Computer Communications 157 (2020) 53–63

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

TMSE: A topology modification strategy to enhance the robustness of scale-free wireless sensor networks

Shihong Hu [a], Guanghui Li [b,*]

[a] Department of Computer Science, Jiangnan University, Wuxi, Jiangsu, 214122, China
[b] Department of Computer Science and the Research Center for IoT Technology Application Engineering (MOE), Wuxi, Jiangsu, 214122, China

ARTICLE INFO

Keywords:
Wireless sensor network
Robustness
Malicious attacks
Scale-free networks
Onion-like

ABSTRACT

Scale-free wireless sensor networks (WSNs) are tolerant to random attacks but vulnerable to malicious attacks. With the increase of cyber-attacks, improving the survivability and robustness is critical to scale-free WSNs. This paper introduces a scale-free topology evolution mechanism (SFTEM) for WSNs, and the evolution model considers the fault probability of nodes as well as the communication range. Then, a new topology modification strategy for enhancing the robustness of scale-free WSNs is presented, namely TMSE. Different from previous works, we consider different types of malicious attack into the algorithm design, making the TMSE more resistant to realistic attacks. Besides, TMSE consists of two operations, in which the high degree operation (HDO) changes the network connections among high degree nodes base on the probability of being attacked, and the degree associativity operation (DAO) transforms the network topology into the onion-like structure using its degree–degree correlation. Meanwhile, all the nodes modified by TMSE maintain the node degree, thus the final topology preserves scale-free properties. Simulation results demonstrate that the network topology generated by SFTEM has the scale-free characteristics, and its robustness can be effectively improved by TMSE, compared to the existing algorithms.

1. Introduction

Internet of things supported by wireless sensor networks (WSNs) [1–4] is an attractive and flexible option to be applied in a wide range of many real-world scenarios, such as environmental monitoring [5], intelligent transportation [6] and other fields. In many applications, WSNs often operate in rigorous and hostile environments [7]. Depending on the criminal intent, a network attack can be random or malicious. Nodes in WSNs may fail due to random attacks including software or hardware faults [8] and hostile weather [9]. Moreover, the threats to malicious attacks based on intelligent node selections increase rapidly. Scale-free theory in complex networks [10,11] can be applied to evolve the topology and increase the survivability of WSNs [12–14]. A remarkable characteristic of scale-free WSNs is that most nodes have a lower node degree and thus have strong anti-random failure ability [10]. However, scale-free networks are vulnerable to malicious attacks [15] due to a small proportion of nodes hold most of the connections. Once such nodes are attacked, the network will split into independent graphs or even be paralyzed [16]. In our previous work [17], we proposed a topology evolution mechanism for scale-free WSNs to improve the fault tolerance against random attacks. In scale-free WSNs, a few key nodes possess most connections of network and thus the energy of these nodes will be exhausted much faster than the other nodes. Therefore, our previous scheme combined joint failure probability and other characteristics including node degree, node saturation and the distance between nodes to keep energy balance of the network. However, our previous scheme failed to consider the robustness of topology under malicious attacks. Therefore, the purpose of this paper is to design a method to ensure that even if a malicious attack causes some nodes to fail, the network can remain connected and functioning properly.

In recent years, various enhancing robustness strategies of network topology have been proposed [18–23]. Since networks with complex topologies can be used to model many systems in nature and society, the scale-free theory as one type of complex networks is generally applied to model the large-scale homogeneous WSNs. Many studies have investigated the robustness of the scale-free topology. The hill-climbing [24] as the most classic algorithm uses the feedback information to help generate a better robustness metric to optimize the robustness continuously. However, as an improved depth-limited search method, the hill-climbing algorithm may converge at a local optimal situation. Particularly, it is found that the onion-like network can acquire adaptive capacity in resilience by a change of routing policy for flow control to absorb cascading overload failures triggered by attacks [25]. Since the onion-like structure is robust against malicious

* Corresponding author.
E-mail addresses: jnuhsh@163.com (S. Hu), ghli@jiangnan.edu.cn (G. Li).

https://doi.org/10.1016/j.comcom.2020.04.007
Received 16 October 2019; Received in revised form 9 March 2020; Accepted 5 April 2020
Available online 9 April 2020

attacks and has been confirmed by theory and experiments [26], a new robustness strategy (ROSE) [27] was designed to change the topology to an onion-like structure to improve the robustness. However, all operations in ROSE target at all nodes in the network may generate redundant operations.

We proposed a new topology modification strategy that includes two operations to enhance the robustness of scale-free WSNs. In general, the network nodes with high degrees are vulnerable to malicious attacks; hence, we design an operation to improve the robustness by modifying the connections of these nodes. Then, another operation follows the idea that the network topology with an onion-like structure that has a positive degree of correlation would be strongly tolerant against malicious attacks [25]. The main contributions of this study can be summarized as follows.

- An improved topology evolution mechanism is introduced to generate the scale-free WSNs. Considering the fault tolerance of network and the limited communication range, the networks evolved by the mechanism have scale-free properties.
- The proposed TMSE strategy includes two operations: high degree operation (HDO) and degree associativity operation (DAO). Different types of malicious attacks are firstly discussed to determine the parameters of TMSE. HDO is designed to change the network connections of some important nodes to enhance robustness, and DAO uses the degree–degree correlation property to make the topology close to the onion-like structure.

The remainder of this paper is organized as follows. In Section 2, the related work is reviewed and summarized. Then, we introduce the evolution mechanism of scale-free topologies and robustness measures under different attacks in Section 3. Section 4 describes the ideas and details of TMSE. In Section 5, simulation results are presented. Finally, we conclude this study in Section 6.

2. Related work

To increase the survivability of WSNs, there are some works to improve the energy efficiency and extend the lifetime of the network [28,29]. One way of maintaining survivability in WSNs is key management. Yousefpoor and Barati [30] categorized dynamic key management schemes based on the type of keys, key distribution mechanisms, key cryptography methods and network models. Besides, Bosch et al. [31] provided an overview of state of the art commercial and scientific solutions of management schemes and showed their strengths and weaknesses. Barabási and Albert [11] provided the other way to increase the survivability of networks, the proposed BA model applies the following two criteria to achieve a scale-free topology: (1) growth: new nodes join the network one by one, (2) the newly joined node is connected to the existing node with a probability proportional to the degree of the existing node. This leads to the phenomenon that the more connections a node has, the more likely it is to receive a new connection. In recent years, many researchers have proposed methods based on BA model to construct a scale-free WSN to achieve the goal of fault tolerance, energy-saving or prolonging the lifetime. Liu et al. [13] proposed a small-world and scale-free topology model for heterogeneous WSN, implemented by preference connection mechanism. The network generated by this topology model has stronger robustness against random faults. Similarly, inspired by the scale-free theory, Peng et al. [32] presented two schemes for large-scale hierarchical WSNs. One scheme constructs a large-scale WSNs based on the BA model, and the other one avoids establishing links with potential hub nodes and thus improving the energy efficiency of the network. Using scale-free property, He et al. [33] designed a topology evolution method, in which the cluster nodes are distributed evenly and evolve by random walk based on the residual energy and the degree of the nodes. Zhao et al. [34] used Gaussian distribution to define a 3D terrain with multimodal and proposed a new scale-free WSN topology in 3D terrain. They considered the requirements of WSNs in practical application and a scale-free network model is established by the growth and preferential connection criteria for WSN in 3D terrain. Tan et al. [35] presented a new novel energy-efficient and fault-tolerant evolution model for large-scale wireless sensor networks based on complex network theory. In the evolution model, not only is the residual energy of each node considered, but also the constraint of links is introduced, which makes the energy consumption of the whole network more balanced.

A characteristic of a scale-free network is that the degree of a small number of nodes is very high, which makes the network vulnerable to malicious attacks. Once nodes with high degrees are attacked, the network can easily be paralyzed by the loss of a great number of connections. Therefore, the purpose of this paper is to enhance the robustness of scale-free WSNs against malicious attacks. Adding connected edges and critical nodes to the network can alleviate this problem effectively, but it will change the scale-free network properties and consume too much energy. Recently, many studies have focused on the robustness improvement of scale-free WSNs. To create a robust network, Schneider et al. [36] proposed a novel metric of robustness R, which measures the average maximum connected component after attacks. The scale-free network can be improved with a variety of optimization techniques by using metric R. Herrmann et al. [24] used the hill-climbing algorithm to make the topology of WSN close to the onion-like structure, but one problem with their algorithm is that it may fall into local optimum. Based on the hill-climbing algorithm, Buesser et al. [37] proposed a simulated annealing algorithm, which used a probability switch strategy to deal with the multimodal phenomenon. However, many redundant operations in the process of rewiring to the network may lead to the high time complexity. Rong and Liu [38] proposed a heuristic optimization algorithm to improve the robustness of scale-free networks. The algorithm can maintain the node distribution unchanged while performing different edge operations, but it failed to consider the communication limitations of WSNs. Roy et al. [39] presented a new edge rewiring strategy to enhance the robustness against failures, including edge addition and edge deletion. However, their algorithm is essentially different from the above-mentioned algorithms, as it improves the topology robustness at the expense of changing the scale-free properties. In [40], the authors investigated robustness of the consensus characterized as coherence in the noisy scale-free networks under average degree, random nodal failures and target attacks. Based on the coherence, a new centrality index named as leader centrality is proposed to identify more influential spreaders. Zhang et al. [41] proposed a new link-adding strategy (LLA) for large-scale wireless sensor networks. The robustness and traffic capacity can be enhanced by local world theory. Moreover, LLA is to use the relative position relationship and set division, and establish the new link-adding strategy. Qiu et al. [27] presented a new robustness enhancing strategy (ROSE) by rearranging the edges to resemble an onion-like structure. Meanwhile, ROSE can keep the degree of each node in the topology unchanged such that the resulting topology remains scale-free. Genetic algorithm (GA) is proposed to enhance robustness of networks [42]. However, the single population of possible solutions in the evolution may cause a local optimum result. To overcome this limitation, Qiu et al. [43] used multi-population co-evolution to enhance the robustness of scale-free topologies. The robustness optimization scheme for scale-free WSNs (ROCK) introduces novel crossover and mutation operators to rewire the edges in network topologies.

3. Network modeling and robustness measures

In this section, we introduce a scale-free topologies model for WSNs and describe four malicious attack strategies and robustness metrics.

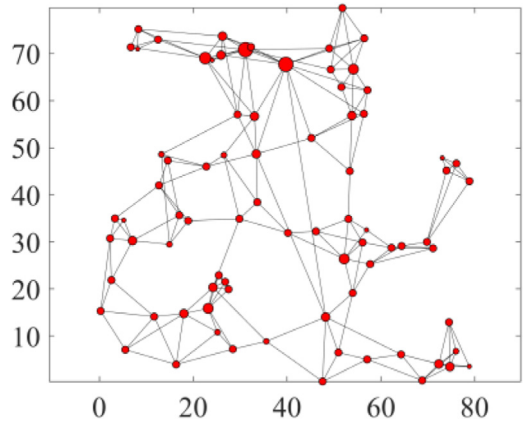

Fig. 1. The illustration of a scale-free WSN with 20 nodes.

3.1. Fault-tolerant topology model in WSNs

Nowadays, a large number of IoT sensors are deployed in buildings, hospitals and shopping centers to support a variety of smart services. Because of the high communication capacity and a large number of sensors, the resulting WSN will be very dense. In particular, dense WSNs are prone to node failures. Therefore, it makes sense to consider the robustness of the dense WSN. WSNs have obvious dynamic characteristics, including the increase of new nodes and new links, and the node failures caused by environmental factors or energy depletion. In our previous work, we proposed a scale-free topology evolution mechanism (SFTEM) for WSNs [17]. SFTEM can generate a fault-tolerant network, especially against random attacks. In this study, SFTEM will be used to generate the original scale-free WSNs. The rules of SFTEM are as follows.

(1) Initialization: There are m_0 nodes and e_0 edges in the initial network at time $t = 0$.
(2) Preferential growth: Add one node at a time, the newly added node connects m current nodes ($m \le m_0$), and the probability that the new node connect node n is represented as $\prod k_n$, which is given by

$$\prod k_n = \left(1 - \frac{k_n}{k_{\max}}\right) \frac{F_n \times k_n}{\sum_{l \in \Omega} F_l \times k_l} \tag{1}$$

where k_n is the node degree and $F_n = 1/p(n) \times d_i$, $p(n) = 1 - e^{-\lambda_t t_s}$, and $p(n)$ denotes the fault probability of node n (λ_t is the failure rate of a sensor node [44]), and d_n is the distance between the newly added node and node n. F is the fitness function of the node and associates the fault probability and the distance between nodes considering the fault tolerance of network and the limited communication range. The local world Ω of node n represents its one-hop neighbor nodes. k_{max} is the threshold of node degree, which limits the maximum degree of the nodes. According to the above-mentioned evolution rules, we can generate a fault-tolerant scale-free network with node degree satisfying the power-law distribution, which will be validated in the simulation section (Specific details can be found in [17]). Fig. 1 gives an example of the scale-free WSN generated by SFTEM, where red points represent nodes and the size of the point indicates the different degrees of the node: the larger the point is, the higher the degree is.

3.2. Attack types and metrics of robustness

Usually, WSNs are assumed to be subject to random and malicious attacks. Due to the scale-free and power-law characteristics of the generated network, the network has a strong resistance to random attacks, but it is fragile for malicious attacks. For the research of malicious attacks, the order of deleting nodes (or edges) is an open choice. Moreover, damage can be maximized on any fixed number of removed nodes. We adopt four types of malicious attacks, which are degree-based and betweenness-based in this paper.

Definition 1 (*Betweenness [38]*)**.** There is at least one shortest path for every pair of nodes in a connected network. The betweenness B of node i in WSNs is the number of these shortest paths that pass through node i, which is defined as:

$$B(v_i) = \sum_{\substack{1 \le k < l \le N \\ k \ne i \ne l}} \frac{\sigma_{kl}(i)}{\sigma_{kl}} \tag{2}$$

where $\sigma_{kl}(i)$ denotes the number of shortest paths between node k and l that pass through node i, σ_{kl} is the number of shortest paths between node k and l, and N is the number of nodes in the network.

Definition 2 (*Node Degree [45]*)**.** The degree of a node is the number of edges connected to the node.

Definition 3 (*Initial Degree (ID) Attack [11]*)**.** The nodes in the network will be removed one by one in a descending degree order.

Definition 4 (*Recalculated Degree (RD) Attack [16]*)**.** At each attack, the node with the highest degree will be removed. As the degree distribution is different from the initial ones caused by the network structure changes after each attack, the descending order of nodes will be recalculated at each removal step.

Definition 5 (*Initial Betweenness (IB) Attack [11]*)**.** The nodes in the network will be removed one by one in a descending betweenness order.

Definition 6 (*Recalculated Betweenness (RB) Attack [16]*)**.** At each attack, the node with the highest betweenness will be removed. As the betweenness distribution is different from the initial one caused by the network structure changes after each attack, the descending order of nodes will be recalculated at each removal step.

Definition 7 (*Connectivity Coverage*)**.** The connectivity coverage C of the network is defined as

$$C = \frac{M}{N} \tag{3}$$

where M is the node number of the maximal subgraph, and N is the node number in the initial network. When nodes are damaged by the above four types of malicious attacks, the network may gradually be split into isolated parts. To measure the robustness of network topology, Schneider et al. [36] proposed a novel metric based on the percolation theory, which considered the maximal connected component after removing nodes. We combine this measure metric with the above four types of attacks, and then calculate the entire connectivity coverage C according to different attack strategies to evaluate the network's resistance to attack. The robustness metric is defined as

$$R = \frac{1}{N-1} \sum_{s=0}^{N} C_s \tag{4}$$

where C_s is the connectivity coverage of the network after removing s nodes, and $R \in [0, 0.5]$, $R = 0$ represents the network is completely disconnected and $R = 0.5$ represents the fully connected network. The larger the R is, the stronger the network is against the malicious attack. According to the definition of R, we need to use a centralized system to calculate R based on the global information of the network.

4. Tmse overview

TMSE is designed to enhance the robustness of scale-free networks, which includes HDO and DAO modification strategies. First, we try to

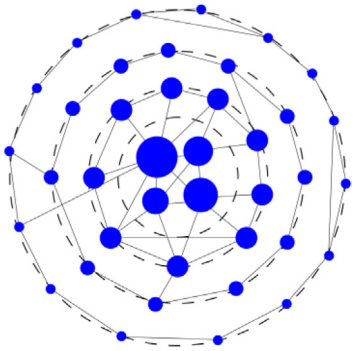

Fig. 2. The illustration of onion-like structure.

change the connections of nodes with high degree without changing the power-law characteristic, thus reducing the connectivity damage of the network. Second, Hayashi et al. [25] found that the network topology with an onion-like structure that has a positive degree of correlation would be strongly tolerant against malicious attacks. As shown in Fig. 2, in the onion-like structure, the degree distribution of nodes from the center to the boundary is hierarchical. The node degree of each ring is the same or similar; that is, the high-degree node connects with a high-degree node, and the low-degree node connects with the low-degree node.

A scale-free WSN is represented as a connected graph $G = (V, E)$, where $V = \{1, 2, \ldots, N\}$ is the node set and $E = \{e_{ij} | i, j \in V, i \neq j\}$ is the edge set. To explain the operation of the edge swap, we first give the definition of independent edges.

Definition 8 (*Independent Edges [27]*)**.** Two edges e_{mn} and e_{kl} are independent edges if they satisfy the conditions: each of the nodes m, n, k and l must be within the communication range of the other three nodes, and there are no extra connections among nodes m, n, k, and l except the existing edges e_{mn} and e_{kl}.

The basis of the edge swap operation is that the selected edges are independent edges, and Fig. 3 illustrates the edge swap operation. As shown in Fig. 3(a), two edges e_{mn} and e_{kl} are independent edges randomly chosen in the original topology graph (red lines). After swapping their connected edges, as shown in Fig. 3(b), the original topology becomes a new topology while maintaining the same degree distribution. That is, the degrees of nodes m, n, k, and l keep unchanged.

4.1. High degree operation (HDO)

In general, high degree nodes in the network are vulnerable to malicious attacks. However, the node degree, as a single indicator, may not accurately measure the importance of nodes in the network. Malicious attacks tend to choose the nodes with higher traffic responsibilities in the network [36,46]. Betweenness describes the influence of nodes on routing bridges in the network, and the higher the betweenness is, the more easily the node is chosen as the target of attack [46]. Moreover, the state of the edge also affects the node, and we usually use the edge degree to reflect the importance of the edge.

Definition 9 (*Edge Degree [16]*)**.** Given an edge e connected to node m and n with node degrees k_m and k_n respectively, edge degree k_e is defined as follows.

$$k_e = k_m k_n \tag{5}$$

The average edge degree of the associated edges of any node i is expressed as:

$$K(n_i) = \overline{k_n^e} = \frac{1}{n_e} \sum_{e_i \in n_e} k_e(i) \tag{6}$$

where n_e is the associated edge number of node i, and $k_e(i)$ denotes the edge degree of edge e connected to node i. Here, we combine betweenness and average edge degree to characterize the probability of a node being attacked.

$$p(n) = \alpha C_B(n) + (1 - \alpha)\mu(K_n) \tag{7}$$

$$C_B(n) = 2B/[(N - 1)(N - 2)] \tag{8}$$

$$\mu(x) = \begin{cases} 1 & x \geq a \\ 1 - e^{-\left(\frac{x-a}{\sigma}\right)^2} & x < a \end{cases} \tag{9}$$

where $\alpha \in [0, 1]$ is the weight value of parameters, $C_B(n)$ is the normalized parameter of betweenness which is defined as (8) and $C_B(n) \in [0, 1]$. Besides, $\mu(x)$ is a fuzzy membership function characterizing the average edge degree, corresponding to the probability of being attacked. The relationship between the average edge degree and the probability of being attacked cannot be quantified precisely. The fuzzy theory provides an effective way, the membership function, which can represent the "true degree" of the average edge degree corresponding to the probability of being attacked. Therefore, a relatively reliable reference value can be given. The probability of the node being attacked increases with the increase of the average edge degree of the node, so we choose the incremental membership function, as shown in (9), and $\mu(x) \in (0, 1]$. Parameter a is determined according to the connectivity coverage C under different attack strategies, and the details can be found in the simulation experiment in Section 5.

After analyzing the attack probability of the nodes, we propose an operation to improve the robustness of the network. Firstly, we find out the set of nodes with high degrees. Then the nodes in the set will conduct the edge swap operation according to the probability of being attacked. As a result, the robustness R can be gradually improved due to the change of the local topology connection. The pseudocode of HDO is given in Algorithm 1.

The variables used in HDO algorithm are interpreted as follows:

- A: adjacency matrix of the original scale-free network nodes.
- E: edge set of the scale-free network.
- N_H: high degree node number.
- A': adjacency matrix of new topology after the edge swap operation.
- $G_2(n)$: two-hop neighbor connected subgraph of node n [47].
- $E_2(n)$: edge set of the two-hop neighbor connected subgraph of node n.
- $P(n)$: the probability of a node being attacked.

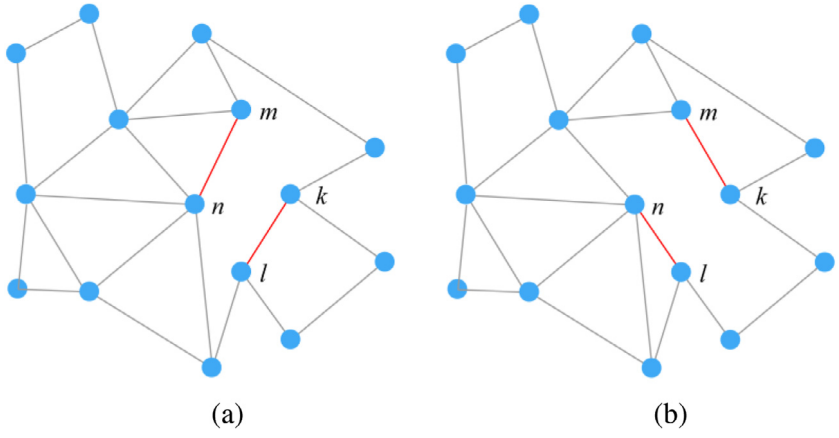

Fig. 3. The illustration of edge swap: (a) Selection of independent edges; (b) Swap of connection. . (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Algorithm 1 HDO

Input: N_H, A, R, E

Output: A

1: $n = 1$;
2: **while** $n \leq N_H$ **do**
3: Find $G_2(n)$, $E_2(n)$
4: **while** there exists edge in $E_2(n)$ not marked **do**
5: Select e_{mn} and e_{kl} randomly
6: **if** e_{mn} and e_{kl} is an independent edge pair **then**
7: swap e_{mn} and e_{kl}
8: $G_2(n)' \leftarrow G_2(n)$
9: **if** $P'(n) < P(n)$ and $R(A') > R(A)$ **then**
10: G2(n)← G2(n)'
11: update A
12: **end if**
13: **end if**
14: Mark e_{mn} and e_{kl}
15: **end while**
16: **end while**

For each node in N_H, find its $G_2(n)$ and corresponding edge set $E_2(n)$. A pair of independent edges e_{mn} and e_{kl} is randomly chosen from $E_2(n)$. After edge swap operation is implemented, a new connected subgraph $G_2(n)'$ and a new adjacency matrix A' can be obtained. Meanwhile, the probability of node n ($P(n) \rightarrow P'(n)$) being attack and the robustness of the whole network topology ($R(A) \rightarrow R(A')$) will be changed. If the probability of node n being attacked reduces and the robustness of the new topology has been improved, then the adjacency matrix will be updated from A to A'. The inner loop ends until all edge swap operations are completed, and the outer loop to the end of the examination of all nodes in the high degree nodes set.

4.2. Degree associativity operation (DAO)

From Fig. 2, we know that the degree of the nodes in the onion-like structure from the inside to the outside decreases successively. The benefit of this structure is that, when the node fails, its neighbor nodes will keep the original functionality to maintain the connectivity of the network. As a result, the damage of malicious attack has been largely weakened in WSNs. Inspired by this characteristic, we take degree associativity defined in the M.E [48] as a parameter to measure the degree–degree correlation of topology.

$$r = \frac{\sum_i k_i \sum_{ij} A_{ij} k_i k_j - \left(\sum_i k_i^2\right)^2}{\sum_i k_i \sum_i k_i^3 - \left(\sum_i k_i^2\right)^2} \tag{10}$$

where A_{ij} denotes the element of adjacency matrix (i, $j = 1, 2, \ldots, N$). The degree associativity of the graph calculates the tendency of nodes with similar degrees to be connected, and it is equivalent to the Pearson correlation coefficient of the degrees. $r \in [-1, 1]$, when r (> 0) increases, the nodes with similar degrees tend to establish the connection, while the nodes with different degrees tend to establish connections as r (< 0) decreases.

To reduce the algorithm complexity, a pair of independent edges e_{mn} and e_{kl} (that is, four nodes m, n, k and l) is randomly selected. Then, the minimum connected subgraph g of these four nodes from G can be found by the Dijkstra algorithm. So we only need to calculate the corresponding parameters of g after each edge swap operation. Algorithm 2 describes the pseudocode of DAO.

A pair of independent edges e_{mn} and e_{kl} are randomly chosen from E and find the Minimal Connected Subgraph g of these four nodes (m, n, k, and l) by Dijkstra algorithm. Then, after two methods of edge swap (Line 5 and Line 6) are implemented, the corresponding g_1, g_2, and A_1 and A_2 will be obtained. Besides, the degree associativity r in all three connection cases is calculated, and we will select the maximum r of three cases. If the maximum r is the result of the initial case, the current operation will be abandoned, and the algorithm will enter the next loop. Otherwise, if the maximum r is the result of the edge swap case and the modification A_1 or A_2 improves the robustness, the swap will be accepted. This process ends until all edge swap operations are completed.

Table 1
Simulation parameters.

Number of nodes (N)	Size of the deployed region (Γ)	Maximum degree (k_{max})	Communication radius (m)
50	50 × 50 m^2	10	25
100	100 × 100 m^2	20	50
150	150 × 150 m^2	30	75
200	200 × 200 m^2	40	100

Algorithm 2 DAO

Input: A, E, N, R

Output: A

1: **while** there exists edge in E not marked **do**
2: Select e_{mn} and e_{kl} randomly
3: Find MinimalConnectedSubgraph g
4: **if** e_{mn} and e_{kl} is an independent edge pair **then**
5: $g_1 \leftarrow g$ *and* $A_1 \leftarrow A$ (Remove e_{mn} and e_{kl} in A and Add e_{ml} and e_{nk} to A_1)
6: $g_2 \leftarrow g$ *and* $A_2 \leftarrow A$ (Remove e_{mn} and e_{kl} in A and Add e_{mk} and e_{nl} to A_2)
7: r=*max* (r_g, r_{g1}, r_{g2})
8: **if** $r = r_{A1}$ **and** $R(A_1) \geq R(A)$ **then**
9: $A \leftarrow A_1$
10: **else if** $r = r_{A2}$ **and** $R(A_2) \geq R(A)$ **then**
11: $A \leftarrow A_2$
12: **end if**
13: **end if**
14: Mark e_{mn} and e_{kl}
15: **end while**

4.3. Analysis complexity of TMSE

Theorem 1. *The complexity of HDO is O (M^2), where M is the maximum number of pair of edges among the nodes with high degrees in HDO. The complexity of DAO is O (L) and L is the maximum number of selected pair of edges of topology in DAO.*

Proof. As shown in the steps of Algorithm 1, the main calculation is processing the pair of edges in two-hop neighbor connected subgraph of nodes with high degree. Let M denote the maximum number of pair of edges, and the complexity of outer loop be denoted as O (M'), where M' is the number of nodes with high degree. Since $M' < M$, the complexity of HDO is $O(M^2)$. Similarly, the main calculation of Algorithm 2 is processing the pair of edges in global graph and the complexity of DAO is O(L), where L is the maximum number of selected pair of edges of topology.

5. Simulation results and analysis

In this section, SFTEM is firstly evaluated for its scale-free properties. Then, four types of attacks are simulated on the generated scale-free topology to determine the value of a in the membership function (Eq. (9)). Especially, all malicious attacks implemented on nodes of scale-free networks are simultaneous attacks. Besides, once the node is attacked, all links connected to it are considered invalid. The different sizes and edge density of scale-free networks are set to evaluate the performance of TMSE, simulated annealing (SA) [25] and ROSE [27]. Simulations were conducted on an Intel Core i7 system with 128 GB memory using Matlab.

Table 2
Determination of a under different cases.

Attack type	Number of nodes (N)			
	50	100	150	200
ID	16	27	33	44
IB	16	27	38	50
RD	15	26	32	40
RB	14	22	27	36

5.1. Evaluation of scale-free properties

Assume that all nodes were randomly deployed in the 2D field Γ, and the size of the region varied with the number of nodes. In the initial network, the node number m_0 is 3, and the new edge number m is selected from $\{1, 2, \ldots, 5\}$, the maximum degree and communication radius of nodes depend on the size and density of the network. Table 1 listed the specific simulation parameters.

We select three cases of network parameter pair (N, m), namely, (50, 2), (50, 4), and (200, 2). The topology of scale-free networks and the probability distribution of node degree are shown in Fig. 4. The red points denote the nodes, and the size of the point indicates the different degrees of the node: the larger the point is, the higher the degree is. As can be seen from the three topology graphs in the first row of Fig. 4, a few nodes have high degrees and the degrees of most nodes are low. As shown in the second row of Fig. 4, the probability distribution of the node degree of the networks is consistent with the power-law property of the scale-free network. It proves that the network topology evolved by SFTEM has scale-free property.

5.2. Determination of parameter a under different attack types

We take the attacked node number that makes the connectivity coverage C of the network be less than 0.5 as the value of parameter a. That is, when the number of nodes under attack is greater than or equal to a, $C < 0.5$ and decreases rapidly, and the probability of the node being attacked is estimated to be 1 (as shown in (9)). To observe the change of connectivity coverage C with the number of attacked nodes, four types of attacks (see Section 3.2) are simulated on different size networks. From four graphs in Fig. 5, we know that RB attack has the strongest destructive power on connectivity coverage C, followed by RD attack. Besides, ID and IB attacks have almost the same destructive power. As shown in Fig. 5(a), $N = 50$, when the number of attacked nodes is 16, $C < 0.5$ under the ID and IB attack, so the value of a in the membership function under the attack of IB and ID is set to 16. Under the attack of RD and RB, $C < 0.5$ until the number of the attacked nodes is 15 and 14, respectively. The value of a in each case is summarized in Table 2, and the following experiments set the corresponding parameters based on the data in Table 2.

5.3. Comparison of the robustness for different size of WSNs

To verify the performance of TMSE, we conducted robustness testing experiments under different attacks and compared them with SA [25] and ROSE [27]. The size of scale-free networks in this experiment is 50, 100, 150 and 200, respectively. The number of added edges m in the evolution of scale-free networks is fixed to 2. We compared the robustness of different sizes of WSNs under four types of attack, as shown in Fig. 6.

As shown in Fig. 6(a)–(d), the value of R shows a descending trend, as N increases. Compared with the original scale-free topology (OSFT), three algorithms have greatly enhanced the robustness. From Fig. 6(a) and (b), it is observed that TMSE has little superiority over ROSE under ID or RD attack, but is far better than SA algorithm. Besides, we found that the performance of TMSE is obviously better than ROSE under IB or RB attack, and sometimes the performance of SA is better than that

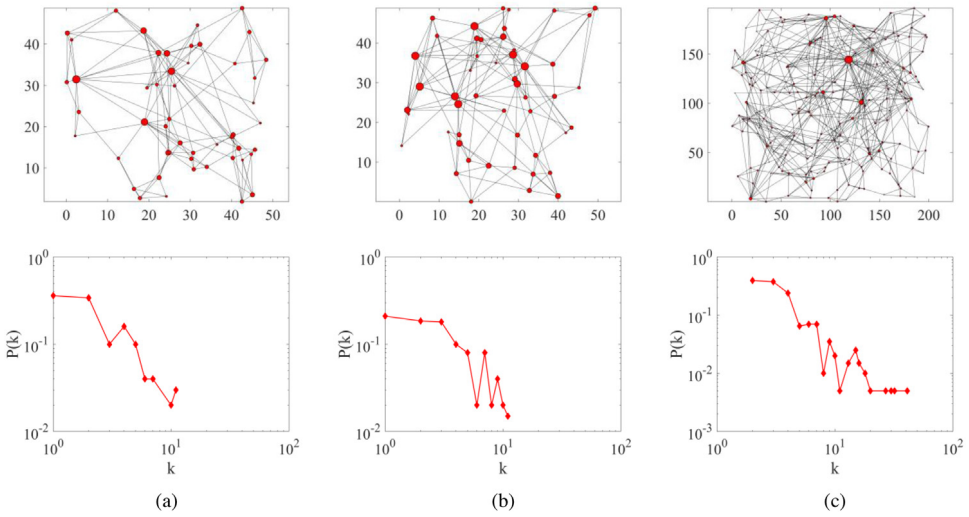

Fig. 4. Properties of scale-free in WSNs. (a) $N = 50$, $m = 2$. (b) $N = 50$, $m = 4$. (c) $N = 200$, $m = 2$. . (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

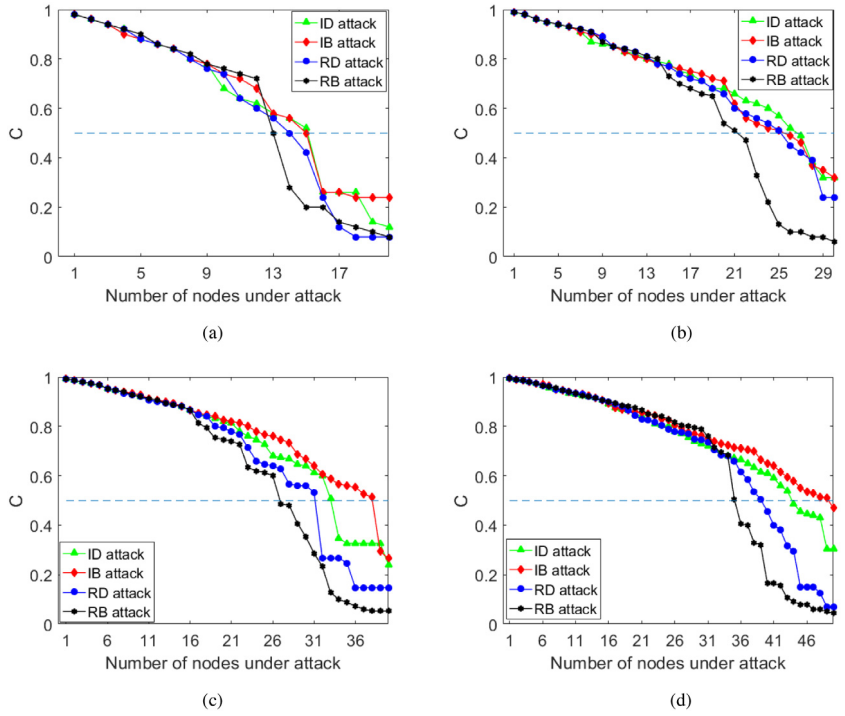

Fig. 5. The changing trend of C with the number of nodes under attack for different attack types and different sizes of WSNs. (a) $N = 50$. (b) $N = 100$. (c) $N = 150$. (d) $N = 200$.

of ROSE, as shown in Fig. 6(c) and (d). In conclusion, regardless of the attack type, TMSE is superior to SA and ROSE for improving robustness under different sizes of WSNs.

Fig. 7(a) and (b) show the topology and node degree distributions of the scale-free WSN after TMSE, where $m = 2$. It is found that the node in scale-free networks tends to connect the node with the same degree after robustness enhancement by TMSE. Meanwhile, the degree distribution of the network keeps the power-law distribution successfully. As shown in Fig. 8(b), the network topology highlights the characteristics of the onion structure after TMSE, compared to Fig. 8(a). The degree distribution of nodes from the center to the boundary is hierarchical, and the nodes of each ring tend to connect nodes with similar degrees in Fig. 8(b), which indicates the scale-free topology is more similar to the onion-like structure.

5.4. Comparison of the robustness for different edge density of WSNs

For further comparison, the scale-free networks with different edge density are generated to verify the performance of TMSE. The network size N is set to 50, $m \in \{1, 2, \ldots, 5\}$ to satisfy the condition of different edge density, and the RD attack and RB attack is selected for comparison experiments. Fig. 9 shows the performance of the robustness of TMSE, SA, ROSE and OSFT for different edge density of networks. It can be observed that R increases with the increase of edge density because the increase of edge density of the network enhances the robustness of the topology. Three algorithms effectively enhance the robustness of the topology and TMSE is better than the other two algorithms compared with the initial scale-free network. As can be seen from Fig. 9(a), under RD attack, the robustness difference between TMSE and ROSE is small, and TMSE performs better than ROSE in general. As

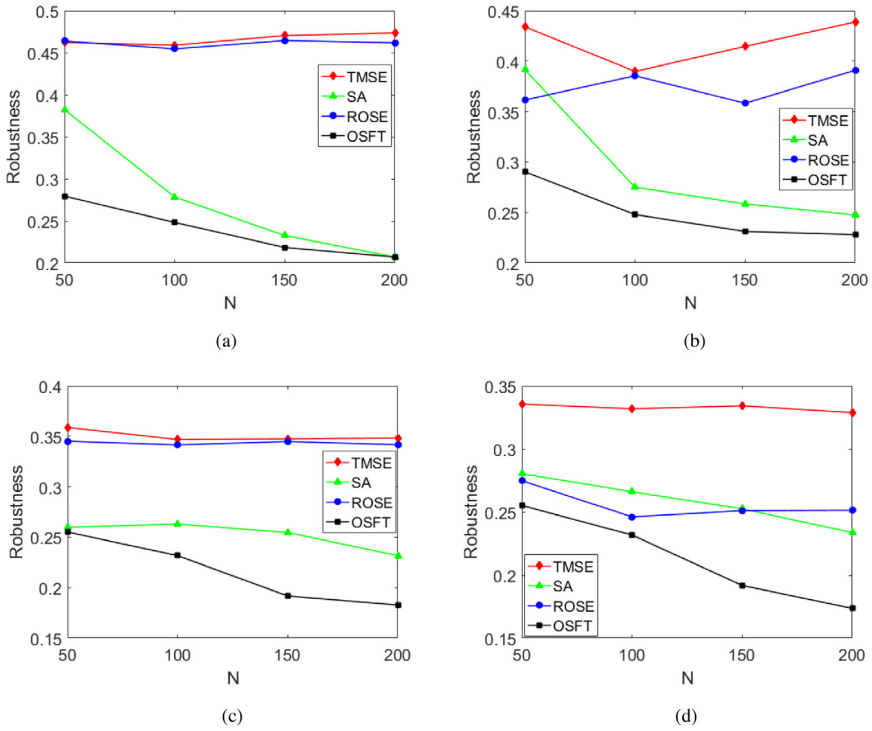

Fig. 6. Comparison of the robustness for different sizes of WSNs under four types of attack. (a) ID attack. (b) IB attack. (c) RD attack. (d) RB attack.

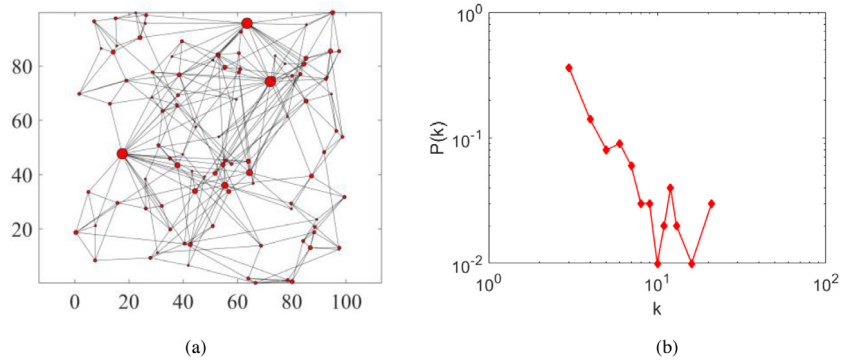

Fig. 7. Scale-free topology and degree distribution after TMSE when $N = 100$. (a) Scale-free topology. (b) Degree distribution.

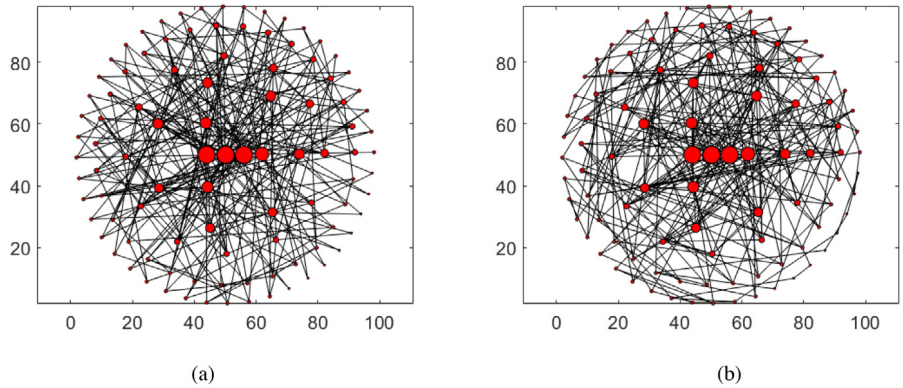

Fig. 8. Onion-like structure before and after TMSE when $N = 100$. (a) Redeployed the nodes before TMSE. (b) Redeployed the nodes after TMSE.

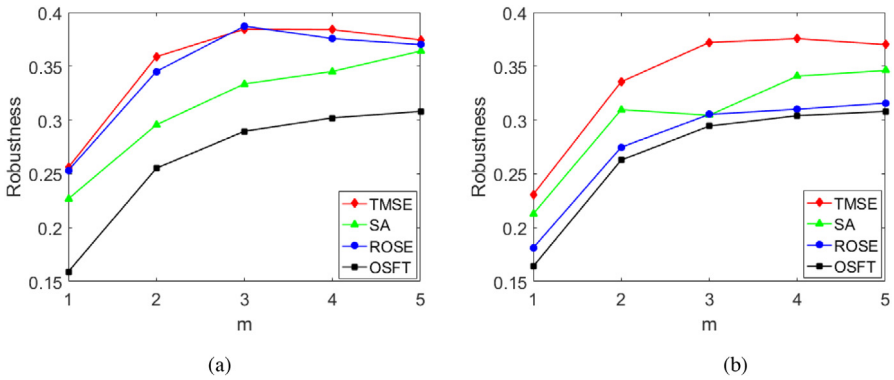

Fig. 9. Comparison of the robustness for different edge density of WSNs. (a) RD attack. (B) RB attack.

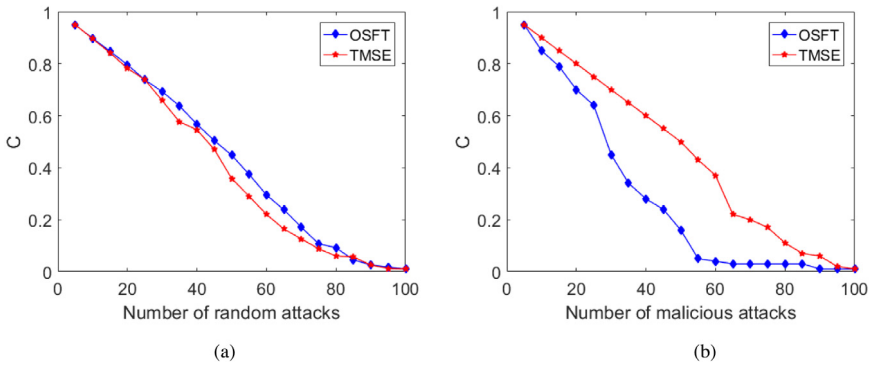

Fig. 10. The connectivity coverage C before and after TMSE under random and malicious attacks. (a) Under random attack. (B) Under malicious attack.

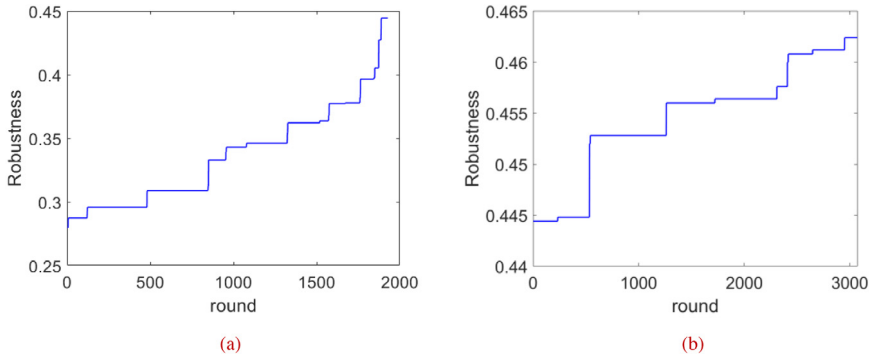

Fig. 11. The convergence property of TMSE when $N = 50$. (a) HDO. (B) DAO.

shown in Fig. 9(b), TMSE is superior to other algorithms in robustness optimization under RB attack.

5.5. Comparison of the connectivity coverage C under RD attack before and after TMSE

WSNs are often subjected to random and malicious attacks. TMSE has good robustness against malicious attacks while maintaining the power-raw distribution of scale-free networks at the same time. In this experiment, the number of nodes is 100, and the value of m is 2, and RD attack is selected as a malicious attack. As shown in Fig. 10, the comparison of the value of C before and after TMSE under random and malicious attacks is given. With the increase of the number of attack nodes, the value of C descends. Fig. 10(a) shows that when the random attack number is bigger than 25, the value of C after TMSE starts to be lower than that of the original network, but the difference is very small. This may be due to the partial connection of the original network that has been changed after TMSE, so its ability against random attacks is slightly reduced. In Fig. 10(b), it can be observed that the topology after TMSE improves the robustness against malicious attacks compared with the initial network. Besides, the value of C of the initial network decreases rapidly as the number of attacks increases, which means that the initial network is very vulnerable to malicious attacks. In contrast, C can still maintain 0.8 when the number of attacks is 20 after TMSE.

5.6. Convergence property of TMSE

To evaluate the convergence property of TMSE, we give the growth trend of robustness of two operations when $N = 50$. As shown in Fig. 11(a), under HDO operation, when the iteration round approaches 2000, the robustness tends to converge. In Fig. 11(b), when the iteration round over 3000, the robustness under DAO operation reaches the limit. Besides, from Fig. 11(b), we can observe that there are still some redundant operations that do not improve the robustness, and the reason is the randomness of independent edge selection in DAO

operation. However, the overall convergence and performance of TMSE is satisfactory.

6. Conclusions

Scale-free WSNs have attracted wide attention to the resistance to random attacks, but they are fragile for malicious attacks. This paper studies the strategy of improving the robustness of scale-free WSNs under malicious attacks. Considering the practical applications of WSNs, a fault-tolerant topology model with scale-free properties is introduced to generate the scale-free WSNs. The new strategy named TMSE is designed to improve the robustness of the scale-free topologies under malicious attacks. The HDO operation in TMSE improves robustness by changing the connection of high degree nodes, and the DAO operation makes the topology approach to an onion-like structure to enhance the robustness. Both HDO operation and DAO operation need the information of the entire network to support the selection of independent edges. So the implementation of improving robustness cannot directly be run in a distributed system. Besides, the resulted topology keeps the scale-free properties. The extensive experimental results show that TMSE can effectively improve the robustness against different types of malicious attacks compared with other algorithms, including SA and ROSE. Moreover, we will work on reducing the redundant operations to improve the convergence of the algorithm in the future.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Shihong Hu: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Writing - original draft, Writing - review & editing. **Guanghui Li:** Funding acquisition, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing - review & editing.

Acknowledgments

This work is partially supported by the National Natural Science Foundation of China (No. 61472368), Jiangsu Agriculture Science and Technology Innovation Fund, China (No. CX (19)3087), Wuxi International Science and Technology Research and Development Cooperative Project, China (No. CZE02H1706) and the Postgraduate Research & Practice Innovation Program of Jiangsu Province, China (No. KYCX_1862).

References

[1] K. Fukuda, et al., Transmit control and data separation in physical wireless parameter conversion sensor networks with event driven sensors, in: 2018 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet), 2018, pp. 12–14.
[2] H. Huang, T. Gong, R. Zhang, L. Yang, J. Zhang, F. Xiao, Intrusion detection based on k-coverage in mobile sensor networks with empowered intruders, IEEE Trans. Veh. Technol. 67 (12) (2018) 12109–12123.
[3] Y. Nishikawa, et al., Design of stable wireless sensor network for slope monitoring, in: 2018 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet), Anaheim, 2018, pp. 8–11.
[4] C. Wang, J. Li, Y. Yang, F. Ye, Combining solar energy harvesting with wireless charging for hybrid wireless sensor networks, IEEE Trans. Mob. Comput. 17 (3) (2018) 560–576.
[5] V.J. Hodge, S.O. Keefe, M. Weeks, A. Moulds, Wireless sensor networks for condition monitoring in the railway industry: A survey, IEEE Trans. Intell. Transp. Syst. 16 (3) (2015) 1088–1106.
[6] L. Azpilicueta, et al., Characterization of wireless channel impact on wireless sensor network performance in public transportation buses, IEEE Trans. Intell. Transp. Syst. 16 (6) (2015) 3280–3293.
[7] W. Tian, et al., Fog-based storage technology to fight with cyber threat, Future Gener. Comput. Syst. 83 (2018) 208–218.
[8] M. Younis, S. Lee, I.F. Senturk, K. Akkaya, Topology management techniques for tolerating node failure, in: The Art of Wireless Sensor Networks: Volume 1: Fundamentals, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, pp. 273–311.
[9] D. Czerwinski, S. Przylucki, P. Wojcicki, J. Sitkiewicz, Path loss model for a wireless sensor network in different weather conditions, in: Computer Networks, Cham, 2017, pp. 106–117.
[10] S.V.B. Heidelberg, Statistical mechanics of complex networks, Rev. Modern Phys. 74 (1) (2001) xii.
[11] A.L. Barabasi, R. Albert, Emergence of scaling in random networks, Science 286 (5439) (1999) 509–512.
[12] H. Liu, R. Yin, B. Liu, Y. Li, A scale-free topology model with fault-tolerance and intrusion-tolerance in wireless sensor networks, Comput. Electr. Eng. 56 (2016) 533–543.
[13] L. Liu, X. Qi, J. Xue, M. Xie, A topology construct and control model with small-world and scale-free concepts for heterogeneous sensor networks, Int. J. Distrib. Sens. Netw. 10 (3) (2014) 374251.
[14] G. Zheng, Q. Liu, Scale-free topology evolution for wireless sensor networks, Comput. Electr. Eng. 39 (6) (2013) 1779–1788.
[15] R.-H. Li, J.X. Yu, X. Huang, H. Cheng, Z. Shang, Measuring robustness of complex networks under MVC attack, in: Presented at the Proceedings of the 21st ACM International Conference on Information and Knowledge Management, Maui, Hawaii, USA, 2012.
[16] H. Petter, K. Beom Jun, Y.C. No, H. Seung Kee, Attack vulnerability of complex networks, Phys. Rev. E 65 (2) (2002) 056109.
[17] S. Hu, G. Li, Fault-tolerant clustering topology evolution mechanism of wireless sensor networks, IEEE Access 6 (2018) 28085–28096.
[18] I. Kleilat, H. Al-Sheikh, N. Moubayed, G. Hoblos, Robust fault diagnosis of sensor faults in power converter used in hybrid electric vehicle, IFAC-PapersOnLine 51 (24) (2018) 326–331.
[19] O. Lordan, M. Albareda-Sambola, Exact calculation of network robustness, Reliab. Eng. Syst. Saf. 183 (2019) 276–280.
[20] S.A. Markolf, C. Hoehne, A. Fraser, M.V. Chester, B.S. Underwood, Transportation resilience to climate change and extreme weather events – Beyond risk and robustness, Transp. Policy 74 (2019) 174–186.
[21] H. Wang, M. Li, L. Deng, B.-H. Wang, Robustness of networks with assortative dependence groups, Physica A 502 (2018) 195–200.
[22] J. Wang, C. Jiang, J. Qian, Robustness of internet under targeted attack: A cascading failure perspective, J. Netw. Comput. Appl. 40 (2014) 97–104.
[23] S. Wang, J. Liu, Designing comprehensively robust networks against intentional attacks and cascading failures, Inform. Sci. 478 (2019) 125–140.
[24] H.J. Herrmann, C.M. Schneider, A.A. Moreira, J.S. Andrade Jr, S. Havlin, Onion-like network topology enhances robustness against malicious attacks, J. Stat. Mech. Theory Exp. 2011 (1) (2011) P01027.
[25] Y. Hayashi, N. Uchiyama, Onion-like networks are both robust and resilient, Sci. Rep. 8 (1) (2018) 11241.
[26] T. Tanizawa, S. Havlin, H.E. Stanley, Robustness of onionlike correlated networks against targeted attacks, Phys. Rev. E 85 (4) (2012) 046109.
[27] T. Qiu, et al., ROSE: Robustness strategy for scale-free wireless sensor networks, IEEE/ACM Trans. Netw. 25 (5) (2017) 2944–2959.
[28] D.-R. Chen, L.-C. Chen, M.-Y. Chen, M.-Y. Hsu, A coverage-aware and energy-efficient protocol for the distributed wireless sensor networks, Comput. Commun. 137 (2019) 15–31.
[29] M. Manojprabu, V.R. Sarma Dhulipala, Improved energy efficient design in software defined wireless electroencephalography sensor networks (WESN) using distributed architecture to remove artifact, Comput. Commun. (2020).
[30] M.S. Yousefpoor, H. Barati, Dynamic key management algorithms in wireless sensor networks: A survey, Comput. Commun. 134 (2019) 52–69.
[31] P. Bosch, T. De Schepper, E. Zeljković, J. Famaey, S. Latré, Orchestration of heterogeneous wireless networks: State of the art and remaining challenges, Comput. Commun. 149 (2020) 62–77.
[32] H. Peng, S. Si, M.K. Awad, N. Zhang, H. Zhao, X.S. Shen, Toward energy-efficient and robust large-scale WSNs: A scale-free network approach, IEEE J. Sel. Areas Commun. 34 (12) (2016) 4035–4047.
[33] Y. He, W. Zhang, N. Jiang, X. Luo, The research of scale-free sensor network topology evolution based on the energy efficient, in: 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Guangdong, 2014, pp. 221–226.
[34] A. Zhao, T. Qiu, F. Xia, C. Lin, D. Luo, A scale-free network model for wireless sensor networks in 3D Terrain, in: Industrial IoT Technologies and Applications, Cham, 2016, pp. 201–210.
[35] T. Xiaobo, T. Ji, Y. Liting, W. Jialu, A new energy-efficient and fault-tolerant evolution model for large-scale wireless sensor networks based on complex network theory, Int. J. Distrib. Syst. Technol. (IJDST) 10 (3) (2019) 21–36.
[36] C.M. Schneider, A.A. Moreira, J.S. Andrade, S. Havlin, H.J. Herrmann, Mitigation of malicious attacks on networks, Proc. Natl. Acad. Sci. 108 (10) (2011) 3838.

[37] P. Buesser, F. Daolio, M. Tomassini, Optimizing the robustness of scale-free networks with simulated annealing, in: Adaptive and Natural Computing Algorithms, Berlin, 2011, pp. 167–176.
[38] L. Rong, J. Liu, A heuristic algorithm for enhancing the robustness of scale-free networks based on edge classification, Physica A 503 (2018) 503–515.
[39] S. Roy, V.K. Shah, S.K. Das, Design of robust and efficient topology using enhanced gene regulatory networks, IEEE Trans. Mol. Biol. Multi-Scale Commun. 2019 (Feb.) (2019) 1.
[40] W. Sun, M. Sun, J. Guan, Q. Jia, Robustness of coherence in noisy scale-free networks and applications to identification of influential spreaders, IEEE Trans. Circuits Syst. II (2019) 1.
[41] Z. Zhang, S. Liu, Y. Yang, Y. Bai, A link-adding strategy for improving robustness and traffic capacity in large-scale wireless sensor networks, Cluster Comput. 22 (2019).
[42] H. Ren, X. Huang, J. Hao, Finding robust adaptation gene regulatory networks using multi-objective genetic algorithm, IEEE/ACM Trans. Comput. Biol. Bioinform. 13 (3) (2016) 571–577.
[43] T. Qiu, J. Liu, W. Si, D.O. Wu, Robustness optimization scheme with multi-population co-evolution for scale-free wireless sensor networks, IEEE/ACM Trans. Netw. 27 (3) (2019) 1028–1042.
[44] NIST, Engineering Statistics Handbook: Exponential Distribution, 2011, Available: http://www.itl.nist.gov/div898/handbook/apr/section1/apr161.htm.
[45] M.R. Ismail, Exploiting irregular variable node degree in a MIMO system, in: 2006 10th IEEE Singapore International Conference on Communication Systems, 2006, pp. 1–5.
[46] V.H.P. Louzada, F. Daolio, H.J. Herrmann, M. Tomassini, Smart rewiring for network robustness, J. Complex Netw. 1 (2) (2013) 150–159.
[47] X.-C. Hao, Y.-X. Zhang, N. Jia, B. Liu, Virtual game-based energy balanced topology control algorithm for wireless sensor networks, Wirel. Pers. Commun. 69 (4) (2013) 1289–1308.
[48] M.E.J. Newman, Assortative mixing in networks, Phys. Rev. Lett. 89 (20) (2002) 208701.

Shihong Hu received the bachelor's degree in communication engineering from Jiangnan University in 2016. She is a Ph.D. candidate of the School of Internet of Things (IoT) Engineering, Jiangnan University. Her current research includes the fault-tolerance of wireless sensor network and edge computing.

Guanghui Li received the Ph.D. degree from the Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China, in 2005. He is currently a Professor with the Department of Computer Science, Jiangnan University, Wuxi, China. He has published over 70 papers in journal or conferences. His research interests include wireless sensor networks, fault tolerant computing, and nondestructive testing and evaluation. His research was supported by the National Foundation of China, Zhejiang, Jiangsu Provincial Science and Technology Foundation, and other governmental and industrial agencies.