failure of a large number of nodes will increase the average path length of the network, reduce network performance, lead to disconnection of this network, and stop the service of the system. Therefore, the threat of the viruses in the wireless sensor networks is more vulnerable than the traditional wired networks [8, 9].

However, in essence, wireless sensor network virus propagation is similar to traditional virus propagation in other computer networks. Some studies have found that worms, malignant virus, and other viruses can use the vulnerability of the communication protocol or mechanism loopholes to expand communication by web pages, emails, Bluetooth, WIFI, etc. [10]. Besides, some studies have found

that the virus can intensify the transmission process in mobile networks by the dynamic movement of devices [11]. There are many existing pieces of research on the dynamic process of virus propagation in wireless sensor networks. But because the wireless access layer of wireless sensor networks (WSNs) has a relatively new view on the influence of virus propagation, there are few relevant studies and few references on the impact of wireless access layer in the relevant literature. So, it is necessary to do further research on this subject.

In this paper, we intend to study the virus propagation process in the wireless sensor networks by using the susceptible-infectious-removed (SIR) propagation model. We mainly consider the influence of the media access control (MAC) mechanism on virus propagation in wireless sensor networks with uniform random distribution and limited communication capacity. A random network topology model with a limited communication range is established based on the Waxman algorithm, and the SIR virus propagation model is developed on this basis. We considered the effect of the MAC mechanism on the virus infection process in wireless sensor networks. The research results reveal the pattern of virus propagation in wireless sensor networks, which can provide a basis for improving the security of wireless sensor networks.

The rest of this paper is structured as follows: Section 2 introduces the current research on virus propagation in wireless sensor networks and the basic principle of the influence of MAC mechanism on virus propagation in wireless sensor networks. Section 3 proposes an improved SIR model. Section 4 conducts this improved SIR simulation. Section 5 analyzes the experimental results. Section 6 makes a conclusion and outlook.

2. Related Work

With the continuous expansion of wireless sensor networks in the fields of industry, agriculture, military, etc., the importance of security issues has become increasingly prominent, among which the wireless sensor network virus attack has attracted much attention. Many researchers have participated in the study of virus propagation in wireless sensor networks. In the research process, some researchers will consider the network application scenarios or the environment. Some researchers will consider network constraints, such as communication range, node energy, etc. Some researchers have also enhanced the security and robustness of the network by establishing devices and data trust system in networks [12, 13] and proposed trust evaluation mechanisms [14]. Some researchers will pay attention to the applicable model of virus propagation in wireless sensor networks, such as the susceptible-infectious (SI) model, SIR model, etc.

The SIR model is one of these typical virus propagation models. Due to the moderate complexity of the SIR model, it can better characterize the dynamical state of nodes in virus propagation, so it has a specific model reference value. Besides, there are many versions of improved SIR models in wireless networks, which are modified or extended based on the SIR model. Hu et al. [15] analyzed the dynamic propagation characteristics of wireless sensor networks with regional detection mechanisms using a two-dimensional cellular automata-based SIR model. They found that the regional detection mechanism can not only regionalize the wireless sensor network but also prevent the malware propagation in the wireless sensor network by implementing the detection strategy. The regional detection mechanism can reduce the risk of virus outbreaks. Tang et al. [16] used the susceptibility-infection-recovery-maintenance (SIR-M) model to describe the dynamic process of the malicious viruses spreading from a single node to the entire network in WSN. Zhou et al. [17] modified the traditional SIR model according to low energy adaptive clustering hierarchy (LEACH) protocol communication rules, formed a new SIR model, and used it to describe the virus propagation dynamics in IPv6 wireless sensor networks. Feng et al. [18] used a SIRS model as considering the communication radius and node distribution density to capture the space-time dynamics of the worm propagation process. Wang et al. [19] analyzed the propagating dynamics of worms in wireless sensor networks by introducing the death node state and susceptible-infectious-removed-susceptible (SIRS) mechanism that cannot normally work due to energy depletion based on the traditional SIR model. Srivastava et al. [20] used the susceptibility-infection-dead-recovery (SIDR) propagation model that introduced the concept of death node to discuss the propagating dynamics of digital worms in wireless sensor networks with limited node energy. Singh et al. [21] introduced exposure state and inoculation state based on the SIR model to study the transmission behavior of a digital worm virus. By considering the sleep mechanism of WSN, Upadhyay et al. [22] developed an e-epidemic energy-efficient susceptible-infected-terminally infected-recovered (SITR) model to study and analyze worm attack behavior in wireless sensor networks using cyrtoid-type functional response. They obtain the stability and directionality of the Hopf bifurcation of the local equilibrium point by using the central accessible theorem analysis.

As far as we know, the original model and improved version of SIR are applicable to not only WSN networks, but also other complex networks, and the scope of application is quite extensive. For example, Xiang et al. [23] used SIR model to simulate emotion contagion in dynamic crowd aggregation process, and they found that the SIR model can effectively improve the fidelity of emotional interaction processes and crowd aggregation. Lamb et al. [24] described the SIR stochastic epidemic model of computer virus by combining the time-Markov chain of the minimum traffic model and the control of virus propagation. They applied the model to the scale-free networks to determine how the free flow and traffic flow in the crowded phase affect virus propagation. Androulidakis et al. [25] used the susceptible-exposed-infectious-removed (SEIR) model to simulate the infection of malware in the Private Branch eXchanges (PBX) network and monitor their development. And the results show that two days are sufficient for the malware diffusion. No matter which researchers use virus propagation model, this model is selected according to the principle of optimal

and most suitable, which can adequately reflect the characteristics of virus propagation in a specific wireless sensor network structure.

In the existing studies on virus propagation in wireless sensor networks, most researches concern the influence of network structure or node state changes on virus propagation. Some other researchers will also pay attention to the impact of the MAC, and they will add MAC mechanisms to the study on virus propagation in wireless sensor networks. MAC mechanism, also known as the media access mechanism, is applied to the data link layer. In wireless sensor networks, it is mainly used to solve network channel disputes and allocate channel access, and wireless communication resources [26]. However, in wireless sensor networks, viruses generally function in the application layer, so virus propagation is restricted by the MAC layer, the same as other standard data transmissions [27]. Li et al. [28] pointed out that MAC protocol is a very complicated protocol, which can control the entry channel of nodes and influence the number of infected nodes at the time of t to influence the spread of network virus. Wang et al. [29] showed that the channel monitoring of the MAC mechanism can limit the communication between nodes and inhibit the propagation of network virus by reducing the density of network infected nodes. Research shows that the smaller the duty cycle of sleep/listening, the better the suppression effect of network virus propagation. Also, the network structure will affect virus propagation. For example, the network node distribution strategy with local clustering features will increase the virus propagation speed. From the current research status, few studies consider the influence of the MAC mechanism in the study of wireless sensor network virus propagation. However, the MAC mechanism is often used in wireless sensor network communication and has a far-reaching influence on network virus propagation. Therefore, it is necessary to consider the MAC mechanism in the study of wireless sensor network virus propagation.

In this paper, wireless sensor networks with uniform and random distribution of network nodes are established by using the Waxman model. It is assumed that the sensor nodes in the network have a limited communication radius, and an improved version of the SIR model is used to study the propagation of viruses in these networks. At the same time, we use the MAC mechanism to avoid channel disputes in wireless sensor networks in the process of virus propagation. In the wireless sensor network, the MAC mechanism can reasonably allocate the right to use the channel, reducing and avoiding channel collision and channel interference. Meanwhile, the role of the MAC mechanism will also have an impact on the network virus propagation process, which increases the difficulty and complexity of virus propagation research to some extent. Energy consumption in the process of virus propagation is also analyzed in this paper.

3. Virus Propagation Model for Wireless Sensor Networks with MAC Mechanism

In this part, according to the Waxman algorithm and the Warshall algorithm, we build a wireless sensor network topology model with a limited communication range of nodes. On this basis, we develop an SIR virus propagation model. Because WSNs have a wireless access layer, we consider the influence of the MAC mechanism in every step of virus propagation from infected nodes to neighboring nodes.

3.1. Wireless Sensor Network Structure Model. Wireless sensor networks are generated on the Waxman algorithm [30] in our study, which is a typical random network topology generation algorithm. Considering the limited communication capacity of sensor nodes, when setting up the network environment, the probability of the existence of links between two nodes within the communication radius R_c is P_e, as in

$$P_e(u,v) = \begin{cases} 0, & l(u,v) > R_c, \\ \beta \exp\left(\dfrac{-l(u,v)}{L\alpha}\right), & 0 \le l(u,v) \le R_c, \end{cases} \quad (1)$$

where the parameters of equation (1) are shown in Table 1.

The network topology is generated by adding relationships between all pairs of nodes in the network with probability P_e. However, since the Waxman algorithm cannot guarantee the network connectivity, the Warshall algorithm [31] is needed to verify the connectivity of network.

3.2. SIR Virus Propagation Model with MAC Mechanism. The SIR propagation model is used to study the dynamics of virus propagation in wireless sensor networks under the MAC mechanism. The interaction between data transmission and virus propagation in wireless sensor networks is also considered in this model. It is assumed that N nodes are uniformly and randomly distributed in the wireless sensor network, each node has a limited communication radius R_c, and at each moment, n nodes in the wireless sensor network have data sending requests, and these n nodes are called active nodes. According to the SIR model, each node in the wireless sensor network has three different states; namely, the susceptible state (S-state) node can be infected easily by viruses, the infectious state (I-state) node can infect S-state node, and the removed state (R-state) node is invalid after virus infection. In these three states, only the node in the R-state could not work correctly; that is, it could not send data or transmit the viruses. At time t, the number of S-state, I-state, and R-state nodes are denoted as $S(t)$, $I(t)$, and $R(t)$, respectively, and $N = S(t) + I(t) + R(t)$ at each time step t. At the beginning moment of virus propagation, an arbitrary node is set as the infected node and begins to transmit the viruses outwards.

In wireless sensor networks, virus propagation between nodes or other conventional data transmission is constrained by the MAC mechanism. With the MAC mechanism, a node needs to listen to the channel before data transmission or virus propagation. It is only allowed to transmit data or virus outward when the channel is idle. Two

Table 1: Applications in each class.

Symbol	Description
$l(u, v)$	The distance between any node u and node v
R_c	Communication radius of nodes
L	Maximum distance between pairs of nodes
β	Adjustment parameter of the average node degree
α	Adjustment parameter of the ratio of long and short links

dynamic processes of data transmission and virus propagation are performed simultaneously in wireless sensor networks. To describe the problem more clearly and concisely, we regard the listen/sleep mechanism in the MAC mechanism of sensor networks as periodic and discretize time [32–34]. The specific process is as follows: during the monitoring (listening) period of each unit time t, the active node publishes a data reception request in the broadcast form to all working nodes in the R_c communication range. To meet the requirements of the MAC mechanism, the monitor channel is idle. And the data sent by the active node is received by an idle node. An active node cannot send data to its neighbor node if this neighbor is busy. Then, this active node needs to wait unit time to re-enable channel monitoring. After the monitoring period ends, the working nodes in the network will enter the dormant period, while the nodes in the dormant period cannot work. However, since the active node issues the receiving request in a broadcast form, the information-receiving channels of all nodes (except the data receiving node) within the communication range are overwhelmed and interfered by the receiving request of the active node, and the active node can no longer receive communication requests from other nodes except the active node. Such a node with limited receiving function is called an interfered node, and the viruses cannot infect it.

Assume the active node to send very little data that is a virus. After the active node sends the virus data, each I node infects the S node whose normal operation and the channel is idle in the communication range R_c with the infection probability λ. And at each unit time step t, each I-state node turns to an R-state node that cannot normally work with probability γ. Without loss of generality, let $\gamma = 1$ [35].

3.3. Model Theory Analysis. It is assumed that N nodes are uniformly and randomly distributed in the 2-dimensional square area X^2 of the wireless sensor network with length X. Initially, most of the nodes are S-state nodes, and very few nodes are I-state nodes. The average node degree adjustment parameter in the network is β, and the proportion of active nodes that need to send data is δ, where $\delta = (N_a/N)$, where N_a is the number of active nodes, and the size of the area where the signal is disturbed is $(Na\pi R_c^2/X^2)$. In a unit time, an arbitrary node v of an I-state infects a normal working S-state node in the idle state within the communication radius R_c of the node v with probability λ. Then, the node v is transformed into the R-state node with a probability of $\gamma = 1$. The listen/sleep duty cycle of the MAC mechanism is τ. Based on the above description, we propose a relatively reasonable and applicable virus propagation model. This model is as follows:

$$\frac{dS(t)}{dt} = -\lambda\tau\varphi(1-\delta)\left(1 - Na\frac{\pi R_c^2}{X^2}\right)\beta\frac{\pi R_c^2}{X^2}S(t)I(t), \tag{2}$$

$$\frac{dI(t)}{dt} = \lambda\tau\varphi(1-\delta)\left(1 - Na\frac{\pi R_c^2}{X^2}\right)\beta\frac{\pi R_c^2}{X^2}S(t)I(t) - \gamma I(t), \tag{3}$$

$$\frac{dR(t)}{dt} = \gamma I(t). \tag{4}$$

And at each time step t, $S(t)$, $I(t)$, and $R(t)$ satisfy the following equation:

$$S(t) + I(t) + R(t) = N. \tag{5}$$

Let $A = \tau\varphi(1-\delta)(1 - Na(\pi R_c^2/X^2))\beta(\pi R_c^2/X^2)$, $\rho = (\gamma/\lambda)$, and φ is the inhibitor of virus propagation, that is, the inhibition of viral transmission by the number of active nodes. Since the proportion of active nodes in the network will affect the inhibitory effect of the MAC mechanism, the more active nodes there are, the more obvious the inhibitory effect of the MAC mechanism will be, and the fewer nodes the viruses can infect. Therefore, we regard the relationship between the number of active nodes and virus propagation rate as inversely proportional, and regard constant φ as a constraint constant. According to equations (2)–(4), the following equations can be obtained:

$$\frac{dI(t)}{dS(t)} = \frac{\rho}{AS(t)} - 1, \tag{6}$$

$$\frac{dR(t)}{dS(t)} = -\frac{\rho}{AS(t)}. \tag{7}$$

Assume that the initial S-state node number is $S(0) = S_0$ and the initial R-state node number is $R(0) = 0$. Then, we have the following results about $S(t)$ and $I(t)$ from equations (6) and (7):

$$\begin{aligned} S(t) &= S_0 e^{-(A/\rho)R(t)}, \\ I(t) &= N - R(t) - S_0 e^{-(A/\rho)R(t)}. \end{aligned} \tag{8}$$

3.4. Basic Regeneration Number R_0. Since $(dS/dt) < 0$, $S(t)$is monotonically decreasing and has a lower bound, the limit of

$$\lim_{t\longrightarrow\infty} S(t) = S_\infty, S_\infty = 0, \tag{9}$$

exists. It can be known from equations (2), (3), (6) that when $S(t) = (\rho/A)$, $I(t)$ reaches a maximum value. From equation (6), when the number of susceptible nodes $S(0) = S_0 > (\rho/A)$ at the beginning moment, with the increase of time, the number of infected nodes $I(t)$ will first increase to the maximum, then gradually decrease, and eventually die. This phenomenon shows that as long as $S_0 > (\rho/A)$, that is, $S_0 A\lambda(1/\gamma) > 1$, the viruses will spread in wireless sensor

networks. Therefore, the basic regeneration number R_0 of this model is

$$R_0 = S_0 A\lambda \frac{1}{\gamma} = \frac{AS_0}{\rho}. \tag{10}$$

When $R_0 > 1$, the viruses can spread exponentially on a large scale, and when $R_0 < 1$, the viruses will not spread, and the number of infected nodes will decrease monotonically to zero. The spreading of viruses meets a critical state if $R_0 = 1$. In this critical moment, viruses may spread only in a small area and die locally. To prevent the viruses from spreading in wireless sensor networks, reduce R_0 to less than 1 to achieve the purpose of hindering the spread of the viruses. From equation (10) and the definition of A, we can know that the virus infection ability λ can be reduced or the disease period $(1/\gamma)$ can be reduced through virus killing and other means. In addition, R_0 can be reduced by reducing the MAC mechanism listen/sleep duty cycle τ, node communication radius R_c, and network average node adjustment parameters β.

3.5. Stability Analysis. From the perspective of virus propagation dynamics, the behavior of removed state (R) nodes in the mathematical model of virus propagation is independent of susceptible state (S) nodes and infected state (I) nodes. Therefore, from equations (2) and (3), the SIR model has an infinite number of non-negative equilibrium points $S = S_0, I = I_0 = 0$, where S_0 is any non-negative real number, and because these equilibrium points satisfy $I = I_0 = 0$, it is also called disease-free equilibrium. When $R_0 \le 1$, the virus cannot spread out or die in a local area; therefore, the disease-free equilibrium point $(S_0, 0)$ is stable. But on the contrary, if $R_0 > 1$, the disease-free equilibrium point $(S_0, 0)$ is unstable. The proof is as follows:

Defining function (11),

$$\begin{cases} f_1(S, I) = -\lambda ASI, \\ f_2(S, I) = \lambda ASI - \gamma I. \end{cases} \tag{11}$$

Find the partial derivatives of S and I for the formulas f_1 and f_2, respectively,

$$\begin{cases} \dfrac{\partial f_1}{\partial S} = -\lambda AI, \\ \dfrac{\partial f_1}{\partial I} = -\lambda AS, \end{cases} \tag{12}$$

$$\begin{cases} \dfrac{\partial f_2}{\partial S} = \lambda AI, \\ \dfrac{\partial f_2}{\partial I} = \lambda AS - \gamma. \end{cases} \tag{13}$$

The linear parts of the Taylor expansions in equations (11) and (12) at $S = S_0$ and $I = I_0 = 0$ are

$$\begin{aligned} -\left(f_1(S_0, 0) + \frac{\mathrm{d}f_1}{\mathrm{d}S}\Big|_{(S_0,0)} (S - S_0) + \frac{\mathrm{d}f_1}{\mathrm{d}I}\Big|_{(S_0,0)} (I - 0) \right) &= \lambda AS_0 I, \\ -\left(f_2(S_0, 0) + \frac{\mathrm{d}f_2}{\mathrm{d}S}\Big|_{(S_0,0)} (S - S_0) + \frac{\mathrm{d}f_2}{\mathrm{d}I}\Big|_{(S_0,0)} (I - 0) \right) &= (\lambda AS_0 - \gamma) I. \end{aligned} \tag{14}$$

So, the linear equation at $S = S_0$ and $I = I_0 = 0$ is

$$\begin{cases} \dfrac{\mathrm{d}S(t)}{\mathrm{d}t} = \lambda AS_0 I, \\ \left(\dfrac{\mathrm{d}I(t)}{\mathrm{d}t} \right) = (\lambda AS_0 - \gamma) I. \end{cases} \tag{15}$$

The matrix of its linear equation is

$$B = \begin{bmatrix} 0 & \lambda AS_0 \\ 0 & \lambda AS_0 - \gamma \end{bmatrix}. \tag{16}$$

The characteristic equation of equation (16) is

$$\left| \lambda_E E - B \right| = \begin{vmatrix} \lambda_E & -\lambda AS_0 \\ 0 & \lambda_E - \lambda AS_0 + \gamma \end{vmatrix} = 0. \tag{17}$$

The eigenvalues of equation (17) are $\lambda_{E1} = 0$ and $\lambda_{E2} = \lambda AS_0 - \gamma$. From $R_0 > 1$, know $\lambda AS_0 > \gamma$, $\lambda_{E2} > 0$ and from the theory of ordinary differential equations, this disease-free equilibrium point $(S_0, 0)$ is unstable.

4. Simulation

In the simulation experiment using MATLAB, we randomly distribute $N = 1000$ nodes in an $X^2 = 100 \times 100$ square area and set the ratio between the number of long links and the number of short links in the network topology with $\alpha = 0.87$. We set all nodes as S-state nodes at the beginning and then randomly set a node as infected I-state to spread the viruses. Thus, at $t = 0$, we have $S(0) = 999$, $I(0) = 1, R(0) = 0$. As shown in Figure 1, at each time step, an I-state node infects each of the idle S-state neighbor nodes in its communication range with probability λ; then, the I-state node immediately transforms to the R-state with probability $\gamma = 1$. The newly infected node will turn to I-state in the next time step.

With the MAC mechanism, the energy consumption during the spread of virus in wireless sensor networks is considered. In a typical wireless sensor network, the energy consumed by data transmission and reception is much greater than that of other stages such as information processing, storage, and sleep [36, 37]. Therefore, we assume the initial energy of each node is E_0, and the remaining energy of

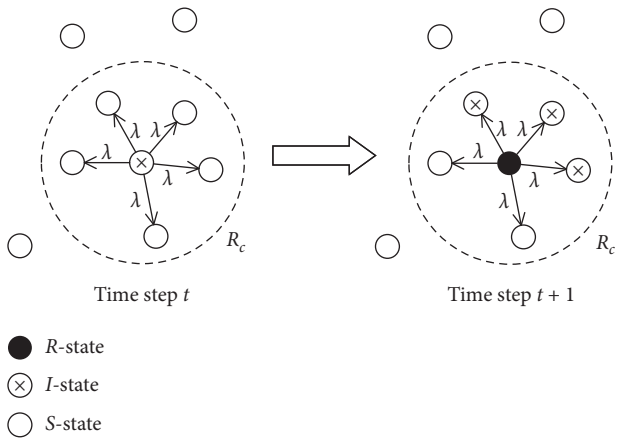

Figure 1: Node infection process state diagram.

the node i at time step t is $E_i(t)$, and the energy consumed by the node to transmit or receive a packet of data is $W = 5\,\text{V} \times 20\,\text{mA} \times 200\,\mu\text{S} = 2 \times 10^{-5}\,\text{J}$.

Then, according to the simulation results, we analyze the virus propagation process with node communication radius R_c, average node degree $\langle k \rangle$, virus infection probability λ, number of active nodes N_a, etc. For each influencing parameter, the result is based on an average of 50 simulations independently. If there is no data sending request in the network, we regard the number of active nodes as 0, and the MAC mechanism is considered as not working in this situation. Otherwise, it will be regarded as the case that the MAC mechanism works.

4.1. Effect of Active Nodes Number in Virus Propagation. Figure 2 shows the effect of the number of active nodes N_a on virus propagation under different infection probabilities λ. In this simulation, in addition to the default value, other parameters are set as follows: node communication radius $R_c = 7$, average node degree $<k> = 0$, active node number $N_a = 0, 5, 10, 15, 20$, respectively, network average degree adjustment parameter $\beta = 0.7$, the listen/sleep duty cycle of the MAC mechanism $\tau = 0.6$. It can be observed from Figure 2 that the infection ability of the viruses increases with the increase of infection probability λ. But the more active nodes in the network, the fewer nodes the viruses can infect with the same infection rate λ. Figure 2 also shows that when there are many active nodes, even if the infection probability λ is large, the viruses cannot spread to the entire network. Through the analysis of the experimental results, it is found that there are two reasons for this phenomenon:

Firstly, the influence of a number of active nodes: the more active nodes, the fewer nodes the viruses infect, and the active nodes will affect the speed of network failure. The more active nodes, the faster the network failure rate, the faster the network failure, and the more nodes retained to work, so that even if the infection probability is large, the viruses cannot spread to the entire network.

Secondly, the influence of the infection probability: the higher the infection probability is, the stronger the ability of the viruses is, and the more nodes are infected.

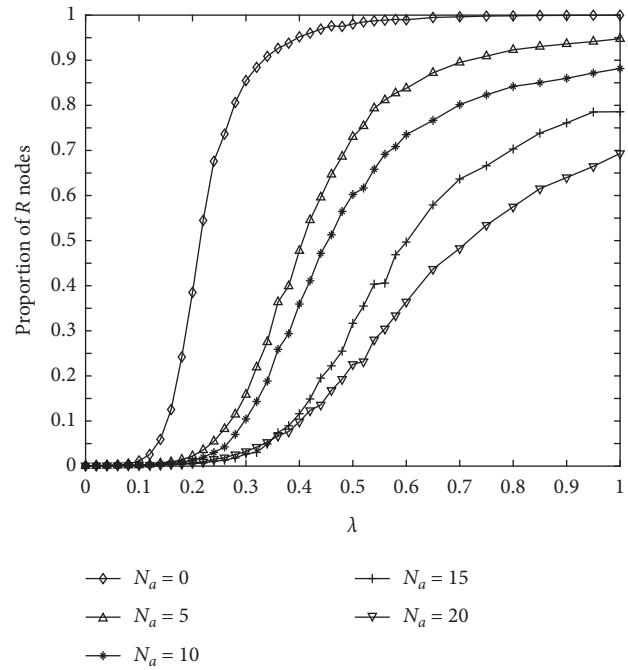

Figure 2: Effect of the number of active nodes on virus propagation under different infection probabilities.

Figure 3 shows the influence of the number of active nodes N_a on the speed of virus propagation under the same infection probability. This part of the simulation analyzes the propagating process of virus propagation in the time domain with a significant value of infection probability $\lambda = 0.6$. Figure 3 reflects that, in the same network environment, the number of active nodes can directly affect the scale of infected nodes, which is roughly inversely proportional. The more active nodes, the slower the virus infects the node and the fewer infected nodes.

4.2. Effect of Listen/Sleep Duty Cycle in Virus Propagation. Figure 4 shows the effect of listen/sleep duty cycle τ on virus propagation under different infection probabilities λ. In this simulation, in addition to the default value, other parameters are set as follows: node communication radius $R_c = 7$, average node degree $<k> = 10$, active node number $N_a = 20$, respectively, network average degree adjustment parameter $\beta = 0.7$, the listen/sleep duty cycle of the MAC mechanism $\tau = 0, 0.2, 0.4, 0.6, 0.8, 1$. The curve change in the figure intuitively reflects that the listen/sleep duty cycle on the MAC mechanism is proportional to the size of the infected node. The larger the listen/sleep duty cycle is, the more nodes infected by the viruses, and the smaller the listen/sleep duty cycle is, the fewer nodes. The listen/sleep duty cycle represents the ratio of the listening period to the length of the sleeping period within a period of time. When the listen/sleep duty cycle approaches zero, it indicates that the network is always in a dormant state, so the viruses cannot spread on the network in this state. The $\tau = 0$ curve in Figure 4 confirms this statement.

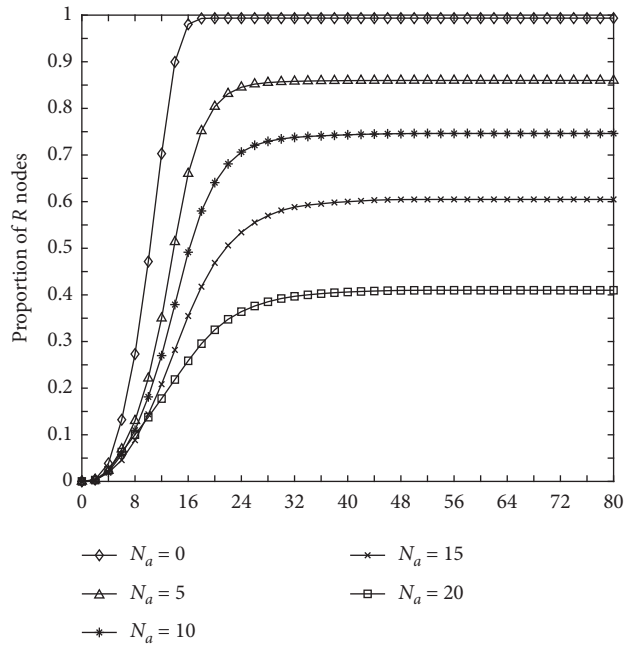

Figure 3: The effect of the number of active nodes on virus propagation in the time domain with $\lambda = 0.6$.

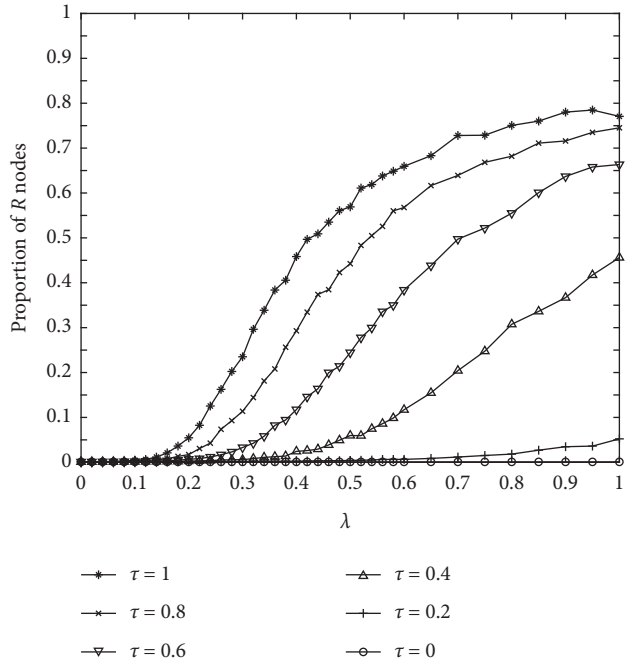

Figure 4: The impact of the listen/sleep duty cycle τ on viral transmission.

The listen/sleep duty cycle of the MAC mechanism affects virus propagation by changing the duration of the listening period. The smaller the listen/sleep duty cycle, the slower the virus propagation and the smaller the scale. Theoretically, to prevent the viruses from spreading in the network, it is better to set the listen/sleep duty cycle as short as possible. But this is not the case. The listen/sleep duty cycle of the MAC mechanism not only affects the virus propagation process but also affects the flow of normal data, causing latency issues. For networks with higher real-time requirements, a lower listen/sleep duty cycle is fatal. Therefore, considering the delay and energy-saving issues, the listen/sleep duty cycle used in this study is 0.6.

4.3. Virus Propagation with MAC Mechanism under Different Values of Infection Probability. The dynamics of virus propagation under different values of infection probabilities λ considering the impact of the MAC mechanism are shown in Figure 5. Node communication radius $R_c = 7$, average node degree $<k> = 10$, virus infection probability $\lambda = 0.4$, 0.8, active node number $N_a = 0$, 20, network average degree adjustment parameter $\beta = 0.7$, and the listen/sleep duty cycle of the MAC mechanism $\tau = 0.6$. The probability of virus infection indicates the infectivity of the viruses. The stronger the infectivity, the more nodes the viruses infect. From the comparison in Figure 5, the higher the infection probability of the same MAC scheme is, the faster the virus propagation speed is, and the larger the infection scale is after it tends to be stable. We also find that using the MAC mechanism can well suppress the speed of network virus propagation and the scale of infection.

Furthermore, the smaller the probability of viral infection, the more obvious the inhibition of viral transmission by MAC mechanism, the slower the viruses spread, and the fewer infected nodes. It indicates that the probability of virus infection or MAC mechanism will have an impact on the spread of the viruses, but the combined effect of the two will be better. What is more, the smaller the probability of viral infection, the more obvious the inhibition of viral transmission by MAC mechanism, the slower the viruses spread, and the fewer infected nodes. It indicates that the probability of virus infection or MAC mechanism will have an impact on the spread of the viruses, but the combined effect of the two will be better.

Figure 6 shows the influence of node averaging degree $\langle k \rangle$ on virus propagation speed. The node communication radius $R_c = 7$, the average node degree $<k> = 7, 10, 13$, the virus infection probability $\lambda = 0.6$, the number of active nodes $N_a = 0, 20$, the listen/sleep duty cycle of the MAC mechanism $\tau = 0.6$, and the regulating parameters of network average degree $\beta = 0.53$, 0.7, 0.9, respectively. It can be observed from Figure 6 that, without considering the MAC mechanism, the greater the average node degree, the faster the viruses spread. Eventually, the viruses infect the entire network. Considering the MAC mechanism, the speed of virus propagation increases with the average node degree, but in the end, it can only infect some nodes, and the number of virus-infected nodes increases as the average node degree increases. Through comprehensive analysis, it is found that the average node degree would affect the speed and scale of virus propagation. At the same time, the MAC mechanism will hinder the propagating speed of viruses and will also inhibit the influence of the average node degree on virus propagation.

The effect of communication radius R_c on virus propagation is shown in Figure 7. The research in this part mainly

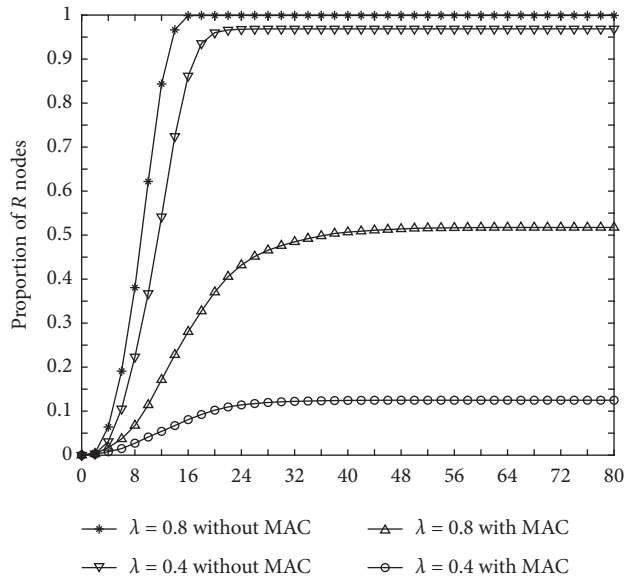

Figure 5: The impact of infection probability λ on viral transmission.

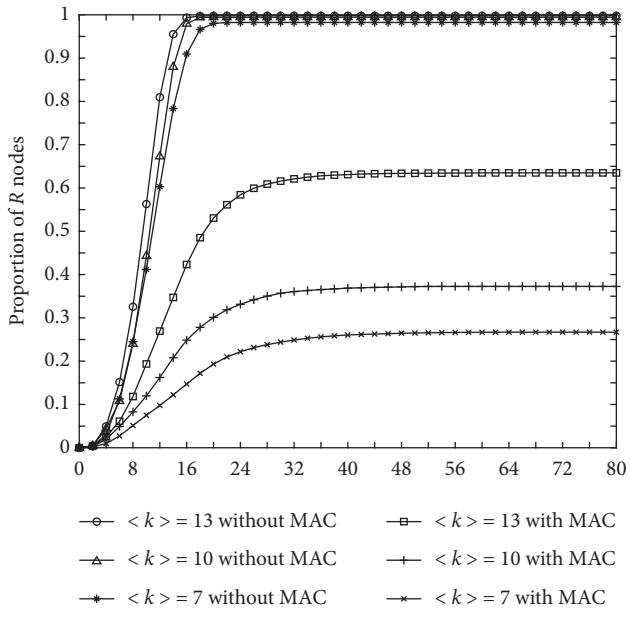

Figure 6: The effect of the average node degree $\langle k \rangle$ of nodes on virus propagation.

focuses on the changes in virus propagation speed and the infection scale after the stabilization caused by the change of node communication radius R_c. The node communication radius $R_c = 6, 7, 8$, the average node degree $<k> = 10$, the virus infection probability $\lambda = 0.6$, the active node number $N_a = 0, 20$, the network average adjustment parameter $\beta = 0.55, 0.7, 0.95$, and the listen/sleep duty cycle of the MAC mechanism $\tau = 0.6$. It can be observed from Figure 7 that, under the same communication radius, the influence of the presence or absence of the MAC mechanism on virus propagation is the opposite. Without considering the impact

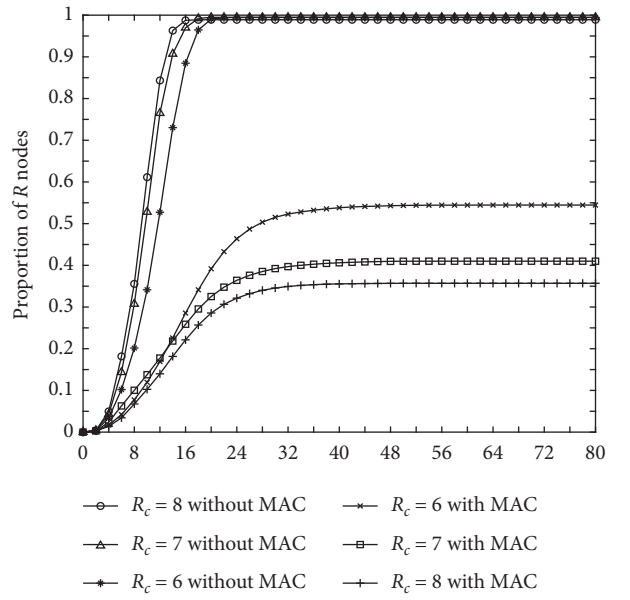

Figure 7: The effect of communication radius R_c on virus propagation.

of the MAC mechanism, the larger the communication radius of the node, the faster the virus propagation will be, and the viruses will eventually infect the whole network. However, under the influence of the MAC mechanism, the larger the node communication radius, the slower the virus propagation speed, and the fewer infected nodes. The experimental results show that whether the MAC mechanism works or not will affect the impact of communication radius on virus propagation. As can be seen from the above, if you want to suppress the spread of network virus better, you can use the MAC mechanism and the network average to work together.

4.4. Energy Consumption in Virus Propagation. Figure 8 shows the energy consumption in virus propagation under different infection probabilities λ. In this simulation, the parameters are set as follows: $R_c = 7$, $<k> = 10$, $\beta = 0.7$, $\tau = 0.6$, and $N_a = 0, 5, 10, 15, 20$, respectively. Figure 8 shows the energy consumption in virus propagation has a peak value as λ increases. When $0 < \lambda < \lambda_{\text{peak}}$, with the increasing of λ, the scale of virus infection in the network increases, so energy consumption also increases. On the contrary, when $\lambda > \lambda_{\text{peak}}$, as λ increases, the energy consumption decreases slowly.

The interaction combined with the infection scale of network and spreading speed of virus leads to the existence of peak value of energy consumption. We assume that, when $\lambda = \lambda_{\text{peak}}$ ($N_a = 0, \lambda_{\text{peak}} = 0.32$; $N_a = 5, \lambda_{\text{peak}} = 0.36$; $N_a = 10$, $\lambda_{\text{peak}} = 0.42$; $N_a = 15, \lambda_{\text{peak}} = 0.6$; $N_a = 20, \lambda_{\text{peak}} = 0.75$), the energy consumption reaches its largest value. There are two factors influencing the energy consumption of virus propagation: the infection scale and the speed of virus propagation. When the virus can spread out in the network, the larger infection scale will cause the faster propagation speed. A larger infection scale consumes more energy. But the faster propagation speed

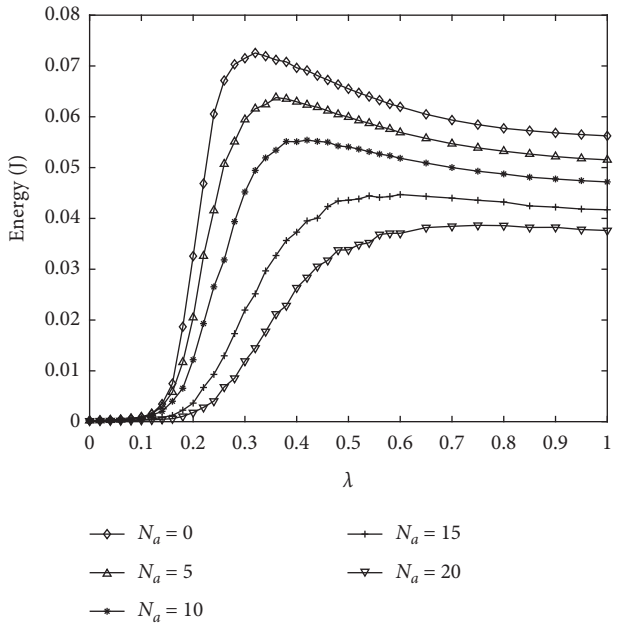

Figure 8: The energy consumption in virus propagation with various values of λ.

reduces the time for the virus to spread out and reduces the energy consumption relatively. Therefore, peak value of energy consumption is the result of the combined effect of the infection scale and propagation speed.

5. Analysis of Results

In the context of the wireless sensor networks, this paper established a random network topology model based on the characteristics of limited node communication radius and wireless access MAC layer. It improved the classical SIR virus propagation model on this basis, to study the virus propagation dynamics in the network environment and find the characteristics of virus propagation. We mainly studied the characteristics of virus propagation process with the number of active nodes N_a, the listen/sleep duty cycle τ, the virus infection probability λ, the average node degree $\langle k \rangle$, the communication radius of nodes R_c, etc. And we verified the conclusion that the MAC mechanism affects virus propagation by comparing the research results with or without the MAC mechanism. Compared with the experimental results, it is found that wireless access to the MAC mechanism does affect the process of virus propagation and has an inhibitory effect. Moreover, it can be known from the propagation model that the listen/sleep duty cycle of the MAC mechanism directly affects the virus suppression effect. The smaller the listen/sleep duty cycle, the smaller the change amount of the infected node per unit moment, and vice versa. The results of the research on the listen/sleep duty cycle also confirm this conclusion. Besides, we also found that factors such as virus infection probability, average node degree, and node communication radius would promote virus propagation. In contrast, the number of active nodes would hinder virus propagation. The probability of virus infection λ and the average node degree $\langle k \rangle$ have similar effects on the virus propagation procedure. Increasing the probability of virus infection λ or the average node degree $\langle k \rangle$ can accelerate the speed of the virus propagation process and increase the scale of virus infection. The number of active nodes N_a will restrain the virus propagation procedure. The more active the node, the larger the range of signal interference, the smaller the virus spread, and the better the suppression effect. The influence of node communication radius R_c on virus propagation is more complicated. Without considering the MAC mechanism, the larger the communication radius R_c is, the faster the viruses spread, and the more nodes the viruses infect. On the contrary, if the MAC mechanism is considered, the virus propagation process is opposite to the previous situation. Increasing the communication radius R_c of nodes can increase the range of signal interference. The larger the range of signal interference, the smaller the range of virus propagation and the fewer nodes infected by viruses. Therefore, in wireless sensor networks with the MAC mechanism, the traditional virus propagation models do not consider the impact of the MAC mechanism and cannot be directly applied. Because the MAC mechanism has played a significant inhibitory effect on virus propagation, the MAC mechanism can not only slow down the virus propagation rate but also reduce the number of infected nodes. In terms of energy consumption, when $\lambda = \lambda_{\text{peak}}$, energy consumption reaches the peak value. When $\lambda > \lambda_{\text{peak}}$, energy consumption reduces with the increasing of λ, because the spread of the virus stops prematurely. This situation is the result of the combined effect of the infection scale and speed of the virus spreading. The results have important reference significance for the study of virus propagation procedure in wireless sensor networks.

6. Conclusion

Aiming at the characteristics of wireless sensor networks with space constraints and the MAC communication mechanism, we explore the virus propagation process wireless sensor networks by using the SIR model. The analysis of the mathematical model of virus propagation shows that the number of active nodes, the probability of virus infection, the average node degree, the communication radius of the nodes, and the listen/sleep duty cycle of the MAC mechanism will affect the virus propagation in the wireless sensor network. Reasoning and qualitative analysis: the increase in the probability of virus infection and the increase in the average node degree will promote the spread of the viruses; the number of active nodes will suppress the spread of the viruses; the larger the number of active nodes, the slower the viruses spread, and the node communication radius is relatively complicated. Under the MAC mechanism, the increase in the phase of the node communication radius will inhibit the viruses from spreading. Still, the opposite is true without the MAC mechanism. The effect of the MAC mechanism on virus suppression depends on the listen/sleep duty cycle. The smaller the listen/sleep duty cycle, the better the virus propagation suppression effect. With the MAC mechanism in wireless sensor networks, the

traditional virus propagation models cannot be applied directly. In addition, with the change of λ, the peak value of energy consumption in the process of virus propagation appears at a specific infection probability λ value. This situation is the result of the combined effect of the infection scale and speed of the virus spreading. This paper relatively comprehensively and systematically studies the specific influence of various factors of wireless sensor networks on the process of virus propagation. To a certain extent, it can provide corresponding theoretical support for solving the security risks of wireless sensor networks and formulating effective virus immunity mechanism of wireless sensor networks.

Data Availability

The simulation data and results used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (61602417), Zhejiang Provincial Key Research and Development Plan (2015C03023), Public Welfare Project of Zhejiang Province under Grant no. 2014C33102, Basic Scientific Research Project of Zhejiang Sci-Tech University (2019Q042), and "521" Talent Project of ZSTU.

References

[1] I. Khan, "An introduction to computer viruses: problems and solutions," *Library Hi Tech News*, vol. 29, no. 7, pp. 8–12, 2012.

[2] B. Sandywell, "Monsters in cyberspace cyberphobia and cultural panic in the information age," *Information, Communication & Society*, vol. 9, no. 1, pp. 39–61, 2006.

[3] G. L. Jr, "Not teaching viruses and worms is harmful," *Communications of the ACM*, vol. 48, no. 1, p. 144, 2005.

[4] S. Venkatraman, "Autonomic conte xt-dependent architecture for malware detection," in *Proceedings of the 2009 International Joint Conferences on e_CASE and e-Technology*, pp. 2927–2947, Singapore, Asia, January 2009.

[5] L. N. Devi and A. N. Rao, "Optimization of energy in wireless sensor networks using clustering techniques," in *Proceedings of the 2016 International Conference on Communication and Electronics Systems (ICCES)*, pp. 1–4, Coimbatore, India, October 2016.

[6] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "A framework for cyber-topology attacks: line-switching and new attack scenarios," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1704–1712, 2017.

[7] R. Arya and S. C. Sharma, "Energy optimization of energy aware routing protocol and bandwidth assessment for wireless sensor network," *International Journal of System Assurance Engineering and Management*, vol. 9, no. 3, pp. 612–619, 2014.

[8] J. Kleinberg, "The wireless epidemic," *Nature*, vol. 449, no. 7160, pp. 287-288, 2007.

[9] B. K. Mishra and N. Keshri, "Mathematical model on the transmission of worms in wireless sensor network," *Applied Mathematical Modelling*, vol. 37, no. 6, pp. 4103–4111, 2013.

[10] Y. Chen, "Analysis on security management strategy of computer and Internet information system," in *Proceedings of the 2016 2nd Workshop on Advanced Research and Technology in Industry Applications*, Dalian, China, May 2016.

[11] T. Wang, Q. Wu, S. Wen et al., "Propagation modeling and defending of a mobile sensor worm in wireless sensor and actuator networks," *Sensors*, vol. 17, no. 12, p. 139, 2017.

[12] T. Li, W. Liu, T. Wang, Z. Ming, X. Li, and M. Ma, "Trust data collections via vehicles joint with unmanned aerial vehicles in the smart internet of things," *Transactions on Emerging Telecommunications Technologies*, Article ID e3956, 2020.

[13] B. Jiang, G. Huang, T. Wang, J. Gui, and X. Zhu, "Trust based energy efficient data collection with unmanned aerial vehicle in edge network," *Transactions on Emerging Telecommunications Technologies*, Article ID e3942, 2020.

[14] Y. Ren, Z. Zeng, T. Wang, S. Zhang, and G. Zhi, "A trust-based minimum cost and quality aware data collection scheme in P2P network," *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, p. 2300, 2020.

[15] J. Hu and Y. Song, "The model of malware propagation in wireless sensor networks with regional detection mechanism," in *Communications in Computer and Information Science Advances in Wireless Sensor Networks*, pp. 651–662, Springer, Berlin, Germany, 2015.

[16] S. Tang and B. L. Mark, "Analysis of virus spread in wireless sensor networks: an epidemic model," in *Proceedings of the 2009 7th International Workshop on Design of Reliable Communication Networks*, pp. 86–91, Washington, DC, USA, October 2009.

[17] Z. Zhou, W. Wang, and Y. Li, "Virus propagation model for wireless sensor networks based on IPv6," *International Journal of Online Engineering (IJOE)*, vol. 14, no. 10, p. 117, 2018.

[18] L. Feng, L. Song, Q. Zhao, and H. Wang, "Modeling and stability analysis of worm propagation in wireless sensor network," *Mathematical Problems in Engineering*, vol. 2015, Article ID 129598, 8 pages, 2015.

[19] X. Wang and S. Li, "An improved SIR model for analyzing the dynamics of worm propagation in wireless sensor networks," *Chinese Journal of Electronics*, vol. 18, no. 1, pp. 8–12, 2009.

[20] A. P. Srivastava, S. Awasthi, R. P. Ojha, P. K. Srivastava, and S. Katiyar, "Stability analysis of SIDR model for worm propagation in wireless sensor network," *Indian Journal of Science and Technology*, vol. 9, no. 31, 2016.

[21] A. Singh, A. K. Awasthi, K. Singh, and P. K. Srivastava, "Modeling and analysis of worm propagation in wireless sensor networks," *Wireless Personal Communications*, vol. 98, no. 3, pp. 2535–2551, 2017.

[22] R. K. Upadhyay and S. Kumari, "Bifurcation analysis of an e-epidemic model in wireless sensor network," *International Journal of Computer Mathematics*, vol. 95, no. 9, pp. 1775–805, 2017.

[23] N. Xiang, Z. Zehong, and P. Zhigeng, "Using SIR model to simulate emotion contagion in dynamic crowd aggregation process," *International Journal of Performability Engineering*, vol. 14, no. 1, pp. 134–143, 2018.

[24] S. Lamzabi, S. Lazfi, A. Rachadi, H. Ez-Zahraouy, and A. Benyoussef, "Modeling the spread of virus in packets on scale free network," *International Journal of Modern Physics C*, vol. 27, no. 6, Article ID 1650068, 2016.

[25] I. Androulidakis, S. Huerta, V. Vlachos, and I. Santos, "Epidemic model for malware targeting telephony networks," in

Proceedings of the 2016 23rd International Conference on Telecommunications (ICT), pp. 1–5, Thessaloniki, Greece, May 2016.

[26] H. Li and P. D. Mitchell, "Medium access control protocols in wireless sensor networks," in *Proceedings of the 2007 15th IEEE International Conference on Networks*, pp. 455–460, Beijing, China, October 2007.

[27] M. Nekovee, "Worm epidemics in wireless ad hoc networks," *New Journal of Physics*, vol. 9, no. 6, p. 189, 2007.

[28] P. Li, S. Liu, J. Jin, and Z. Wang, "Influence of node mobility on virus spreading behaviors in multi-hop network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, p. 172, 2016.

[29] Y.-Q. Wang and X.-Y. Yang, "Virus spreading in wireless sensor networks with a medium access control mechanism," *Chinese Physics B*, vol. 22, no. 4, Article ID 040206, 2013.

[30] S. R. Chamberlain, J. G. Tucker, J. M. Conroy, and H. G. Miller, "Waxman's algorithm for non-Hermitian Hamiltonian operators," *Journal of Physics Communications*, vol. 2, no. 2, Article ID 025026, 2018.

[31] A. Patil, S. Patil, S. Patil, and P. Manickam, "Identification of lung cancer related genes using enhanced floyd warshall algorithm in a protein to protein interaction network," *International Journal of Intelligent Engineering and Systems*, vol. 11, no. 3, pp. 215–222, 2018.

[32] H. Li and P. D. Mitchell, "Reservation packet medium access control for wireless sensor networks," in *Proceedings of the 2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1–5, Cannes, France, September 2008.

[33] V. K. Ramachandran, E. Ayele, N. Meratnia, and P. Havinga, "Potential of wake-up radio-based MAC protocols for implantable body sensor networks (IBSN)-a survey," *Sensors*, vol. 16, no. 12, p. 2012, 2016.

[34] W. Ye, J. Heidemann, and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks," in *Proceedings of the Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, p. 5, Chengdu, China, August 2010.

[35] W. Wang, Q.-H. Liu, L.-F. Zhong, M. Tang, H. Gao, and H. E. Stanley, "Predicting the epidemic threshold of the susceptible-infected-recovered model," *Scientific Reports*, vol. 6, no. 1, Article ID 24676, 2016.

[36] H. Byun and J. So, "Node scheduling control inspired by epidemic theory for data dissemination in wireless sensor-actuator networks with delay constraints," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 1794–1807, 2015.

[37] H.-Y. Zhou, D.-Y. Luo, Y. Gao, and D.-C. Zuo, "Modeling of node energy consumption for wireless sensor networks," *Wireless Sensor Network*, vol. 3, no. 1, pp. 18–23, 2011.