Computers, Materials & Continua
DOI: 10.32604/cmc.2022.029367
Article

Tech Science Press

Network Invulnerability Enhancement Algorithm Based on WSN Closeness Centrality

Qian Sun[1,2], Fengbo Yang[1,2], Xiaoyi Wang[2,3], Jing Li[4,*], Jiping Xu[1,2], Huiyan Zhang[1,2], Li Wang[1,2], Jiabin Yu[1,2], Xiao Peng[1,2] and Ruichao Wang[5]

[1]School of Artificial Intelligence, Beijing Technology and Business University, Beijing, 100048, China
[2]Beijing Laboratory for Intelligent Environmental Protection, Beijing, 100048, China
[3]Beijing Institute of Fashion Technology, Beijing, 100029, China
[4]Smart City College, Beijing Union University, Beijing, 100101, China
[5]University College Dublin, Dublin4, Ireland
*Corresponding Author: Jing Li. Email: jingli@buu.edu.cn
Received: 01 March 2022; Accepted: 01 April 2022

Abstract: Wireless Sensor Network (WSN) is an important part of the Internet of Things (IoT), which are used for information exchange and communication between smart objects. In practical applications, WSN lifecycle can be influenced by the unbalanced distribution of node centrality and excessive energy consumption, etc. In order to overcome these problems, a heterogeneous wireless sensor network model with small world characteristics is constructed to balance the centrality and enhance the invulnerability of the network. Also, a new WSN centrality measurement method and a new invulnerability measurement model are proposed based on the WSN data transmission characteristics. Simulation results show that the life cycle and data transmission volume of the network can be improved with a lower network construction cost, and the invulnerability of the network is effectively enhanced.

Keywords: Wireless sensor networks; invulnerability; small world characteristics; heterogeneous nodes; node centrality

1 Introduction

The Internet of Things (IoT) and the Wireless Sensor Network (WSN) are currently combined to improve data transmission based on sensors in future applications [1]. WSN are considered to be one of the most important technologies in the 21st century. It will have a great impact on the future lifestyle of mankind. Information, intelligence and the interconnection of all things are closely related to it. WSN comprises a massive number of arbitrarily placed sensor nodes that are linked wirelessly to monitor the physical parameters from the target region [2]. WSN are used in many fields because of their low cost and easy deployment [3]. These sensors are battery-driven and resource-restrained devices that consume most of the energy in sensing or collecting the data and transmitting it [4]. The node failure is considered as one of the main issues in the WSN which creates higher packet drop, delay, and energy consumption during the communication [5]. Although the number of sensor nodes

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

in wireless sensor networks is huge, it is easy to fail. It is very easy to cause the original connected network topology segmentation due to the failure of some nodes in the network, which greatly reduces the network coverage and even makes the network invalid [6]. Wireless sensor networks often lead to node failure due to energy depletion, hardware failure or intrusion, which divides the original connected network topology and even leads to the damage of the global network. Therefore, studying the invulnerability of wireless sensor networks has important theoretical value to solve the bottleneck of large-scale application of wireless sensor networks [7]. Network invulnerability measures the ability of the system to provide reliable services in a sustainable and stable manner [8].

Small world network has both short average path length and high clustering coefficient. In sensor networks, the small average path length means that nodes only need less hops and energy when transmitting data to sink [9]. The large clustering coefficient means that the propagation range of local information in the network is relatively wide and the connection between local nodes is relatively close, which makes the data in the network redundant to a certain extent. Therefore, a larger clustering coefficient can improve the fault tolerance of the network and prolong the lifecycle of the network. Therefore, we build a heterogeneous wireless sensor network routing algorithm with small world characteristics to prolong the network life cycle, increase the amount of network data transmission and enhance the invulnerability of wireless sensor networks. The first problem we need to solve is how to determine the location and number of heterogeneous nodes.

2 Related Works

Wireless sensor nodes are generally deployed in complex environments, which are prone to network failure due to malicious attacks and their own energy depletion. Therefore, how to enhance the invulnerability of wireless sensor networks has become a hot topic in WSN. There are many researches on WSN secure routing protocol. Various experts and scholars study how to better prolong the network life cycle and improve the network security transmission index from various angles.

In Sun's paper, a small-world network model is introduced for water quality sensor networks. The energy consumption of the relay nodes near the heterogeneous node is too great, and as such the energy threshold and non-uniform clustering are constructed to improve the lifecycle of the network. Simulation results show that, compared with the low-energy adaptive clustering hierarchy routing algorithm and the best sink location clustering heterogeneous network routing algorithm, the proposed improved routing model can effectively enhance the energy-utilization. The lifecycle of the network can be extended and the data transmission amount can be greatly increased [10]. In Zhang's paper, the scale-free network in complex networks is taken as the research object, and the industrial WSN with scale-free characteristics is modeled. Based on the advantages of the fireworks algorithm, such as strong searching ability and diversity of population, a so-called fireworks and particle swarm optimization (FWPSO) algorithm is proposed, which can improve the global search ability and convergence speed effectively. The proposed FW-PSO algorithm is used to optimize the network topology and form a network with the largest natural connectivity, which can effectively promote the ability of network to resist the cascade failure problem [11]. Fu has built a cascading model of clustering WSNs by introducing the concept of sensing load and relay load. We discuss the impacts of model parameters on network invulnerability and evaluate the invulnerability performance of two types of WSN topologies, i.e., scale-free network and random network. Simulation and theoretical results show that the network invulnerability is negatively related to the proportion of cluster heads and positively related to the allocation coefficient. When the degree of each sensor node bears a linear relationship with its initial load, the network invulnerability is strongest [12]. Zhao accorded

to scale-free and small-world features of complex networks, the nodes of WSNs are divided into different types, including common node, super node, and sink node. From the point of view of invulnerability in complex networks, the influence of different types of nodes on the sensor networks' invulnerability is analyzed. Simulation experiments show that adding super nodes to the WSNs would significantly improve network invulnerability [13]. In wang's paper, according to the event level and the node energy of the sensor networks, the nodes' types are defined, which can help to determine the cluster node. Then, an event driven routing protocol (EDRP) is proposed, which considers the event information and the remaining energy of the whole network. Simulation results show that, compared with distributed energy-efficient clustering algorithm, EDRP can reduce the overall energy consumption of the network by 138%–172%, based on different kinds of events. Besides, EDRP can effectively prolong the life cycle and greatly increase the amount of data transmission of the network [14]. Aiming at the serious impact of the typical network attacks caused by the limited energy and the poor deployment environment of wireless sensor network (WSN) on data transmission, a trust sensing-based secure routing mechanism (TSSRM) with the lightweight characteristics and the ability to resist many common attacks simultaneously is proposed in this paper, at the same time the security route selection algorithm is also optimized by taking trust degree and QoS metrics into account. Performance analysis and simulation results show that TSSRM can improve the security and effectiveness of WSN [15]. In 1998, Watts and Strogatz proposed a network model, which shows that rewiring several links in a regular ring grid graph (the end point of the rewiring link is randomly selected from the graph) can greatly reduce the average path length between any two nodes in the graph, while still maintaining a high degree of clustering in adjacent nodes [16].

The so-called small world network is a network model with shorter average path length and larger clustering coefficient compared with the random network of nodes of the same scale. Previously, people believed that networks were divided into completely regular networks and completely random networks, which have their own characteristics. Regular networks have larger average path length and larger clustering coefficient, while random networks have smaller average path length, but smaller clustering coefficient. In addition, many real networks, such as power grid, transportation network, brain neural network, social network and food chain, show the characteristics of small world, that is, they have both short average path length and large clustering coefficient. In this paper, considering the small world characteristics of small world networks, we construct wireless sensor networks with small world characteristics, and further explore the optimization strategy of network construction.

When studying the network invulnerability, it is necessary to accurately evaluate the impact of different node failures and network damage types on the network invulnerability. When using the network construction method to improve the invulnerability of the network, we need to measure the effectiveness of the improvement. Network invulnerability measurement, as a specific quantitative index to measure the advantages and disadvantages of network invulnerability, has always been a hot spot in the research field of complex network invulnerability.

In Zhu's paper, they classify the coverage problem from different angles, describe the evaluation metrics of coverage control algorithms, analyze the relationship between coverage and connectivity, compare typical simulation tools, and discuss research challenges and existing problems in this area [17].

In Fu's paper, they show that the invulnerability of WSNs can be improved by introducing two new elements: super wires and super nodes. Moreover, on the basis of the definition of a novel centrality measurement, they propose two layout schemes based on super wires and super nodes for enhancing network invulnerability [18].

We propose a new centrality measurement method for wireless sensor networks, determine the location and number of heterogeneous nodes according to the new centrality measurement method, and propose an invulnerability measurement model. The proposed scheme can improve the invulnerability of the network with low network construction cost.

3 Measurement of WSN Centrality

Due to the unequal characteristics of wireless sensor networks, some key nodes determine whether the whole network can operate normally. In order to improve the invulnerability of the network, the most effective method is to improve the centrality of non critical nodes. The essence of the optimization scheme is to improve the importance of non critical nodes, so as to improve the invulnerability. In complex network theory, we usually call the importance of nodes centrality [19]. Different networks need different metrics to measure the centrality of nodes. Typical centrality measures include degree centrality, closeness centrality and betweenness centrality.

Degree centrality, as the earliest and simplest centrality measure, is defined as the number of connections a node has, and this centrality is always interpreted as the direct influence of a node in a static network. The formula for calculating the degree centrality in a network with n nodes is shown in Eq. (1):

$$K_d(x) = \frac{d(x)}{n-1} \tag{1}$$

where $K_d(x)$ is the degree centrality of the point, $d(x)$ is the number of connections between the point and other nodes.

Closeness centrality, reflects the degree to which a node is close to the center of the network. Due to the time consumption of information transmission, the information sent by the node in the center of the network takes the shortest time to spread to each node of the whole network. Therefore, the closer the node is, the shorter the time it takes for the node of the whole network to receive the information of the node, and the greater its importance. The closeness centrality of the shortest path we focus on (closeness centrality for short) refers to the closed centrality of a vertex in the graph, which is the reciprocal of the average shortest path distance from the vertex to any other vertex in the graph [20]. The formula for calculating the closeness centrality in a network with n nodes is shown in Eq. (2):

$$C_n(x) = (n-1)\left[\sum_{y=1}^{n} d_{xy}\right]^{-1} \tag{2}$$

where $C_n(x)$ is the closeness centrality of the point, $\sum_{y=1}^{n} d_{xy}$ is the sum of the average shortest path distance from the point to all other nodes.

The betweenness centrality is a measure of the centrality of nodes in the network. It is usually calculated as the score of the shortest path between node pairs passing through the node of interest. In a sense, betweenness centrality is a measure of the impact of nodes on the dissemination of information in the network [21]. By calculating the number of all the shortest paths passing through a node in the network, it reflects whether the node is in an important position of information dissemination in the network. The larger the number of nodes is, the greater the information flow of the node is, and the position of the node in the whole network is relatively more critical. Betweenness centrality is a measure of the centrality of nodes in the network, which is equal to the number of shortest paths

from all vertices to all other vertices passing through the node. The betweenness centrality of node x is shown in Eq. (3):

$$C_b(x) = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}} \tag{3}$$

where $C_b(x)$ is the betweenness centrality of the point, $\sum_{s \neq v \neq t} \sigma_{st}$ is the number of shortest paths of all node pairs, $\sum_{s \neq v \neq t} \sigma_{st}(v)$ is the number of paths passing through this point in all these paths.

However, due to the existence of sink nodes, wireless sensor networks are a kind of data aggregation network. These classical centrality measurements can't show the different importance of different nodes in the whole network. A typical cluster topology of wireless sensor networks is shown in Fig. 1.

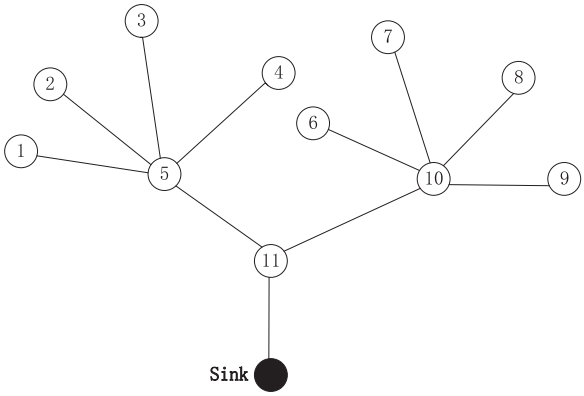

Figure 1: Typical cluster structure of WSN

According to the above centrality measurement method, we calculate the centrality of each node in Fig. 1, as shown in Tab. 1.

Table 1: Comparison of multiple centrality measures

Node	Degree centrality	Closeness centrality	Betweenness centrality	WSN closeness centrality
1∼4, 6∼9	0.09	0.35	0	0.33
5, 10	0.45	0.52	0.51	0.5
11	0.27	0.58	0.64	1

It can be seen from Tab. 1 that the most important importance of node 11 can't be explained according to the measurement of degree, closeness and betweenness centrality. If node 11 stops working, the whole network will collapse, and 50% of the nodes in the network can still work normally in the face of node 5 or node 10 failure. Although the centrality of nodes 5 and 10 is very high, in fact, node 11 is much more important than node 5, node 10 and other nodes. The fundamental reason is that these three centrality measurement methods don't take into account the actual situation of wireless sensor networks. Wireless sensor networks are data transmission centric networks, and the data perceived by all nodes must be transmitted to sink nodes.

Therefore, based on the closeness centrality, we propose a new centrality measurement method, called WSN closeness centrality, which is defined as the reciprocal of the shortest path distance from this point to sink node in wireless sensor networks. WSN closeness centrality is one of the indicators to measure the importance of nodes. It reflects the shortest path distance from the sink node when transmitting data. For directed networks, when data is transmitted in different directions, the shortest path will also change, resulting in differences in the stability and packet delivery success rate when the node transmits data to the sink node. In the process of data transmission, making the WSN closeness centrality of network nodes uniformly is a main strategy to enhance the invulnerability of wireless sensor networks. Whether there are optional redundant links between nodes is the main reason for the invulnerability of the network. Therefore, WSN closeness centrality reflects the role and influence of corresponding nodes in the whole network.

WSN closeness centrality is shown in the following Eq. (4):

$$C = \frac{1}{d_{is}} \tag{4}$$

where d_{is} is the shortest path distance from node i to sink node, Data is transmitted unidirectionally from node i to sink node. In a network with $n(n \geq 2)$ nodes, as shown in Fig. 1, In an extreme case, each shortest path from any other node except node 11 to sink node passes through node 11, therefore, except that the shortest distance from node 11 to sink node is 1, the shortest distance from other nodes to sink node is greater than 1. Therefore, the WSN compactness centrality of node 11 is 1. From Tab. 1, WSN closeness centrality accurately reflects the centrality of the network. The centrality of node 11 is twice that of node 5 and node 10, and the centrality of other nodes is 0.333. It indicates that the failure of node 11 will affect the normal operation of all other nodes and make the network crash and failure.

4 Analysis of Small World Characteristics of Heterogeneous Sensor Networks

4.1 Structure of Heterogeneous Sensor Networks

If heterogeneous nodes with higher energy are deployed at the cluster head in the sensor network, or a certain number of heterogeneous nodes are deployed in the network in an appropriate way, cluster with the heterogeneous nodes as the center, and then the heterogeneous nodes are responsible for receiving the data of the member nodes in the cluster, processing it and sending it to the sink node, the ordinary nodes in the cluster only need to transmit over a short distance, The data can be transmitted to heterogeneous nodes. Because heterogeneous nodes have higher energy, this method can effectively save energy and improve the network life cycle. Generally, the structure of heterogeneous sensors is shown in Fig. 2. Ordinary nodes are only responsible for sending data to heterogeneous nodes, and then heterogeneous nodes communicate with each other to send data to sink nodes.

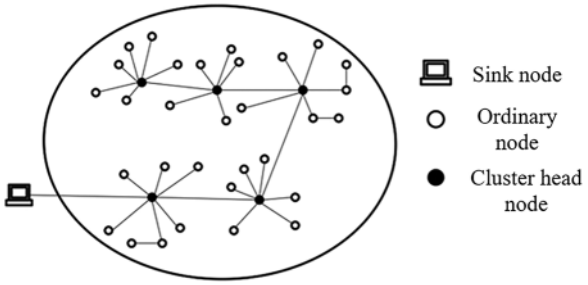

Figure 2: Structural diagram of heterogeneous sensor networks

4.2 Small World Characteristics of Heterogeneous Sensor Networks

Average path length and clustering coefficient are two important indicators to describe small world networks. Small world networks have both short average path length and large clustering coefficient.

In sensor networks, small average path length means that nodes only need less hops and energy to transmit data to sink nodes. The large clustering coefficient means that the local information dissemination range in the network is relatively wide and the connection between local nodes is relatively close. This local effect can have a great impact on the whole network and make the data in the network redundant. Therefore, a larger clustering coefficient can improve the fault tolerance of the network, and can continue to maintain the smooth communication of the network after some nodes fail, so that the performance of the network is not affected and the life cycle of the network is prolonged. Therefore, heterogeneous nodes that can communicate directly with sink nodes are introduced, and the super link formed between heterogeneous nodes and sink nodes is used as a shortcut to construct heterogeneous networks with small world effect, so as to improve the invulnerability of wireless sensor networks.

5 Construction of Small World Network Model Based on WSN Closeness Centrality (WSNCC Algorithm)

5.1 The Main Problems of Constructing Heterogeneous Sensor Networks with Small World Characteristics

(1) Optimize the deployment of heterogeneous nodes. If the same number of heterogeneous nodes are deployed in different ways, the improvement of network performance is very different. Therefore, when setting up heterogeneous networks, we must construct a better heterogeneous node location deployment algorithm according to the network distribution characteristics and topology.

(2) Under the condition of meeting the network performance requirements, the fewer heterogeneous nodes are required, the better. In heterogeneous sensor networks, compared with ordinary nodes, heterogeneous nodes have obvious advantages in power energy, computing power and communication capacity, but the cost of heterogeneous nodes is relatively expensive. Therefore, when setting up heterogeneous sensor networks, we must consider the network cost and can't add heterogeneous nodes indefinitely.

5.2 Heterogeneous Node Location Optimization Deployment Model

DEEC algorithm is a clustering algorithm to balance the energy of multi-level heterogeneous networks. Its main principle is to select the cluster head in a probabilistic manner according to the ratio of the residual energy of each node to the average energy of the network. Because the initial energy and residual energy of each node are different, the time when a node is selected as a cluster head is different. Nodes with high initial energy and residual energy are more likely to be selected as cluster heads than nodes with low energy, so as to realize the balance of network energy and improve the life cycle of the network [22].

After the nodes in the network are clustered by DEEC algorithm, the ordinary nodes transmit the collected data to the cluster head of the cluster. The cluster head processes the received data centrally, which can not only save energy consumption, but also increase the amount of data transmission. With the progress of clustering, the transmission path of network nodes will change accordingly with different nodes selected as cluster heads, so as to make the energy consumption of the network more uniform and enhance the invulnerability of the network.

Before the heterogeneous nodes are deployed in the network, the data of all nodes has only one transmission direction, that is, the data is transmitted to sink. Therefore, it will cause the problems of uneven distribution of network centrality and low network invulnerability. In order to solve this problem, this paper constructs a small world wireless sensor network by introducing heterogeneous nodes that can communicate directly with sink nodes. The node has a transmission direction other than sink node, that is, the node can transmit data to nearby heterogeneous nodes, and then the heterogeneous nodes can transmit data to sink. The energy of heterogeneous nodes can be supplemented, so the energy consumption can't be considered. After clustering the nodes in the network by DEEC algorithm, the WSN closeness of each cluster head is calculated by formula (4) proposed in this paper, and they are sorted from large to small.

The first heterogeneous node is arranged in the center of the region with the smallest WSN closeness, that is, the midpoint of the connection between the node with the smallest WSN closeness and the node with the second smallest WSN closeness. So as to achieve the purpose of uniform network centrality, and then enhance the invulnerability of the network.

After the above steps, this paper assumes that the initial position of the first heterogeneous node is $h(u_c, v_c)$, After the nodes deployed in the network are clustered according to the DEEC algorithm, there are n cluster head nodes whose positions are v_i (x_i, y_i), $i = 1, 2, \ldots, N$, the location of the sink node is (x_m, y_m). The data transmission mode of cluster head node is divided into multi hop transmission mode directly adopted by cluster head node to transmit data to sink node or to sink node through super link.

The data transmission mode of the cluster head node is determined according to the transmission distance d_i^h from the cluster head node to the heterogeneous node and the transmission distance d_i^s from the cluster head node to the sink node. When $d_i^s \geq d_i^h$, the cluster head node transmits the data to the sink node through the super link between the heterogeneous node and the sink node; When $d_i^s < d_i^h$, the cluster head node directly transmits multi hop to the sink node. For example, cluster head node v_1, the distance to sink node through multi hop transmission is less than that to heterogeneous nodes. Therefore, it directly transmits data to sink node through multi hop transmission, as shown in Fig. 3.

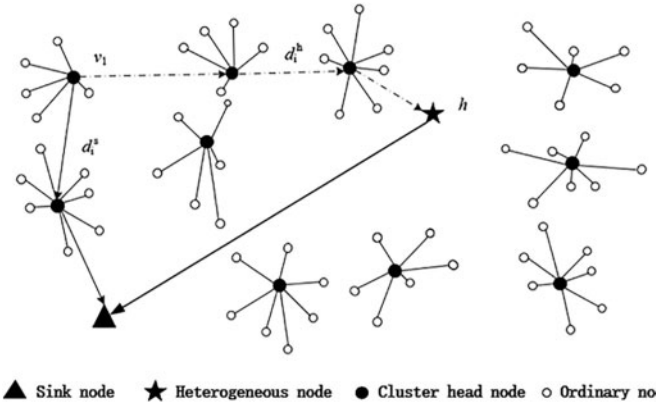

Figure 3: Data transmission mode of cluster heterogeneous network

Suppose that S luster head nodes in the network directly transmit data to sink nodes through multi hop transmission, and H cluster head nodes transmit data to sink nodes through super links, meeting the requirement of $H + S = N$.

When S cluster head nodes directly multi hop transmit data to sink, cluster head node v_i finds the shortest transmission path to transmit data to sink node through greedy algorithm (the cluster head node closest to sink node among all neighbor cluster head nodes is selected as the next hop), and sets the distance from cluster head node v_i to transmit data to sink node as d_i^s. Label the relay cluster head node in the transmission path, assuming that there are j relay cluster head nodes whose coordinates are (γ_n, δ_n), $n = 1, 2, \ldots, j$. The transmission distance Eq. (5) is as follows:

$$d_i^s = \begin{array}{l} \sqrt{(x_i-\gamma_1)^2+(y_i-\delta_1)^2}+\sqrt{(\gamma_1-\gamma_2)^2+(\delta_1-\delta_2)^2}+\cdots \\ +\sqrt{(\gamma_{j-1}-\gamma_j)^2+(\delta_{j-1}-\delta_j)^2}+\sqrt{(\gamma_j-x_m)^2+(\delta_j-y_m)^2} \end{array} \tag{5}$$

Similarly, when H cluster head nodes v_i transmit data to sink node through the super link of heterogeneous node, cluster head node v_i also finds the shortest transmission path from all neighbor cluster head nodes to heterogeneous node h through greedy algorithm, and sets the distance between cluster head node v_i and heterogeneous node h as d_i^h. When the data is transmitted to heterogeneous node, heterogeneous nodes then transmit data to sink nodes through super links. Label the relay cluster head node in the transmission path. It is assumed that there are l relay cluster head nodes with coordinates of (α_n, β_n), $n = 1, 2, \ldots, l$. The transmission distance Eq. (6) is as follows:

$$d_i^h = \begin{array}{l} \sqrt{(x_i-\alpha_1)^2+(y_i-\beta_1)^2}+\sqrt{(\alpha_1-\alpha_2)^2+(\beta_1-\beta_2)^2}+\cdots \\ +\sqrt{(\alpha_{l-1}-\alpha_l)^2+(\beta_{l-1}-\beta_l)^2}+\sqrt{(\alpha_l-u_c)^2+(\beta_l-v_c)^2} \end{array} \tag{6}$$

According to the data transmission mode of cluster head node, the corresponding WSN closeness centrality of cluster head node is calculated. When $d_i^s \geq d_i^h$, the cluster head node transmits the data to the sink node through the super link between the heterogeneous node and the sink node. At this time, $d_{is} = d_i^h$; When $d_i^s < d_i^h$, the cluster head node directly transmits multi hop to the sink node. At this time, $d_{is} = d_i^s$. Then, according to the WSN closeness centrality Eq. (4) proposed in this paper, the corresponding WSN closeness centrality values are calculated and sorted from high to low.

Finally, this paper adds a second heterogeneous node at the midpoint of the cluster head node with the smallest WSN closeness centrality value and the second smallest. The two heterogeneous nodes and sink nodes can directly establish a shortcut to communicate through two, as shown in Fig. 4. Thus, the WSN closeness centrality of most nodes with small WSN closeness centrality in the network is improved, so as to uniform the overall centrality of the network, reduce the importance of a few important nodes, and improve the invulnerability of the network.

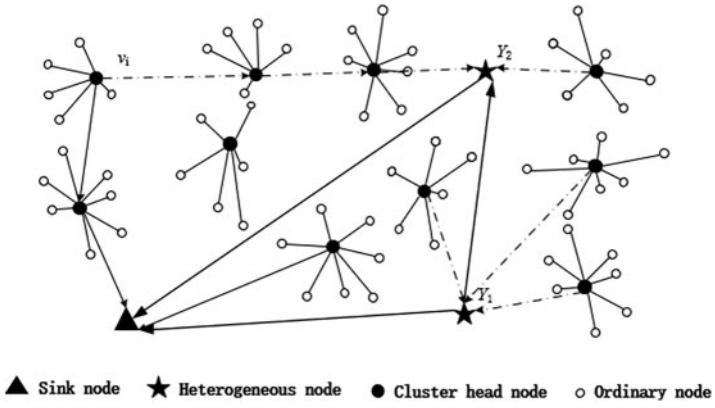

Figure 4: Deployment diagram of heterogeneous nodes in clustered network

5.3 Determination of the Optimal Number of Heterogeneous Nodes

When building heterogeneous sensor networks, if the total cost of the network fluctuates to a certain extent, but the network performance is required to reach a certain standard, then we need to consider how to minimize the cost of the network while the network performance reaches the standard. In this case, the determination of the optimal number of heterogeneous nodes is related to the specific performance requirements of sensor networks. Usually, the closeness centrality is an important factor affecting the network performance, and the WSN closeness centrality can be measured as a standard. The following discusses how to determine the minimum number of heterogeneous nodes in heterogeneous sensor networks when the WSN closeness centrality of cluster head nodes to sink nodes or heterogeneous nodes is used as a standard.

In heterogeneous networks, set the total number of cluster head nodes as N, and find the shortest distance from cluster head node v_i to sink node or heterogeneous node as d_i, The mean value of network WSN closeness centrality $\overline{C}$ is shown in Eq. (7).

$$\overline{C} = \frac{1}{N}\sum_{i=1}^{N}\frac{1}{d_i} \tag{7}$$

where d_i is the shortest distance from node v_i to sink or heterogeneous nodes. Because the mean value of WSN closeness centrality is different when adding different numbers of heterogeneous nodes. The number of heterogeneous nodes in the network is positively correlated with the WSN closeness centrality. Assuming that the average WSN closeness centrality between nodes to sink or heterogeneous nodes required by the network $\overline{C} \geq r_0$, r_0 is a given constant value set according to the network scale and performance requirements. If the network performance requirements are high, the value of r_0 is set to be large. Conversely, the value of r_0 is set smaller. The minimum number of heterogeneous nodes required to meet the requirements of network performance and invulnerability is $\beta_{\min}$.

Further research shows that different application scenarios have different requirements for the performance of wireless sensor networks, including the number of deployed nodes, the amount of data transmission, the life cycle, and the invulnerability performance when attacked.

It can be seen from the above analysis that the minimum number of heterogeneous nodes $\beta_{\min}$ required to meet the centrality mean value of WSN closeness $\overline{C} \geq r_0$. Based on the optimization deployment algorithm of heterogeneous node location, the calculation can be carried out through comparison and iteration. The specific steps of the algorithm are as follows:

Step 1: assign an initial value, and set the number of heterogeneous nodes to be added $m = 1$.

Step 2: $\beta = m$, use the network according to the transmission distance d_i^h from the N cluster head node to the heterogeneous node and the transmission distance d_i^s to the sink node, According to the WSN closeness formula (4) proposed in this paper, the corresponding values of WSN closeness centrality are calculated, and they are sorted from high to low. Then add the next heterogeneous node at the midpoint of the connection between the cluster head node with the smallest value of WSN closeness centrality and the second smallest. All heterogeneous nodes can directly establish a shortcut to communicate with sink nodes.

Step 3: calculate the mean value of network WSN closeness centrality $\overline{C}$.

Step 4: if $\overline{C} \geq r_0$ is satisfied, stop the iteration, and take $\beta_{\min} = \beta$.

Step 5: otherwise, make $m = m + 1$ and turn to step 2.

The value $\beta_{\min}$ obtained by the above iterative algorithm is the minimum number of heterogeneous nodes required to meet $\overline{C} \geq r_0$. Generally, when the distance from the cluster head node to the heterogeneous node or sink node is within one hop, the energy consumption is minimized and the invulnerability is greatly improved. Therefore, here $r_0 \leq \frac{1}{R}$, where R represents the maximum communication radius of the cluster head node.

6 WSN Invulnerability Measurement Model

Part of the invulnerability of WSN is defined as the ability of network topology to maintain connectivity when nodes or edges in the network fail or are attacked [23].

Next, the invulnerability measurement model is built, and the distribution functions of WSN closeness centrality and degree centrality of the network are given. In the network $G = (V, E)$, let the number of nodes in the network be n and the number of nodes with degree K be $n(K)$. Then the degree distribution of the network is shown in Eq. (8).

$$P_K = \frac{n(K)}{n}, \sum_{k=k_{\min}}^{k\max} P(k) = 1 \tag{8}$$

In the network $G = (V, E)$, let the number of nodes in the network be n and the number of nodes with WSN closeness C be $n(C)$. Then the WSN closeness distribution of the network is shown in Eq. (9).

$$P_C = \frac{n(C)}{n}, \sum_{C=C_{\min}}^{C\max} P(C) = 1 \tag{9}$$

When the WSN density centrality and degree centrality of the network are evenly distributed, the invulnerability of the network can be enhanced.

Firstly, according to the concept of variance, we characterize the fluctuation centrality of network node, and calculate the fluctuation WSN closeness centrality of network and degree centrality respectively, the following Eqs. (10) and (11) are shown:

$$B(K)=\frac{\sum_1^n (K_i - \overline{K})^2}{n} \tag{10}$$

where, i is the node number, n is the total number of nodes in the network, K is the node degree, $\overline{K}$ is the degree average value of network.

$$B(C)=\frac{\sum_1^n (C_i - \overline{C})^2}{n} \tag{11}$$

where, i is the node number, n is the total number of nodes in the network, and C is the WSN closeness centrality, $\overline{C}$ is the average WSN closeness of the network.

$B(C)$ in Eq. (11) is the fluctuation degree of network WSN closeness to measure the fluctuation of node WSN closeness. If the fluctuation degree $B(C)$ is large, it indicates that the WSN closeness centrality distribution of the network is uneven. When the nodes with high centrality of this kind of network are attacked or energy is exhausted, it will cause great harm to the network and even make the global network ineffective. On the contrary, it shows that the centrality of the network is evenly distributed. The node centrality of this kind of network is generally high. When the node is attacked or energy is exhausted, it will not cause great harm to the network and enhance the invulnerability of the network.

In the same way, $B(K)$ in Eq. (10) is the fluctuation degree of network degree centrality, which is composed of the difference between the degree of a single node and the average degree of all nodes. If the fluctuation degree of network degree centrality $B(K)$ is large, it indicates that the degree centrality of the network is not uniformly distributed. When the nodes with high centrality of this type of network are attacked or their energy is exhausted, it will cause great harm to the network, and even make the entire network invalid. On the contrary, it means that the centrality of the network is evenly distributed. The node centrality of this type of network is generally high. When the node is attacked or the energy is exhausted, it will not cause great harm to the network, so that the network's invulnerability is enhanced.

Node degree K is the first proposed measurement method, which is related to the connection degree of nodes. Adding degree centrality to the model establishment of invulnerability measurement can effectively balance the defects and deficiencies caused by only considering the closeness centrality of WSN. The existence of nodes with large degree of centrality can ensure network traffic and avoid network congestion. The size of neighbor network and the number of data transmission paths affect the ability of network information transmission and resisting attacks. In directed networks, the centrality of node degree determines the stability and invulnerability of directed data transmission system, which is an important standard to measure the invulnerability of networks.

From the perspective of whether the centrality distribution is uniform, combined with the two factors of WSN closeness centrality and degree centrality of the network, this paper constructs an invulnerability measurement model to measure the importance of nodes and their impact on the network invulnerability, as shown in Eq. (12).

$$T = \frac{1}{n(B(K) + B(C))} + \overline{C} \tag{12}$$

where $\overline{C}$ is the average WSN closeness of the network, and $B(C)$ is the fluctuation degree of WSN closeness of the network, $B(K)$ is the fluctuation degree centrality of network, n is the total number of cluster head nodes.

According to Eq. (12), the invulnerability measure T has a negative correlation with the fluctuation of the node's WSN closeness centrality and the node's degree centrality fluctuation. It is positively correlated with the average WSN closeness of the network. In traditional wireless sensor networks, the degree centrality and WSN closeness centrality of most nodes are small, the degree centrality and WSN closeness centrality of a small number of nodes are large, the network centrality distribution is uneven, and the average WSN closeness of the network is small, so the invulnerability measure T is small. Such networks have strong invulnerability in the face of random attacks and poor invulnerability in the face of selective attacks. On the contrary, when the network centrality is uniform enough and the average WSN closeness is large, the invulnerability measure T is large, and the network has strong invulnerability to node loss and selective attacks.

Heterogeneous sensor networks with small world effect are constructed by introducing heterogeneous nodes that can establish a shortcut to communicate with sink nodes. Due to the addition of heterogeneous nodes, the data transmission mode of nodes is divided into the multi hop transmission mode directly adopted by cluster head nodes to transmit data to sink nodes or to sink nodes through super links. The data transmission of nodes has another choice other than sink nodes. Therefore, the average path of data transmission is shortened, and the increased connection between nodes increases the clustering coefficient. Further, while improving the WSN closeness C of the node, the node's WSN closeness centrality distribution is more uniform. Similarly, the network improves the node degree K

and makes the node's degree distribution more uniform. That is, by building a small world network model, the invulnerability of the network is improved.

7 Simulation Analysis and Discussion

The ultimate purpose of the WSNCC algorithm proposed in this paper is to improve the energy utilization of the network and prolong the life cycle of the network. In the simulation analysis, this paper not only compares the common network invulnerability measurement models, such as the number of dead nodes (life cycle), data transmission and energy consumption, but also simulates and compares the WSN closeness and invulnerability measurement T proposed in this paper.

Use MATLAB to simulate WSNCC algorithm and DEEC algorithm, deploy 100 sensor nodes, and set other conditions of sensor network in the monitored area as follows.

1) The energy of ordinary nodes is limited, and sink is located in the monitoring area, and the energy can be supplemented;
2) Each node has an independent ID number;
3) Each node has the ability to sense and transmit data.

The network simulation parameter settings are shown in Tab. 2.

Table 2: Network simulation parameters

Parameter name	Parameter value
Network area	100 m × 100 m
Number of nodes	100
Sink node coordinates	(50, 50)
Number of routing execution rounds	5000
Node initial energy	0.5 J
Energy consumption ERX of transmitting ETX and receiving circuit	5 × 10^−8 J
Energy consumption of power amplifier circuit E_{mp}	1.3 × 10^−13 J

The number of dead nodes of the network indicates that the dead nodes of the whole network change with the operation of the network. It is an important indicator, which can intuitively display the length of the network life cycle. It can be seen from Fig. 5 that the node death speed of WSNCC algorithm is much slower than that of DEEC algorithm. The death of all nodes of WSNCC algorithm is round 4952, while the death of all nodes of DEEC algorithm is round 2857, That is, the life cycle of WSNCC algorithm is 57.6% longer than that of DEEC algorithm.

The amount of network data transmission is an important indicator to measure whether the performance of wireless sensor networks is superior. The amount of data transmission determines the accuracy and application way of data analysis. A large amount of data transmission can make the realization of functions more effective. Fig. 6 shows the data transmission volume of WSNCC algorithm and DEEC algorithm. After calculation, WSNCC algorithm transmits 183519 bit data in total after 5000 iterations. Compared with 70082 bit data transmitted by DEEC algorithm, it transmits 113437 bit more data, that is, 1.62 times more data.

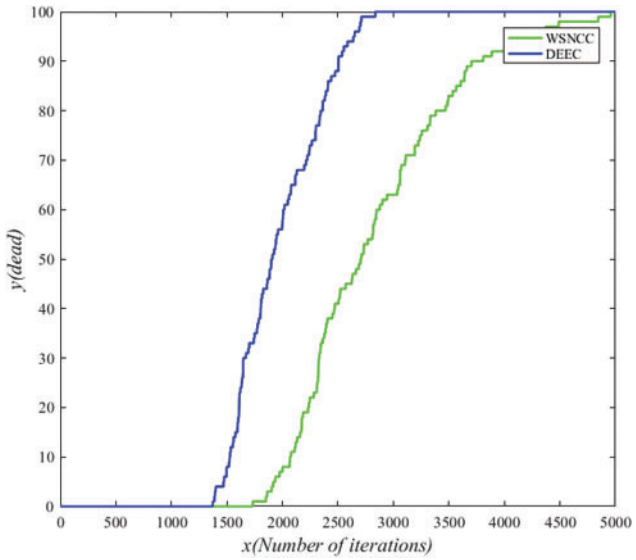

Figure 5: Comparison of network dead nodes

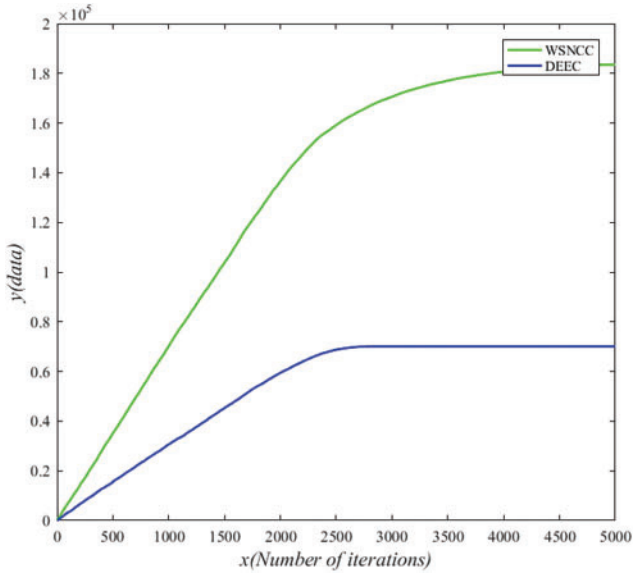

Figure 6: Comparison of network data transmission volume

Reducing energy consumption is the goal of all research institutes. Due to the limitation of hardware, the energy of wireless sensor networks will gradually decrease over time until the node dies. Reducing energy consumption can make the network data transmission more lasting and the network life cycle longer. Fig. 7 shows the comparison of energy consumption between WSNCC algorithm and DEEC algorithm. After calculation, the energy consumption of WSNCC algorithm and DEEC algorithm proposed in this paper is about 36.7% lower than that of DEEC algorithm.

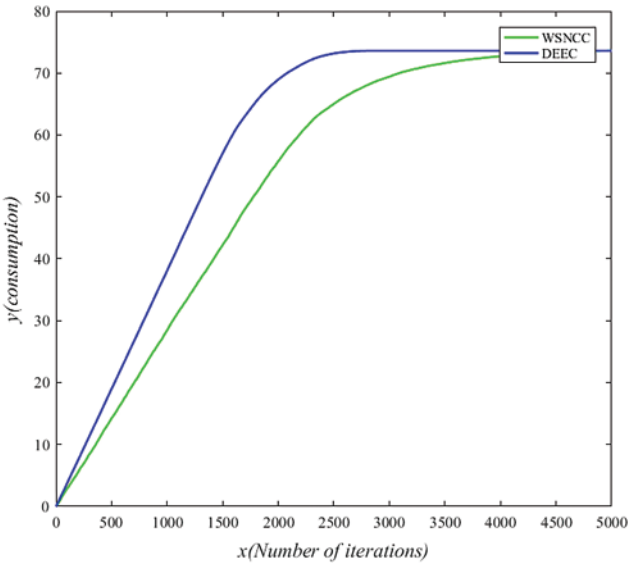

Figure 7: Comparison of network energy consumption

WSN closeness centrality is one of the indicators to measure the importance of nodes. It reflects the shortest path distance between nodes and sink nodes when transmitting data. For directed networks, when data is transmitted in different directions, the shortest path will also change, resulting in differences in stability and packet success rate when nodes transmit data to sink nodes. In the process of data transmission, the uniformity of WSN closeness centrality of some important nodes is a main strategy to enhance the invulnerability of wireless sensor networks. Whether there are optional redundant links between nodes is the main reason for the invulnerability of wireless sensor networks. Therefore, WSN closeness centrality reflects the role and influence of corresponding nodes in the whole network. As shown in Fig. 8, the network average WSN closeness centrality of the DEEC algorithm. It can be seen from the figure that the average WSN closeness centrality of each round of DEEC algorithm is almost below 0.1. When the network is working, the average WSN closeness centrality of the DEEC algorithm is only 0.0343. However, as shown in Fig. 9, the average WSN closeness centrality of the WSNCC algorithm. It can be seen from the figure that the average WSN tightness centrality of some rounds of the WSNCC algorithm is higher than 0.1, and even a few rounds of the average WSN tightness centrality is higher than 0.2. When the network is working, the average WSN closeness centrality of the WSNCC algorithm is 0.0528. Compared with the DEEC algorithm, the average centrality of the network in each round of the WSNCC algorithm is significantly improved, and the life cycle is longer. After calculation, the average WSN closeness centrality of the WSNCC algorithm proposed in this paper is almost doubled compared to the DEEC algorithm. It shows that the WSNCC algorithm greatly improves the centrality of the nodes with a small centrality value.

According to the invulnerability metric T proposed in this paper, the invulnerability metric T of WSNCC algorithm is 3.3218, which is higher than that of DEEC algorithm $T = 1.8983$. It shows that the algorithm proposed in this paper effectively enhances the invulnerability of the network.

Under the condition of setting the network simulation parameters in this paper, it is concluded that the network performance is better when the average value of network WSN closeness centrality $\bar{D} \geq 0.05$. At this time $\beta_{\min} = 2$, that is, adding two heterogeneous nodes can make the network meet the performance requirements.

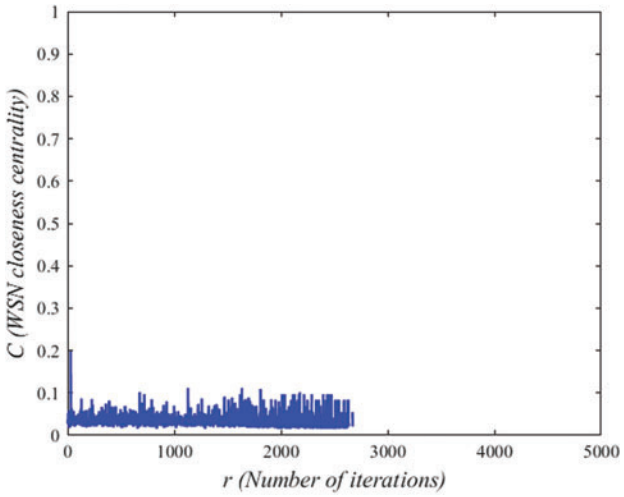

Figure 8: The network average WSN closeness centrality of the DEEC algorithm

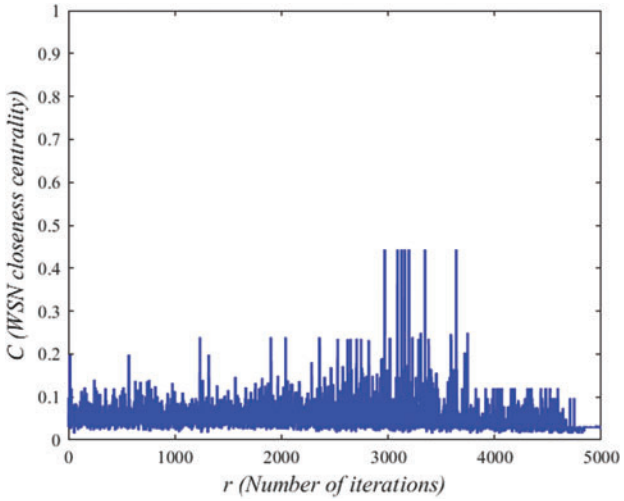

Figure 9: The network average WSN closeness centrality of the WSNCC algorithm

8 Conclusions

Firstly, the importance of invulnerability of wireless sensor networks, and the strategy of building a small world network model are proposed. By introducing heterogeneous nodes, the network is reconstructed into a heterogeneous network with small world characteristic, so as to greatly improve the invulnerability of the network. However, the random deployment of heterogeneous nodes can not optimize the network performance. A new centrality measurement method is proposed, which can accurately reflect the centrality of the network. On this basis, a heterogeneous node deployment scheme and network invulnerability measurement model are proposed. Simulation results show that this scheme can improve the invulnerability of wireless sensor networks with low construction cost. The WSNCC algorithm can improve the centrality of the network, and the future work is not only to consider the centrality of the nodes, but also to consider the actual monitoring environment, which can make the proposed scheme more practical and effective.

Funding Statement: This research was funded by the National Natural Science Foundation of China, No. 61802010; Hundred-Thousand-Ten Thousand Talents Project of Beijing No. 2020A28; National Social Science Fund of China, No. 19BGL184; Beijing Excellent Talent Training Support Project for Young Top-Notch Team No. 2018000026833TD01 and Academic Research Projects of Beijing Union University, No. ZK30202103.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Daniel, K. Baalamurugan, V. Ramalingam and K. Arjun, "Energy aware clustering with multihop routing algorithm for wireless sensor networks," *Intelligent Automation & Soft Computing*, vol. 29, no. 1, pp. 233–246, 2021.

[2] R. Punithavathi, C. Kurangi, S. P. Balamurugan, I. V. Pustokhina, D. A. Pustokhin *et al.,* "Hybrid BWO-IACO algorithm for cluster based routing in wireless sensor networks," *Computers, Materials & Continua*, vol. 69, no. 1, pp. 433–449, 2021.

[3] S. R. Lahane and K. N. Jariwala, "Secured cross-layer cross-domain routing in dense wireless sensor network: A new hybrid based clustering approach," *International Journal of Intelligent Systems*, vol. 36, no. 1, pp. 3789–3812, 2021.

[4] H. Shahid, H. Ashraf, H. Javed, M. Humayun, N. Jhanjhi *et al.,* "Energy optimised security against wormhole attack in IOT-based wireless sensor networks," *Computers, Materials & Continua*, vol. 68, no. 2, pp. 1967–1981, 2021.

[5] S. Perumal, M. Tabassum, G. Narayana, S. Ponnan, C. Chakraborty *et al.,* "ANN based novel approach to detect node failure in wireless sensor network," *Computers, Materials & Continua*, vol. 69, no. 2, pp. 1447–1462, 2021.

[6] L. W. Lin, L. Xu and X. C. Ye, "A novel method and its simulation to evaluate the invulnerability of wireless sensor networks," *Computer Systems & Applications*, vol. 19, no. 4, pp. 32–36, 2010.

[7] W. F. Li and X. W. Fu, "Survey on invulnerability of wireless sensor networks," *Chinese Journal of Computer*, vol. 38, no. 3, pp. 625–647, 2015.

[8] Y. J. Tan, J. Wu, H. Z. Deng and D. Z. Zhu, "Summary of research on invulnerability of complex networks," *Systems Engineering*, vol. 24, no. 10, pp. 1–5, 2006.

[9] B. C. Gong, X. L. Wang and R. Shun, "Wireless sensor network routing protocol and its application," *Science Press*, vol. 32, no. 21, pp. 89–113, 2017.

[10] Q. Sun, G. X. Cheng and X. Y. Wang, "Energy efficient routing algorithm based on small world characteristics," *Computers, Materials & Continua*, vol. 69, no. 2, pp. 2749–2759, 2021.

[11] Y. Zhang, G. Yang and B. Zhang, "FW-PSO algorithm to enhance the invulnerability of industrial wireless sensor networks topology," *Sensors*, vol. 20, no. 4, pp. 1114, 2020.

[12] X. W. Fu, Y. S. Yang and P. Octavian, "Invulnerability of clustering wireless sensor networks against cascading failures," *IEEE Systems Journal*, vol. 13, no. 2, pp. 1431–1442, 2019.

[13] Z. G. Zhao, "Research on invulnerability of wireless sensor networks based on complex network topology structure," *International Journal of Online Engineering*, vol. 13, no. 3, pp. 100–112, 2017.

[14] X. Y. Wang, G. X. Cheng, Q. Sun, J. P. Xu, H. Y. Zhang *et al.,* "An event-driven energy-efficient routing protocol for water quality sensor networks," *Wireless Networks*, vol. 26, no. 8, pp. 5855–5866, 2020.

[15] D. Y. Qin, S. Jia and S. X. Yang, "Research on trust sensing based secure routing mechanism for wireless sensor network," *Journal on Communications*, vol. 38, no. 10, pp. 60–70, 2017.

[16] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, pp. 440–442, 1998.

[17] C. Zhu, C. Zheng, S. Lei and G. Han, "A survey on coverage and connectivity issues in wireless sensor networks," *Journal of Network & Computer Applications*, vol. 35, no. 2, pp. 619–632, 2012.

[18] X. Fu, W. Li and G. Fortino, "Empowering the invulnerability of wireless sensor networks through super wires and super nodes," in *Proc. the 13th IEEE/ACM Int. Symp. on Cluster, Cloud, and Grid Computing*, Delft, Netherlands, pp. 561–568, 2013.
[19] J. Wu and Y. J. Tan, "Research on invulnerability measurement of complex networks," *Journal of Systems Engineering*, vol. 20, no. 2, pp. 128–131, 2005.
[20] K. Okamoto, W. Chen and X. Y. Li, "Ranking of closeness centrality for large-scale social networks," in *Proc. Int. Workshop on Frontiers in Algorithmics*, Berlin, Heidelberg, Springer, vol. 5059, pp. 186–195, 2008.
[21] M. E. J. Newman, "A measure of betweenness centrality based on random walks," *Social Networks*, vol. 27, no. 1, pp. 39–54, 2005.
[22] Q. Li, Q. X. Zhu and M. W. Wang, "Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks," *Computer Communications*, vol. 29, no. 12, pp. 2230–2237, 2006.
[23] C. Y. Sun, M. X. Shen and H. Sheng, "Optimization design of structure invulnerability for air defense multiple sensor network," *Journal on Communications*, vol. 38, no. 6, pp. 118–126, 2017.