Control Mechanism of Virus Propagation in Wireless Sensor Networks Based on Analytic Hierarchy Process

Lurong Jiang,1,2,3 Hangyi Pan,1 Jiawang He,1 Renwang Li,2 Changguo Xu,3 Qiaoyu Xu,1 Yanyun Dai,1 Fang Dong,4 and Jijun Tong1

1School of Information Science and Technology, Zhejiang Sci-Tech University, Hangzhou, China
2School of Mechanical Engineering and Automation, Zhejiang Sci-Tech University, Hangzhou, China
3Postdoctoral Workstation, Zhejiang Dafeng Technology Co., Ltd., Hangzhou, China
4College of Information and Electric Engineering, Zhejiang University City College, Hangzhou 310015, China

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

Received 15 November 2021; Revised 10 April 2022; Accepted 23 April 2022; Published 17 May 2022

The research on virus propagation process and control method in wireless sensor networks (WSNs) is one of the essential challenges of network security. This paper proposes a virus control mechanism of degree, betweenness centrality, and k-core-based analytical hierarchy process (DBC-AHP) for WSNs. According to the topology of WSNs, the virus control mechanism uses the DBC-AHP to identify the crucial nodes of the network. It uses the way of crucial nodes’ self-disconnection to suppress the spread of the virus, to improve the network security. In this paper, the effectiveness of the virus control mechanism based on the DBC-AHP is verified by comparing and analyzing the effect of four different crucial node recognition algorithms. With the research of virus control mechanisms in various network environments, it is found that the average degree of nodes, the communication radius of nodes, and the probability of virus infection can affect the inhibition effect of the virus control mechanism. Furthermore, the inhibition effect of virus control mechanisms is studied under the condition with/without MAC mechanism.

1. Introduction

Wireless sensor networks (WSNs) are wireless communication networks formed by a large number of sensor nodes connected in a self-organizing manner. In general, WSNs is the subclass of computer network, using complex network communication protocols, so the WSNs face the virus threat [1]. The spatial openness [2] and topology heterogeneity [3] of WSNs make it easy for attackers to invade the networks. In addition, the limited energy of nodes makes WSNs vulnerable to resource consumption [4, 5]. In addition, protocols of WSNs at different layers will also suffer from different types of attacks, for example, MAC (media access control) layer DoS attack [6], routing attack [7], and so on. Therefore, with the development of the application of WSNs, the network safety problem against virus propagation has increased prominently.

The virus propagation model in complex networks can describe the process of the virus spreading in computer networks or wireless networks [8, 9]. In the process of virus propagation, some nodes can accelerate or inhibit the dynamical spreading process as influential spreaders. We call these nodes crucial nodes. With the identification and strength of crucial nodes, the virus spread speed or the scale of infected nodes can be effectively controlled [10]. Although the research on crucial node identification and virus control methods in complex networks is abundant, there are still few related researches due to the structural characteristics of WSNs.

This paper proposes a crucial node identification and virus control method in WSNs. In detail, we use the node degree, betweenness centrality, and k-core as the indicators of the importance of node, then rank the importance of nodes by the analytical hierarchy process (AHP) method in
the process of virus propagation in WSNs, and finally reduce the scale of virus infection. This paper is organized as follows: in Section 2, we study the relative works of the virus propagation process and the virus control mechanism in WSNs. Then, we introduce the network construction model and the SIR model of network virus propagation in our research in Section 3. Section 4 describes the detail of the crucial node identification and virus control method. The simulation results show that the algorithm is effective to suppress the infection scale of the virus in Section 5. In Section 6, we conclude.

2. Related Works

To explore the virus propagation dynamics in WSNs, many researchers use the virus propagation principle of complex networks theory in WSNs. Upadhyay and Kumari [11] develop an electronic popular SITR model to analyze the attack behavior of worms in WSNs with cytoid type functional response. Considering channel interference and dynamic linking, Liu et al. [12] study the influence of mobility in the spread of malignant software in WSNs in extended mode and communication mode. Some researchers use classical methods such as the principle of percolation to quantitatively analyze the virus propagation process in WSNs [13]. Liu et al. [14] considered the low power consumption characteristics of WSNs. They introduced a low-energy state to the traditional SIR model and then described the virus propagation and mutation process in the rechargeable WSNs. In our former work [15], we proposed an SIR model considered with media access control (MAC) mechanism and found out that MAC with listen/sleep duty cycle can inhibit the scale of virus propagation. Shakya et al. [16] used spatial correlation to improve the SIR model in WSNs and study the influence of basic reproduction number, spatial correlation, and node density on the speed of virus propagation. Nwokoye et al. [17] established a multistate virus propagation model, adding a variety of intermediate states between the susceptible state and the infectious state. In summary, the SIR model can describe the virus propagation process in WSNs, but it is also necessary to improve the SIR model for the characteristics of low power consumption, the openness of wireless channels, and self-organization in WSNs [18].

The immunization control of virus propagation is one of the hotspots in studying virus dynamics. The existing WSN virus immunization control mechanisms can be divided into network-structure- and machine-learning-based control methods. And the network-structure-based control methods can be further subdivided into uniform control, acquaintance control, and target control methods. Each immunization control mechanism has its advantages and disadvantages.

The uniform control method randomly [19–21] selects a certain proportion of nodes as immune nodes in the network. This mechanism is relatively simple to apply, but the accuracy is not high, the immune cost is high, the virus suppression effect is not apparent, and the virus spread cannot be accurately and quickly suppressed due to the strong randomness.

The acquaintance control method [22, 23] is an improved random control mechanism. The mechanism first selects a certain proportion of nodes. It then randomly selects a node from the neighbor nodes of each selected node for control. Compared with the random control mechanism, the accuracy of the acquaintance control mechanism has been improved; the virus suppression effect has also been enhanced; and it is suitable for large-scale network virus defense, but the acquaintance control mechanism is unstable.

The target control method is a relatively complete mechanism among these three immunization control mechanisms [24, 25]. Xia et al. [26] take the clustering attribute as a critical feature of nodes, find out the crucial nodes, and strengthen their protection. Zhang et al. [27] provide a LeaderRank algorithm to find out the crucial spreaders of the virus with node degree and clustering coefficient. Li and Xiao [28] rank the importance of nodes based on the precise radius and value information. Guo et al. [29] identify the crucial nodes with the indicator of entropy. The core idea of target control is to identify crucial nodes based on network structure information, and then strengthen the immunity of these nodes. As long as a few nodes are immunized, the spread of the virus can be quickly suppressed. Therefore, this mechanism has strong performance and high accuracy.

Machine learning is a type of essential method to realize intrusion detection and security [30]. Machine learning technology can predict the dynamic behavior of networks according to develop a model for completing specific security tasks. Some researchers have applied machine learning technology to identify the crucial spreaders in virus propagation. Rathore and Jha [31] use bio-inspired machine learning technology to identify the crucial spreaders in virus propagation. Xia et al. [32, 33] use graph convolutional networks (GCNs) to distinguish between fraudulent nodes and good nodes in the system. Some researchers identify the crucial nodes with graph convolutional networks (GCNs) [32, 33]. Though machine learning technology shows an excellent application effect on security situation assessment, the identification of crucial nodes is still mainly based on network structure. The reason is that the crucial node identification method based on network structure has strong interpretability and better generalization performance for all kinds of networks [34].

3. Network Construction and Virus Spreading Model

3.1. Network Construction Model. The wireless sensor node is limited by energy and a terrible environment, making charging and checking the sensor node difficult. Therefore, it is vital that prolong the sensor node’s life [35]. Besides, WSNs are composed of a free-networking mode, which causes topological randomness significantly. Therefore, we have proposed a random network topology generation model based on the Waxman algorithm in our former work [15]. We deploy $N$ nodes randomly in an area with a size of $S \times S$ and then link two arbitrary nodes with $p_c$. The probability $p_c$ of the existing a link between two nodes in a WSN is
\[ p_c(u,v) = \begin{cases} 0, & I(u,v) > r_c, \\ \beta \exp\left(-\frac{(u,v)}{L}\right), & 0 \leq I(u,v) \leq r_c, \end{cases} \tag{1} \]

where \( r_c \) is the node communication radius, \( I(u,v) \) is the distance between two nodes \( u \) and \( v \), \( L \) is the longest distance between arbitrary pair of nodes, \( \beta \) is the adjustment parameter of average node degree, and \( \alpha \) can adjust the ratio of long links number to short links number.

### 3.2. Virus Propagation Model

The model of virus propagation in WSNs is based on the classic SIR virus propagation model, and this model is further constructed by comprehensively considering the environment and the propagation characteristics of the virus itself [36, 37]. We proposed an improved SIR propagation model according to the effect of the link-layer listening/sleeping mechanism and limited energy in WSNs. Furthermore, we explore the effect of duty ratio in the WSNs link-layer listening/sleeping mechanism and the interaction of data translation and virus propagation in WSNs.

Each node in WSNs has three different states, namely susceptible state (\( S \)), infectious state (\( I \)), and removed state (\( R \)). A node in a susceptible state can be infected and turns to be infectious state. And then, the infected node turns into removed state. Every node can only be in one of three states at each moment. Only the \( R \) node became invalid, which means it cannot transfer the data or propagate the virus or be infected again. Let \( S(t) \) denote the number of susceptible nodes at time \( t \), \( I(t) \) denote the number of infectious nodes at time \( t \), and \( R(t) \) denote the number of removed nodes at time \( t \). At every moment the equation \( N = S(t) + I(t) + R(t) \) is always satisfied. All node states in the networks are \( S \) when the topology of the networks is generated. At the beginning of the virus spreading, set an arbitrary node as \( S \) state. Then, this node starts propagating virus outward. The proportion of nodes in each state of the initial networks is \( S(0) = N - 1, I(0) = 1, \) and \( R(0) = 0 \).

Virus propagation or normal data transmission between any nodes in WSNs is subject to a link-layer mechanism. Nodes need to check the transmission channel status before any nodes in WSNs is subject to a link-layer mechanism. Furthermore, we explore the effect of duty ratio in the WSNs link-layer listening/sleeping mechanism and the interaction of data translation and virus propagation in WSNs.

\[
\begin{align*}
\frac{dS(t)}{dt} &= -\eta \tau \frac{c_1 - c_2}{\delta} a \beta \pi r^2 X S(t) I(t), \\
\frac{dI(t)}{dt} &= \eta \tau \frac{c_1 - c_2}{\delta} a \beta \pi r^2 X S(t) I(t) - \gamma I(t), \\
\frac{dR(t)}{dt} &= \gamma I(t).
\end{align*}
\tag{2}
\]

Let \( A = \tau \frac{c_1 - c_2}{\delta} a \beta \pi r^2 X^2 \) and \( \rho = \gamma / \eta, a, c_1, \) and \( c_2 \) are adjustment constant. We also can combine (2) that can be viewed as

\[
\begin{align*}
\frac{dS(t)}{dt} &= \frac{\rho}{A S(t)} - 1, \\
\frac{dR(t)}{dt} &= -\frac{\rho}{A S(t)}.
\end{align*}
\tag{3}
\]

At the beginning of virus spreading, the initial proportion of the \( S \)-state node is \( S_0 \), and the initial proportion of the \( R \)-state node is 0. We also can get the following equations from equations (3):

\[
\begin{align*}
S(t) &= S_0 \exp\left(-\frac{A}{\rho} R(t)\right), \\
I(t) &= N - R(t) - S_0 \exp\left(-\frac{A}{\rho} R(t)\right). \\
R(t) &= \gamma I(t).
\end{align*}
\tag{4}
\]

### 4. Crucial Node Identification in Virus Propagation

#### 4.1. Degree, Betweenness Centrality, and k-Core

In the complex network, node important evaluation indicators based on topological structure are node degree, betweenness centrality [38], k-core decomposition [39], and so on.

The degree of a node is the number of connections it has to other nodes. In WSNs, the node degree \( k \) indicates the number of direct communication relations between a node and its \( k \) neighbors.

Betweenness centrality measures the centrality in a network based on the shortest paths. Betweenness centrality of node \( i \) in network is defined as

\[
b_c(i) = \sum_{uv} \frac{I_{uv}}{l_{uv}}, \tag{5}
\]

where \( l_{uv} \) is the number of shortest paths between an arbitrary pair of nodes \( u \) and \( v \) and \( l_{uv} \) is the number of shortest paths between nodes \( u \) and \( v \) and pass through node \( i \). Therefore, betweenness centrality is a parameter that measures the importance of a node according to the amount of information passing through it. The higher the betweenness centrality of the node in the network, the more the importance of this node as a bridge. Betweenness centrality measures the centrality in a network based on the shortest paths. Betweenness centrality of node \( i \) in network is defined as

\[
b_c(i) = \sum_{uv} \frac{I_{uv}}{l_{uv}}, \tag{5}
\]

where \( l_{uv} \) is the number of shortest paths between an arbitrary pair of nodes \( u \) and \( v \) and \( l_{uv} \) is the number of shortest paths between nodes \( u \) and \( v \) and pass through node \( i \). Therefore, betweenness centrality is a parameter that measures the importance of a node according to the amount of information passing through it. The higher the betweenness centrality of the node in the network, the more the importance of this node as a bridge.
centrality is the characterization of nodes in the global scope of the entire network.

The $k$-core means the largest subgraph where nodes in the network have at least $k$ interconnections [40]. We can get the $k$-core of each node starting with $k = 1$ as follows:

Step 1. Remove all nodes with degrees less than $k$ in the network and their edges.

Step 2. If some of the rest nodes remain with less than degree $k$, then repeat step 1; otherwise go to step 3.

Step 3. If there are remaining nodes in the rest of the network, let $k = k + 1$ and go to step 1. Or the decomposition is completed if there is no node left.

Figure 1 is an example of $k$-core decomposition. The $k$-core reflects the depth of the network, which is a medium-granularity scale parameter between local scale degree and global scale betweenness centrality to describe network characteristics.

4.2. Degree, $k$-Core, and Betweenness Centrality Based Analytical Hierarchy Process. The degree, betweenness centrality, and $k$-core can describe the importance of nodes on local, medium, and global scales. Therefore, we adopt a degree, betweenness centrality, and $k$-core based analytical hierarchy process (DBC-AHP) to rank the importance of nodes in the process of virus propagation in WSNs. Then we can locate the crucial node according to the rank list.

The DBC-AHP is divided into three layers. The highest layer is the target layer, which indicates the crucial nodes in the network. The second layer is the criterion layer, including node degree, $k$-core, and betweenness centrality of a node. The bottom layer is the object layer, corresponding to each node in the networks. Figure 2 illustrates the diagram of DBC-AHP.

In the analytical hierarchy process (AHP) [41], the relative importance comparison scales of each pair of criteria are shown in Table 1 [42]. In complex networks, the relative importance of node degree, $k$-core evaluation, and betweenness centrality indicators are as follows: compared with the node degree index, the betweenness centrality is the most important criterion, and $k$-core is slightly important [43–45]. In the criterion layer, we denote the three criteria of degree, $k$-core, and betweenness centrality as $c_1$, $c_2$, and $c_3$, respectively, so that indicators set is $C = \{c_1, c_2, c_3\}$. Then, we can structure a $3 \times 3$ pairwise comparison matrix as

$$A = (a_{ij})$$

$$= \begin{pmatrix}
  c_1 & c_2 & c_3 \\
  \frac{1}{7} & \frac{1}{3} & \frac{1}{5} \\
  \frac{1}{5} & \frac{1}{5} & \frac{1}{5}
\end{pmatrix}$$

Then we get the sum of each row and normalized it as

$$w = [0.083, 0.723, 0.193]^T.$$  

With $Aw = \lambda w$, we can get the largest eigenvalues $\lambda_{max} = 3.066$. And then, we can get the consistency of the judgment as $C.I. = \frac{\lambda_{max} - n/n - 1}{0.58} < 0.1$ and get $R.I. = 0.58$ by inquiring mean random consistency table. Through mentioned above, the judgment matrix satisfied the consistency condition. Eventually, the final weights of the three indicators are $w = [0.083, 0.723, 0.193]^T$.

If there are $N$ nodes in the WSN, the set of nodes in the object layer can be denoted as $A = \{a_1, a_2, \ldots, a_N\}$. Therefore, all the pairs of the $j$-th criterion $c_j$ and the $i$-th node $a_i$ composed of a judgment matrix, which is denoted as

$$X = \begin{pmatrix}
  a_1(s_1) & a_1(s_2) & a_1(s_3) \\
  a_2(s_1) & a_2(s_2) & a_2(s_3) \\
  \cdots & \cdots & \cdots \\
  a_N(s_1) & a_N(s_2) & a_N(s_3)
\end{pmatrix}.$$  

Each $a_i(s_j)$ can be normalized as
### 4.3. Time Complexity of DBC-AHP

The DBC-AHP can be divided into two steps: the first step is to calculate the values of degree, k-core, and betweenness centrality for each node. Then the second step is to sort the node importance according to the AHP.

For the first step, we analyze the time complexity of degree, k-core, and betweenness centrality of nodes. The calculation of node degree is straightforward, and its time complexity is related to the number of nodes n, that is, the complexity is \( O(\log(N)) \) [46]. The k-core has a low computational complexity with \( O(M) \) [46], where \( M \) stands for the links in the network. According to a fast method of calculating the betweenness centrality, the complexity of the unweighted graph is \( O(MN) \) [47]. In the first step, it is obvious that the stage with the highest time complexity is the calculation of betweenness centrality. For a network of average degree \( \langle k \rangle \), the number of edges is \( M = \langle k \rangle M/2 \). Therefore, the time complexity of the first step is determined by betweenness centrality with \( O(N^2) \).

In the second step, the time complexity of AHP is \( O(\min NC^2, N^2C) \) [48], where \( M \) stands for the number of nodes in the object layer and \( C \) stands for the number of criteria. In our application, the criteria is a constant \( C = 3 \), which refers to degree, k-core, and betweenness centrality. Therefore, the time complexity of AHP in our application is \( O(N) \).

Finally, considering the time complexity of the first and second steps, it can be found that the calculation of betweenness centrality has the highest time complexity. Therefore, the time complexity of DBC-AHP is \( O(N^2) \).

### 5. Numerical Results and Analysis

#### 5.1. Comparison of Four Virus Control Mechanisms in WSNs

We verify the efficiency of DBC-AHP by comparing virus propagation processes with/without various control mechanisms. Referring to our previous work on the research of virus propagation process in WSNs [15], assuming \( N = 1000 \) nodes are randomly distributed in a \( 100 \times 100 \) area, \( \alpha = 0.87 \), \( r_c = 7 \), the listening/sleeping duty ratio of link-layer is \( \tau = 0.6 \), and the infection probability \( \eta = 0.6 \) in this network topology. In our former work, \( \eta = 0.6 \) is the threshold for full virus outbreak in our network structure model, which means the virus cannot infect the entire network when \( \eta < 0.6 \) and only can infect the whole network when \( \eta \leq 0.6 \). The simulation was carried out in MATLAB with the graph theory framework MatlabBGL.

We add four virus control mechanisms to strengthen the immune ability of nodes in WSNs. From the perspective of a complex network, the immunity of a node is equivalent to the deletion of the node or the deletion of the edge of this node [49]. We contrastively analyze the effects of four virus control mechanisms based on node degree, betweenness centrality, k-core, and betweenness centrality.
centrality, $k$-core, and DBC-AHP separately for crucial node immunization. Taking the DBC-AHP index as an example, we rank the nodes in descending order and immunize them in proportion from high to low. Moreover, we also consider the listening/sleeping mechanism in MAC might affect the virus control process. The virus control mechanism comparison process is as follows: at the beginning, we add four types of virus control mechanisms in the virus propagation in WSNs. Then, we analyze the effect of four types of virus control mechanisms with the same node proportion by comparing the proportion of the $R$-state node after the virus propagation is over and the network is stable. The simulation results are illustrated in Figures 3 and 4.

The virus control mechanism aims to restrain the virus propagation and decrease the number of $I$-state node. The less of the infectious node means a better inhibitory effect of the virus; meanwhile, the curve is lower. We realize the four virus control mechanisms all can protect the node and improve the antiviral property of the network from Figures 3 and 4. However, the inhibitory effects of the four different virus control mechanisms are disparate. From the simulation result, the inhibitory effect can be divided into two categories. One group is the virus control mechanisms based on the node degree and $k$-core decomposition; the other group is based on the betweenness centrality and the DBC-AHP algorithm. The inhibitory effects of the former group are better than those of the latter group. This phenomenon indicates that global information is essential to inhibit the spread of the virus. However, local information can also take some effects supplementarily. As represented in Figure 4, the scales of virus propagation reduce with the listening/sleeping mechanism of the link layer. The inhibitory effect based on the betweenness centrality mechanism is slightly weak from that of the DBC-AHP mechanism. However, the effects of both are better than the other two methods. Whether with or without the listening/sleeping mechanism, the inhibitory effect based on the DBC-AHP algorithm exceeds the other three mechanisms.

According to the phenomena shown in Figures 3 and 4, the DBC-AHP algorithm has the best inhibition effect on virus propagation. Therefore, in the remaining part, we will discuss the influence of other factors on the virus propagation inhibition effects with the DBC-AHP algorithm.

5.2. Virus Propagation with the Control Mechanism of DBC-AHP. In order to understand the obstruction of virus control mechanism DBC-AHP to virus propagation comprehensively, we explore the dynamic processes with the
changes of $\langle k \rangle$, $r_c$, $\eta$, and the listening/sleeping mechanism of the link layer. Following is the default setting of network and virus propagation models: there are $N = 1000$ nodes distributed randomly in $100 \times 100$ area with $\alpha = 0.87$ and $\beta = 0.7$.

5.2.1. Average Node Degree $\langle k \rangle$. We observed the virus propagation processes with various $\langle k \rangle = 7, 10, 13$ and with or without DBC-AHP. Furthermore, we add the listening/sleeping mechanism of the link layer with $\tau = 0.6$ for comparison. The results of the simulation are shown in Figures 5 and 6.

As shown in Figures 5 and 6, the DBC-AHP can defend the virus effectively, especially in the network with listening/sleeping in MAC. Furthermore, the inhibition effect of DBC-AHP is inversely proportional to the average node degree $\langle k \rangle$. The smaller $\langle k \rangle$ is, the less proportion of removed node $R$ becomes, and the inhibition of the mechanism gets more obvious.

5.2.2. The Communication Radius of Nodes $r_c$. The communication radius $r_c$ of nodes is one of the influencing factors in virus propagation. We set $r_c = 6, 7, 8$ with or without DBC-AHP. Furthermore, we add the listening/sleeping mechanism of the link layer with $\tau = 0.6$ for comparison. The results of the simulation are shown in Figures 7 and 8.

We found that DBC-AHP can inhibit the virus propagation process with various $r_c$. We observed that the less the communication radius $r_c$ is, the less the number of infectious nodes becomes, and the inhibition of the mechanism gets stronger. Furthermore, the inhibitions of virus propagation are stronger with the listening/sleeping in MAC. Therefore, the DBC-AHP will be more effective in WSNs closer to the actual situation.

5.2.3. The Probability of Virus Infection $\eta$. The probability of virus infection $\eta$ reflects the ability of the virus. Different values of $\eta$ refer to different kinds of the virus. In this part, we verify the inhibition effect of DBC-AHP on viruses with different infection probabilities. We set $\eta = 0.4, 0.6, 0.8$ with or without DBC-AHP. Furthermore, we add the listening/sleeping mechanism of the link layer with $\tau = 0.6$ for comparison. The results of the simulation are shown in Figures 9 and 10.

![Figure 4: The comparison of the virus control mechanism with the listening/sleeping in MAC.](image-url)
As shown in Figures 9 and 10, DBC-AHP limits the speed of virus infection and the scale of infectious nodes with or without the listening/sleeping mechanism, which is already verified. The fewer the $\eta$ is, the less the number of infectious nodes become, and the inhibition of DBC-AHP is much better. Figures 9 and 10 show the inhibition effects of DBC-AHP with and without listening/sleeping mechanism. The results show that using DBC-AHP with listening/sleeping mechanism can effectively block the spread of virus. This indicates that the collective effect of DBC-AHP and the listening/sleeping mechanism in MAC would make the network safer.

5.3. Applying DBC-AHP in EDGF Networks. Furthermore, we verify the effectiveness of DBC-AHP in the network generated with the empirical data set generation framework (EDGF) without MAC [50]. The parameters of the network are grid-based deployment with node number $N = 160$, seed value $X[0] = 43$, constants $a = 3.359886$ and $c = 1.902161$, transmission range $TR = 15$, and deployment area $100 \times 100$.

Figure 11 shows infection scale under different infection probability with immune rate values of 5%, 10%, 25%, and 50% in EDGF networks. The immune strategy protects the nodes with large values of average degree, $k$-core, betweenness centrality, and DBC-AHP. In Figures 11(a)–11(d), the red line is the baseline without immune nodes. For example, in Figure 11(a), 95% of nodes are not protected by the virus control mechanism of immune, so the scale of virus propagation will not exceed 95% of nodes. In subfigures 11(a)–11(d), we found that when the proportion of immune nodes increases, the scale of virus infection will continue to decrease with the same value of infection probability $\eta$. Under various immune proportions, the protection results of DBC-AHP were similar to those of betweenness centrality, and the results were the best. The control mechanism of average degree has the worst effect. Under the DBC-AHP and betweenness centrality control mechanisms in Figure 11(b), even if $\eta = 1$, the virus still cannot infect all nodes in the network. The reason is that after those nodes based on DBC-AHP and betweenness centrality are protected, the network connectivity for virus propagation has been split. Therefore, there is
Figure 6: The effect of node degree on the virus control mechanism with the listening/sleeping mechanism of the link layer.
Figure 7: The effect of communication radius of nodes on virus control mechanism without the listening/sleeping mechanism.
Figure 8: The effect of communication radius of nodes on virus control mechanism with the listening/sleeping mechanism.
Figure 9: The effect of the probability of infection on the virus control mechanism without the listening/sleeping mechanism.
Figure 10: The effect of the probability of infection on the virus control mechanism with the listening/sleeping mechanism.

Figure 11: Continued.
always some nodes that will survive in this situation. In Figures 11(c) and 11(d), even if \( \eta = 1 \), the virus cannot infect all nodes under all four control mechanisms. In general, DBC-AHP has a good effect on identifying the crucial nodes in the virus propagation.

6. Conclusion

This paper proposes a virus control mechanism for DBC-AHP in WSNs. In DBC-AHP, we combine the node degree, betweenness centrality, and \( k \)-core comprehensively with AHP and get the rank of the node's importance. After implementing immune protection for crucial nodes, we finally reduce the speed and the scale of virus infection. DBC-AHP shows a better effect than a single indicator method in the context of virus defense in WSNs.

In future work, we can carry out some extended research on the virus control mechanism of WSNs. The DBC-AHP is highly dependent on the global index of betweenness centrality, and the time complexity is high. Therefore, we can find an alternative to betweenness centrality, such as the technology based on information entropy and so on. There are also some other virus control mechanisms in practical applications, such as routing-based mechanisms. Future research can start from the control mechanism and explore the inhibitory effects of other safety measures and other immune mechanisms on the spread of the virus.

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 that they have no conflicts of interest.

Acknowledgments

This research was supported by the “Pioneer” and “Leading Goose” R&D Program of Zhejiang (2022C03117), Zhejiang Postdoctoral Science Foundation (254824), National Natural Science Foundation of China (61602417), Basic Scientific Research Project of Zhejiang Sci-Tech University (2019Q042), and 521 Talent Project of ZSTU.

References

[1] J. Kleinberg, “The wireless epidemic,” Nature, vol. 449, no. 7160, pp. 287-288, 2007.
[2] S. Guan, J. Wang, C. Jiang, J. Tong, and Y. Ren, “Intrusion detection for wireless sensor networks: a multi-criteria game approach,” in Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6, IEEE, Barcelona, Spain, April 2018.
[3] H. El Alami and A. Najid, “Eca,” International Journal of Wireless Networks and Broadband Technologies, vol. 7, no. 2, pp. 19–37, 2018.
[4] H. El Alami and A. Najid, “Optimization of energy efficiency in wireless sensor networks and internet of things,” Nature-Inspired Computing Applications in Advanced Communication Networks, IGI Global, Hershey, PA, USA, 2020.
[5] J.-S. Lee, J. Portilla, G. Mujica, and Y.-H. Sun, "Experimental modeling and measurements of networked wireless sensors for power consumption," International Journal on Advances in Networks and Services, vol. 12, 2019.
[6] D. Yu, J. Kang, and J. Dong, "Service attack improvement in wireless sensor network based on machine learning,"
Microprocessors and Microsystems, vol. 80, Article ID 103637, 2021.

[7] S. Sharma and V. K. Verma, "Security explorations for routing attacks in low power networks on internet of things," The Journal of Supercomputing, vol. 77, no. 5, pp. 4778–4812, 2021.

[8] L.-P. Feng, H.-B. Wang, and S.-Q. Feng, "Improved sir model of computer virus propagation in the network," Jisuan Ji Ying Yong Journal of Computer Applications, vol. 31, no. 7, pp. 1891–1893, 2011.

[9] M. López, A. Peinado, and A. Ortiz, "An extensive validation of a sir epidemic model to study the propagation of jamming attacks against iot wireless networks," Computer Networks, vol. 165, Article ID 106945, 2019.

[10] D. Chen, X.-L. Ren, Q.-M. Zhang, Y.-C. Zhang, and T. Zhou, "Vital nodes identification in complex networks," Physics Reports, vol. 650, pp. 1–63, 2016.

[11] 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. 1775–1805, 2018.

[12] B. Liu, W. Zhou, L. Gao, H. Zhou, T. H. Luan, and S. Wen, "Malware propagations in wireless ad hoc networks," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 6, pp. 1016–1026, 2018.

[13] Q. Li, B. Zhang, L. Cui, Z. Fan, and V. V. Athanasios, "Epidemics on small worlds of tree-based wireless sensor networks," Journal of Systems Science and Complexity, vol. 27, no. 6, pp. 1095–1120, 2014.

[14] G. Liu, Z. Peng, Z. Liang, J. Li, and L. Cheng, "Dynamics analysis of a wireless rechargeable sensor network for virus mutation spreading," Entropy, vol. 23, no. 5, p. 572, 2021.

[15] L. Jiang, Q. Xu, H. Pan, Y. Dai, and J. Tong, "Virus Propagation in Wireless Sensor Networks with media Access Control Mechanism," Security and Communication Networks, vol. 2020, Article ID 6513920, 11 pages, 2020.

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

[17] C. Nwokoye, C. Umeugoji, and C. Umeh, "Evaluating degrees of differential infections on sensor networks' features using the sejir-v epidemic model," Egyptian Computer Science Journal, vol. 44, no. 3, 2020.

[18] S. Awasthi, N. Kumar, and P. K. Srivastava, "A study of epidemic approach for worm propagation in wireless sensor network," in Intelligent Computing in Engineering, pp. 315–326, Springer, Singapore, 2020.

[19] X. Fu, M. Small, D. M. Walker, and H. Zhang, "Epidemic dynamics on scale-free networks with piecewise linear infectivity and immunization," Physical Review, vol. 77, no. 3, Article ID 036113, 2008.

[20] W. Li, T. Guo, Y. Wang, and B. Chen, "Dr-scir public opinion propagation model with direct immunity and social reinforcement effect," Symmetry, vol. 12, no. 4, p. 584, 2020.

[21] L. Zhu and H. Zhao, "Dynamical behaviours and control measures of rumour-spreading model with consideration of network topology," International Journal of Systems Science, vol. 48, no. 10, pp. 2064–2078, 2017.

[22] L. Chen and D. Wang, "An improved acquaintance immunization strategy for complex network," Journal of Theoretical Biology, vol. 385, pp. 58–65, 2015.

[23] G. Xin and Z. H. Z. Jun, "Complex networks immune strategy based on acquaintance immunization," Comput. Sci, vol. 38, no. 11, pp. 83–86, 2011.

[24] Y. Wang, G. Xiao, J. Hu, T. H. Cheng, and L. Wang, "Imperfect targeted immunization in scale-free networks," Physica A: Statistical Mechanics and Its Applications, vol. 389, no. 12, pp. 2355–2356, 2009.

[25] C. Zhang and X. H. Huan, "Optimal control strategy for a novel computer virus propagation model on scale-free networks," Physica A: Statistical Mechanics and Its Applications, vol. 451, pp. 251–265, 2016.

[26] L. Xia, G. Jiang, Y. Song, and B. Song, "An improved local immunization strategy for scale-free networks with a high degree of clustering," The European Physical Journal B, vol. 90, no. 1, pp. 2–7, 2017.

[27] Z.-H. Zhang, G.-P. Jiang, Y.-R. Song, L.-L. Xia, and Q. Chen, "An improved weighted leadderrank algorithm for identifying influential spreaders in complex networks," in Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), pp. 748–751, IEEE, Guangzhou, China, July 2017.

[28] S. Li and F. Xiao, "The identification of crucial spreaders in complex networks by effective gravity model," Information Sciences, vol. 578, pp. 725–749, 2021.

[29] C. Guo, L. Yang, X. Chen, D. Chen, H. Gao, and J. Ma, "Influential nodes identification in complex networks via information entropy," Entropy, vol. 22, no. 2, p. 242, 2020.

[30] D. Puri and B. Bhushan, "Enhancement of security and energy efficiency in wsns: machine learning to the rescue," in Proceedings of the 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), pp. 120–125, IEEE, Noida, India, October 2019.

[31] H. Rathore and S. Jha, "Bio-inspired machine learning based wireless sensor network security," in Proceedings of the 2013 World Congress on Nature and Biologically Inspired Computing, pp. 140–146, IEEE, Fargo, ND, USA, August 2013.

[32] E.-Y. Yu, Y.-P. Wang, Y. Fu, D.-B. Chen, and M. Xie, "Identifying critical nodes in complex networks via graph convolutional networks," Knowledge-Based Systems, vol. 198, Article ID 105893, 2020.

[33] G. Zhao, P. Jia, A. Zhou, and B. Zhang, "Infsgcn: identifying influential nodes in complex networks with graph convolutional networks," Neurocomputing, vol. 414, pp. 18–26, 2020.

[34] A. Ullah, B. Wang, J. Sheng, J. Long, N. Khan, and Z. Sun, "Identification of nodes influence based on global structure model in complex networks," Scientific Reports, vol. 11, no. 1, pp. 6173–6211, 2021.

[35] D. Estrin, "Wireless sensor network network tuorial part iv: sensor network protocols," in Proceedings of the ACM Mobile Computing and Networking (MobiCom), Kasavanhalli, Karnataka, 2002.

[36] X. Wang and Y. 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.

[37] 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. 108, no. 3, pp. 1363–1377, 2019.

[38] M. Kitsak, L. K. Gallos, S. Havlin et al., "Identification of nodes influence based on global structure model in complex networks," Physica A: Statistical Mechanics and Its Applications, vol. 388, no. 11, pp. 83–86, 2011.
[40] D. Sn, "k-core organization of complex networks/sn dor-govtsev, av goltsev, jf mendes," *Physical Review Letters*, vol. 96, no. 4, Article ID 040601, 2006.

[41] E. K. Saito, S. Shea, A. Jones, G. Ramos, and M. Pitesky, "A cooperative approach to animal disease response activities: analytical hierarchy process (ahp) and vvibd in California poultry," *Preventive Veterinary Medicine*, vol. 121, no. 1-2, pp. 123–131, 2015.

[42] B. Liu, H. Tian, B. Wang, and B. Fan, "Ahp and game theory based approach for network selection in heterogeneous wireless networks," in *Proceedings of the 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, pp. 501–506, IEEE, Las Vegas, NV, USA, January 2014.

[43] K. Kanwar, S. Kaushal, and H. Kumar, "An ahp-topsis based framework for the selection of node ranking techniques in complex networks," in *Proceedings of the International Conference on Machine Learning, Image Processing, Network Security and Data Sciences*, pp. 527–542, Springer, Silchar, India, July 2020.

[44] X. Gao, Y. Liu, Y. Qiu, and H. Liu, "A comprehensive assessment method of asset importance for key asset protection," in *Proceedings of the 2019 the 9th International Conference on Communication and Network Security*, pp. 79–83, Chongqing, China, November 2019.

[45] T. Bian, J. Hu, and Y. Deng, "Identifying influential nodes in complex networks based on ahp," *Physica A: Statistical Mechanics and Its Applications*, vol. 479, pp. 422–436, 2017.

[46] S. Sun, X. Liu, L. Wang, and C. Xia, "New link attack strategies of complex networks based on k-core decomposition," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 12, pp. 3157–3161, 2020.

[47] M. Borassi and E. Natale, "Kadabra is an adaptive algorithm for betweenness via random approximation," *ACM Journal of Experimental Algorithmics*, vol. 24, pp. 1–35, 2019.

[48] R. K. Dewi, B. T. Hanggara, and A. Pinandito, "A comparison between ahp and hybrid ahp for mobile based culinary recommendation system," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 12, no. 1, p. 133, 2018.

[49] F. Nian, S. Ren, and Z. Dang, "The propagation-weighted priority immunization strategy based on propagation tree," *Chaos, Solitons & Fractals*, vol. 99, pp. 72–78, 2017.

[50] D. K. Sah, K. Cengiz, P. K. Donta, V. N. Inukollu, and T. Amgoth, "Edgf: empirical dataset generation framework for wireless sensor networks," *Computer Communications*, vol. 180, pp. 48–56, 2021.