Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 212074, 9 pages
http://dx.doi.org/10.1155/2013/212074

Research Article

A Betweenness Calibration Topology Optimal Control Algorithm for Wireless Sensor Networks

Ting Yang, Zhixian Lin, and Bo Yuan

School of Electrical Engineering and Automation, Tianjin University, Tianjin 300072, China

Correspondence should be addressed to Ting Yang; yangting@tju.edu.cn

Received 24 July 2013; Accepted 19 August 2013

Academic Editor: Zhaoxia Wang

In self-organized wireless sensor networks (WSNs), any two sensor nodes can connect if they are placed in each other's communication range. Therefore, the physical topology of WSNs is usually a strongly connected topology. Sensor nodes should frequently receive and process data from their large number of neighbors, which will consume great amounts of energy. Shocking wireless channel collision also causes low throughput and high loss packets ratio during data transmission. To improve the transmission performance and save scarce energy, a logical topology generating from the physical one is necessary for the self-organized WSNs. Based on the complex network theory, this paper proposed a novel *betweenness addition edges expansion* algorithm (BAEE). With betweenness calibration, BAEE algorithm expanded the minimum-cost edges to optimize the network topology. Two performance metrics-connectivity functions, robustness function $R(G)$ and efficiency function $E(G)$, were utilized to evaluate the network capability of the robustness and invulnerability. $R(G)$ is the parameter to measure the topology connectivity, and $E(G)$ is the parameter to evaluate the network exchanging information capability. Based on the simulation under various random failures and intentional attack scenarios, BAEE can effectively optimize WSNs' topology and improve the network's robust connectivity and extremely efficient exchanging information capability.

1. Introduction

Wireless sensor networks (WSNs) are a class of self-organized wireless communication networks, in which many sensor nodes collect, process, and exchange information acquired from the physical environment or the monitor objects and then send it to the external base station, called *Sink* [1]. WSNs have a wide range of potential applications including environment monitoring, smart grid, medical systems, and robotic exploration [2].

There are two main difficulties in WSNs' design: (1) the limited and nonreplenishable energy supply and (2) the limited transmission bandwidth and high packet loss rate caused by the out-of-order distributed communication. Hence, the energy control algorithm and robust infrastructure are necessary to prolong the networks' lifetime and improve the communication performance.

Topology optimal control (TOC) is to design a good logical network infrastructure, one of the key techniques used in wireless self-organized sensor networks [3]. In a network, if there is at least one route to connect any two sensor nodes, such network is regarded as a connected one. Because of the omnidirectional antenna, any two nodes in WSNs can communicate if the *Euclidean* distance between them is less than the communication range. Therefore, the physical topology of WSNs is usually a strongly connected topology. Any node will frequently receive and process data from the quantity of its neighbors, which will consume great amounts of energy. The minimum energy network connectivity (MENC) problem was defined and proved to be an NP-complete problem [4].

In the research on TOC, the previous research can be classified into two types based on the optimized objects: physical topology control algorithms (PTCA) and logical topology control algorithms (LTCA) [5, 6]. PTCA adjust sensor nodes' transmission power to control the physical topology. On the other hand, LTCA restrict one node connected with a certain number of neighbors to satisfy the network connectivity. This neighbor reduction mechanism helps to reduce the routing overhead and relieve the channel collision problems.

Different from the wired communication network, such as IP network, WSN is one type of dynamic networks.

There are many factors causing the dynamic structure—from system hardware to application—for unattended sensor nodes with miniature sizes (mm scale for smart dust motes), limited battery-power, and low reliable hardware circuits when coping with harsh conditions. Other factors that may affect network connectivity and communication among sensor nodes are fading, signal strength, obstacles, weather conditions, interference, and so forth [7, 8]. An immutable topology structure is not enough for the WSNs, and any dynamic change will break original optimization and reduce the network performance.

To overcome this critical problem, this paper proposed a novel *betweenness addition edges expansion* algorithm (BAEE). With the betweenness parameter, BAEE algorithm expanded the minimum-cost edges to optimize the network topology with maximum improving of the efficiency function values. The preliminary simulation results, compared with *Fiedler-vector-based* strategy, showed that our algorithm could obtain more robust topology with higher invulnerability under both the random failures and intentional attack scenarios.

This paper is organized as follows. Section 1 introduces the TOC problem in WSNs, and Section 2 presents the related work. The problem's mathematic description and model building are presented in Section 3. Section 4 proposes the BAEE algorithm in detail. Section 5 presents simulation results to demonstrate the effectivity of the algorithm. Section 6 concludes the paper.

2. Related Work

There are three types of approaches in the previous TOC research presented as follows. (1) Control each node's emission power to reduce the strong connectivity of the physical topology and to effectively save the energy consumption and prolong network lifespan. Rodoplu and Meng [9] introduced the notion of relay region and enclosure for the purpose of power control. It was shown that the network was strongly connected if every node maintained links with the nodes in its enclosure. With reducing the transmission power, the topology connectivity becomes thin. Building a minimum-power-connected topology is a multiobjective optimization problem. (2) Reduce the total number of working nodes in WSNs, and let other nodes suspend to hibernate. It can also reduce the topology complexity. Moreover, the approach helps to reduce the interference that exists in wireless network, which means that a greater signal-to-noise ratio will be obtained at receiving nodes. The most common schemes based on this principle are sensor-MAC (S-MAC) [10], timeout-MAC (T-MAC) [11], and data-gathering MAC (D-MAC) [12]. (3) Control sensor node's logical degree in its logical topology, thus helping to reduce MAC layer contention and improve space reuse. A less node's logical degree may also help to mitigate the hidden and exposed terminal problems. Clustering topology control strategy is one of the effective approaches, similar to spanning-tree structure in WSN. The low-energy adaptive clustering hierarchy (LEACH) [13] is the most notable clustering algorithm for wireless sensor networks. LEACH combines the ideas of energy-efficient cluster with application-specific data aggregation to achieve good performance. Its improved algorithm, power-efficient gathering in sensor information systems (PEGASIS) [14], is a chain-based clustering scheme. Another effective topology structure is the spanning-tree [15]. Li et al. [16] proposed a fully distributed topology control algorithm called LMST. A similar method, k-local MST, was addressed by Li et al. [17].

With the number of sensor nodes increasing, the topology of large-scale WSNs becomes more and more complex, and TOC, as a type of multiobjective optimization problems, is very difficult to explore the global optimal solution, such as the degree-constrained minimum spanning-tree problem. Some heuristic methods were developed to improve the optimization performance [18–23]. In [18], the authors proposed two heuristics based on a minimum spanning-tree algorithm and a broadcast incremental power method, respectively. Konstantinidis developed a genetic algorithm with local search that performs better than the MST heuristic [19]. Guo presented an improved discrete particle swarm optimization algorithm for generating topology schemes [20]. A simulated annealing algorithm was designed in [21], and it is also applied to solve the problem of minimizing broadcast tree, one type of the physical topology control problems [22]. In [23], ant colony optimization, a framework inspired by the ant foraging behavior in the area of swarm intelligence, is applied to physical topology control.

The above heuristic algorithms focused on the solution procedure of optimization problem itself, in which topology control had been abstracted into the multiobjective optimization problem. On the different view to analyze the topology control problem, we use the complex network theory to calculate the network's long-range and short-range connectivity, and then a novel BAEE algorithm is proposed to improve the networks' robustness and invulnerability with the minimum-cost edges expanded.

3. The Network Model and the Parameters of Complex Network

The formal definition of the TOC problem in WSNs is presented as follows. In a special sensor area, there are a set of n wireless nodes $V = \{v_1, v_2, \ldots, v_n\}$. $E = \{e_1, e_2, \ldots, e_n\}$ is the set of communication links. When an adjacent pair v_j, v_k shows the same wireless medium, $e_i(v_j, v_k)$ indicates that both nodes are within their wireless transmitting ranges λ_0; that is, $E = \{e_i(v_j, v_k) \mid D(v_j, v_k) \leq \lambda_0, v_j, v_k \in V\}$. Therefore, the wireless sensor network is represented as a simple digraph $G = (V, E)$. Because of the omnidirectional antenna, in WSNs, any two nodes can communicate if the *Euclidean* distance between them is less than the communication range. Therefore, WSNs' topology is usually strongly connected. The complex network theory is utilized to analyze this type of strongly connected topology in this paper. Some parameters of complex network are presented firstly in the following section.

3.1. The Parameters of Complex Network. A complex network's attribute can be described by its key parameters: degree

distribution, clustering coefficient, average path length, and betweenness [24, 25].

(1) Cumulative Degree Distribution Function. The degree of a node in a network is the number of connections, and the degree distribution $p(k')$ is the probability distribution of these degrees over the whole network. The cumulative degree distribution function $P_c(k)$ is the probability distribution of all of the nodes whose degree is not less than k. Consider the following:

$$P_c(k) = \sum_{k' \geq k}^{k_{\max}} p\left(k'\right). \tag{1}$$

(2) Clustering Coefficient. In graph theory, a clustering coefficient is a measure of the degree to which nodes in a graph tend to cluster together. Firstly, the local clustering coefficient C_i of a node v_i in a graph quantifies how close its neighbors are to being a clique, that is, complete graph. Let $\lambda_G(v)$ be the number of triangles on $v \in V(G)$ for undirected graph G. That is, $\lambda_G(v)$ is the number of subgraphs of G with three edges and three nodes, one of which is v. Let $T_G(v)$ be the number of triples on $v \in V(G)$. That is, $T_G(v)$ is the number of subgraphs (not necessarily induced) with two edges and three nodes, one of which is v such that v is incident to both edges. Then, local clustering coefficient C_i can be defined as

$$C_i = \frac{\lambda_G(v)}{T_G(v)}. \tag{2}$$

The clustering coefficient for the whole network is given as the average of the local clustering coefficients of all of the nodes N as follows:

$$C = \frac{1}{N} \sum_{i=1}^{N} C_i. \tag{3}$$

Evidence suggests that, in most real-world networks, nodes tend to create tightly knit groups characterized by a relatively high density of ties; this likelihood tends to be greater than the average probability of a tie randomly established between two nodes.

(3) Average Path Length. Average path length L is defined as the average number of steps along the shortest paths for all possible pairs of network nodes. It is a measure of the efficiency of information or mass transport on a network. The definition is shown as

$$L = \frac{1}{N(N-1)/2} \sum_{1 \leq i, j \leq N} d_{i,j}. \tag{4}$$

Average path length is one of the most robust measures of network topology.

(4) Betweenness. There are two definitions: the vertex betweenness $B(v)$ and the edge betweenness $B(e)$. Here, we used the $B(v)$ as the example. Betweenness $B(v)$, a centrality measure of a node within a graph, centrality quantifies the number of times a node acts as a bridge along the shortest path between two other nodes. Consider the following:

$$B(v) = \sum_{v \neq i, v \neq j, i \neq j} \frac{\sigma_{ij}(v)}{\sigma_{ij}}. \tag{5}$$

Here, σ_{ij} is the total number of the shortest paths from node i to node j, and $\sigma_{ij}(v)$ is the number of those paths that pass through v.

3.2. Two Evaluation Functions for Measuring the Network's Robustness and Invulnerability. Based on the above four parameters, connectivity robustness function and efficiency function can be defined and utilized to evaluate the network's robustness and invulnerability.

(1) Connectivity Robustness Function $R(G)$. Connectivity robustness refers to maintaining the connection capability of the remaining nodes when some of the nodes or edges in the network were removed [26]. In the network $G = (V, E)$ with n nodes, the connectivity robustness is defined as follows:

$$R(G) = \frac{S\left(G'\right)}{N - N_r}. \tag{6}$$

Here, $S(G')$ is the largest connected component remaining after the removal of N_r nodes. The connectivity robustness is normalized; that is, $0 < R(G) \leq 1$. The maximum value of the connectivity robustness function $R(G) = 1$ is obtained in the case that G' is also a connected graph after N_r nodes were removed.

(2) Efficiency Function $E(G)$. Instead of L and C, the network is characterized in terms of how efficiently it propagates information on a global and on a local scale, respectively defined as the *global efficiency function* $E_{\text{glob}}(G)$ and *local efficiency function* $E_{\text{loc}}(G)$ [25, 27]. We assume that the efficiency ε_{ij} in the communication between nodes i and j is inversely proportional to the shortest distance: $\varepsilon_{ij} = 1/d_{ij}$, $\forall i, j$. In this definition, when there is no path in the graph between i and j, $d_{ij} = +\infty$, and consistently $\varepsilon_{ij} = 0$. The global efficiency of the graph G can be defined as

$$E_{\text{glob}}(G) = \frac{\sum_{i \neq j \in G} \varepsilon_{ij}}{N(N-1)} = \frac{1}{N(N-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}}. \tag{7}$$

The local efficiency function can be defined as the average efficiency of local subgraphs as follows:

$$\begin{aligned} E_{\text{loc}}(G) &= \frac{1}{N} \sum_{i \in G} E\left(G_i\right), \\ E_{\text{loc}}(G) &= \frac{1}{k_i\left(k_i - 1\right)} \sum_{l \neq m \in G} \frac{1}{d'_{lm}}, \end{aligned} \tag{8}$$

where G_i is the subgraph of the neighbors of i, which is made by k_i nodes and at most $k_i\ (k_i - 1)/2$ edges. It is important

to notice that the quantities $\{d'_{lm}\}$ are the shortest distances between nodes l and m calculated on the graph G_i.

Both the global and the local efficiency are already normalized; that is, $0 \le E_{\text{glob}}(G) \le 1$, and $0 \le E_{\text{loc}}(G) \le 1$. The maximum values of the efficiency $E_{\text{glob}}(G) = 1$ and $E_{\text{loc}}(G) = 1$ are obtained in the ideal case of a completely connected graph, that is, in the case in which the graph G has all of the $N(N-1)/2$ possible edges and $d_{ij} = 1,\ \forall i, j$.

In the efficiency-based formalism, a network is extremely efficient in exchanging information both on a high global and local efficiency functions value. Moreover, the description of a network in terms of its efficiency can be extended to unconnected networks and, more important, with only a few modifications, to weighted networks. A weighted network is a case in which there is a weight associated with each of the edges. Such a network needs two matrices to be described. Consider the following.

(1) The usual adjacency matrix $[a_{ij}]$ telling about the existence or nonexistence of a link is defined as follows:

$$a_{ij} = \begin{cases} 1, & e_{ij} \in E, \\ 0, & \text{otherwise.} \end{cases} \tag{9}$$

(2) The second weights matrix associated with each link $[w_{ij}]$, where w_{ij} can be defined as communication cost, depended on the optimal problem. Obviously, weighted network optimal problem, such as TSP (traveling salesman problem), is more complex than topology control.

In this paper, we focus instead on the simpler case of unweighted networks topology. We will use the connectivity robustness function and the global efficiency function to evaluate the network's robustness and invulnerability under the random failures and the intentional attacks.

4. Description of Betweenness Addition Edges Expansion Algorithm

In order to improve the network's robustness and invulnerability under the random failures and the intentional attacks, a novel betweenness addition edges expansion algorithm is proposed. Based on the traffic analysis in practical WSNs, we find that the communication connection is established usually by events driven, in which both the vertex betweenness B_{vet} and edge betweenness B_{edg} follow heavy-tailed distribution. As in the above definition, the betweenness is the number of the shortest paths through node v_i or edge e_i, which shows the importance of v_i and e_i in network transmission. The vertex v_i with high-betweenness B_{vet} bears more packets switching, which is the core vertex in the network. The edge e_i with high-betweenness B_{edg} bears more traffic flows, which is the key edge for the network's connectivity. In order to improve the networks robustness and avoid transmitting congestion, network's core parts should be identified. BAEE carefully selects special vertex parts and connects edges with betweenness addition strategy. After the optimal operation, the network diameter can be effectively reduced, and the transmission delay will be shortened. BAEE process is given as follows.

(1) According to the vertex betweenness $B(v)$ formula and network adjacency matrix $[A]_{n\times n}$, each vertex betweenness is calculated and saved in the column vector $\overline{B}_n$. Consider the following:

$$\overline{B}_n = \left[b\left(v_1\right), b\left(v_2\right), \ldots, b\left(v_n\right)\right]^T. \tag{10}$$

(2) Using the vector betweenness column vector $\overline{B}_n$, a new betweenness plus column vector $[\overline{B}^+]_m$ is calculated, where $m = C_n^2$, as follows:

$$\begin{gathered} \overline{B}^+(k) = b\left(v_i\right) + b\left(v_j\right), \\ k = (i-1) \times n + j. \end{gathered} \tag{11}$$

(3) Sort $[\overline{B}^+]_m$ in descending order and generate $[\overline{B}^+]'_m$. Here, we used the bubble method to sort column vector $[\overline{B}^+]_m$, which has lower space complexity $O(1)$ and better stability compared with other sorting algorithms. Then, the elements in front of $[\overline{B}^+]'_m$ have larger value of betweenness addition.

The process of the bubble method is shown as follows

(a) Compare the first element, that is, 0th, with the latter element; if smaller, then switch. Sequentially compare m times element and eventually change the smallest value element into mth unit; the element $b(m)$ does not move anymore.

(b) Repeat step (a), and sequentially compare until the $(m-1)$th element. Eventually, the minimum value in the front of $(m-1)$ elements is moved to the $(m-1)$th unit. $b(m-1)$ does not move.

⋮

(m) Compare $b(0)$ and $b(1)$; if $b(0) < b(1)$, switch each other. Then, $b(0)$ is maximum, and the array is in descending order. The bubble method terminates.

(4) Check $[\overline{B}^+]'_m$ from the first elements $b^+(0)$. For $\overline{B}^+(k) = b(v_i) + b(v_j)$ if vertex parts v_i and v_j have connection edge, that is, $e(v_i, v_j) \in E$, then check the next element of $[\overline{B}^+]'_m$.

(5) Else, if $e(v_i, v_j) \notin E$, then add an edge between vertex parts v_i and v_j. Then, calculate the connectivity robustness function $R(G)$ and efficiency function $E(G)$.

(6) If both $R(G)$ and $E(G)$ reach the optimization requirements, the algorithm terminates. Otherwise, return to step (4) to look for other connected edges.

BAEE algorithm is presented in Algorithm 1.

According to the above optimization approach, the experimental simulation was taken to evaluate the algorithm's performance. The detailed analysis about results was shown in the following section.

5. Simulation and Performance Evaluation

The simulation scenario is that 100 sensor nodes were randomly placed in a 900 m × 900 m field. Each node's radio propagation range is 300 m. After the self-organized process, a strongly connected physical topology is established. To reduce the interference, the neighbors of each sensor node are control based on the traffic requirements, and then a logical topology is generated, which is the topology that we really need for data transmission, shown in Figure 1.

The connectivity robustness function $R(G)$ and efficiency function $E(G)$ for the initial network are calculated as follows: $R(G) = 1$, because it is a connected graph; $E(G) = 0.226$. In the simulation, BAEE algorithm is used to optimize the network topology, compared with *Fiedler-vector-based strategy* (FVBS), another well-known method for TOC presented in [28]. FVBS main idea is adding a link between a node pair with the maximal $|u_i - u_j|$, the absolute difference between the ith and jth elements of the Fiedler vector of G. Because the Fiedler vector is related to the algebraic connectivity of G, to maintain the fairness of evaluation, the simulation results are analyzed through the connectivity robustness function $R(G)$ and efficiency function $E(G)$, except for the algebraic connectivity.

In the simulation, firstly, using BAEE and FVBS to optimize the original topology, the new topologies G'_{BAEE} and G'_{FVBS} are generated. To maintain the fairness, the same number of edges is added in G'_{BAEE} and G'_{FVBS}, shown in Table 1.

Then, the identical random failures and the intentional attacks are applied on the two G'. The robustness and invulnerability are evaluated by the two performance metrics $R(G)$ and $E(G)$.

5.1. The Experiments under Random Failures. Random failures mean that nodes in the network are randomly failed, and at the same time the edges connecting with the failure nodes are also failed. Because of the low reliable hardware circuits, the limited battery-power, and the harsh wilderness conditions, the case of sensor node failed often occurs in the practical application. Figure 2 shows the connectivity robustness function value for the increasing of the number of random failure nodes. From Figure 2, we can observe that the two optimized topologies have higher R value than the original network confronting random failures. Moreover, BAEE is better than FVBS; the R value has an average 5.23% increase, which means that the optimized network has the stronger capability of maintaining connectivity. Different from the other two curves, the $R(G'_{\mathrm{BAEE}})$ curve of BAEE is stable. For example, at 11 failure nodes scenario, the $R(G'_{\mathrm{BAEE}})$ curve does not shake, different from the sharp decline of $R(G'_{\mathrm{FVBS}})$ and $R(G)$ curves, which indicates that BAEE algorithm has better "resistance."

Figure 3 shows the efficiency function $E(G)$ under random failures. As the number of the failure nodes increases, the efficiency function of the three networks decreases. The reason is that failure nodes make certain shortest paths broken. But $E(G'_{\mathrm{BAEE}})$ is higher than $E(G'_{\mathrm{FVBS}})$ and $E(G)$, whose increase rates are 13.78% and 23.59%, respectively. This is extreme efficiency showed that BAEE algorithm can optimize network and reach extreme efficiency in exchanging information for ubiquitous data-centric wireless sensor networks.

5.2. The Experiments under Intentional Attacks. Intentional attack is another kind of accident for wireless sensor networks. Based on partial information of network, enemy can accurately attack the weakest parts and break down the whole system. So a network should have more robust topology to resist intentional attacks. In the following experiments, two types of attacks are simulated: (1) make nodes with high vertex betweenness fail; (2) make links with high edge betweenness fail. The two metrics $R(G)$ and $E(G)$ are also used to measure the algorithms' performance.

Figure 4 presents the connectivity robustness function $R(G)$ under the intentional attacks with high-betweenness nodes failed. From the three curves, we can find that both BAEE and FVBS algorithms improve the original network's invulnerability. G'_{BAEE} is also stronger than G'_{FVBS} when the number of failed nodes is more than 6. The gap is 25.74% approximately. When the number of failed nodes is continually increasing and more than 13, the values of $R(G'_{\mathrm{BAEE}})$ and $R(G'_{\mathrm{FVBS}})$ have a sharp decline and coincide with $R(G)$. The reason is that the original network has its inherent structure quality, and TOC algorithms can just improve the network performance limited.

The efficiency function $E(G)$ against nodes' failure is shown in Figure 5. BAEE algorithm optimized the network and reached a high value of $E(G'_{\mathrm{BAEE}})$. The average is higher than $E(G'_{\mathrm{FVBS}})$ 22.98%. Moreover, we found that the same two aberration points, occurring in above experiments, also appear in this experiment: when the number of failed nodes is more than 6, $E(G'_{\mathrm{FVBS}})$ and $E(G)$ curves present a dump, but the network topology optimized by BAEE algorithm escapes this shake, showing stronger stability. When the number of failed nodes is more than 13, both $E(G'_{\mathrm{BAEE}})$ and $E(G'_{\mathrm{FVBS}})$ have a sharp decline and coincide with $E(G)$, proving the network's inherent structure quality.

Another attack strategy, high-betweenness links failed, is implemented in the experiments. The top 20 high-betweenness links are sequentially broken to evaluate the network's performance; the curves of $R(G)$ are presented in Figure 6. The results show that, under the high-betweenness edges' attack, FVBS algorithm cannot improve the network's invulnerability capability anymore, shown as the two curves $R(G'_{\mathrm{FVBS}})$ and $R(G)$ coinciding. However, BAEE algorithm is effective under this kind of attack. While the broken links are less than 12, $R(G'_{\mathrm{BAEE}})$ is higher than $R(G'_{\mathrm{FVBS}})$ and $R(G)$ 9.89% averagely.

Figure 7 presents the efficiency function $E(G)$ under the edges intentional attack. BAEE also reaches a higher $E(G'_{\mathrm{BAEE}})$ value than FVBS $E(G'_{\mathrm{FVBS}})$ and original network $E(G)$, in

Betweenness Addition Edges Expansion algorithm

(1) Calculate each vertex's betweenness with the vertex betweenness $B(v)$ formula:

$$B(v) = \sum_{v \neq i, v \neq j, i \neq j} \frac{\sigma_{ij}(v)}{\sigma_{ij}}$$

(2) Save each vertex betweenness $B(v)$ in the column vector $\overline{B_n} = [b(v_1), b(v_2), \ldots, b(v_n)]^T$;
(3) **For** $i = 0$ to n
(4) **For** $j = i + 1$ to n
(5) $k = (i-1) \times n + j$; $\overline{B}^+(k) = b(v_i) + b(v_j)$;
(6) **End for**
(7) **End for**
(8) **For** $i = 0$ to $n * (n-1)/2$
(9) **For** $j = i + 1$ to $n * (n-1)/2$
(10) **If** $\overline{B}_i^+ < \overline{B}_j^+$
(11) Switch $\overline{B}_i^+$ and $\overline{B}_j^+$;
(12) **End for**
(13) **End for**
(14) **For** $k = 0$ to $n * (n-1)/2$
(15) **If** no edge connected vertex parts v_i and v_j, that is, $e(v_i, v_j) \notin E$ //here $\overline{B}^+(k) = b(v_i) + b(v_j)$
(16) $a[i][j] = a[j][i] = 1$; //here $a[][]$ is the element of adjacency matrix $[A]_{n \times n}$;
(17) **End if**
(18) **If** $R(G) > R(G)_{\text{req}}$ && $E(G) > E(G)_{\text{req}}$
(19) Break;
(20) **End for**

Algorithm 1: Pseudocode of BAEE algorithm.

Table 1: Added edges in G'_{BAEE} and G'_{FVBS}.

G'_{BAEE}	(61, 79)	(80, 34)	(45, 78)	(51, 2)	(54, 73)	(50, 57)	(55, 22)	(56, 68)
G'_{FVBS}	(100, 1)	(100, 2)	(99, 1)	(100, 3)	(99, 2)	(100, 4)	(99, 3)	(100, 5)

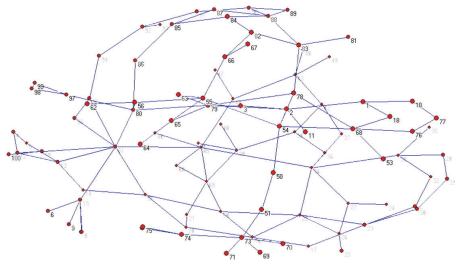

Figure 1: Original logical topology of WSN.

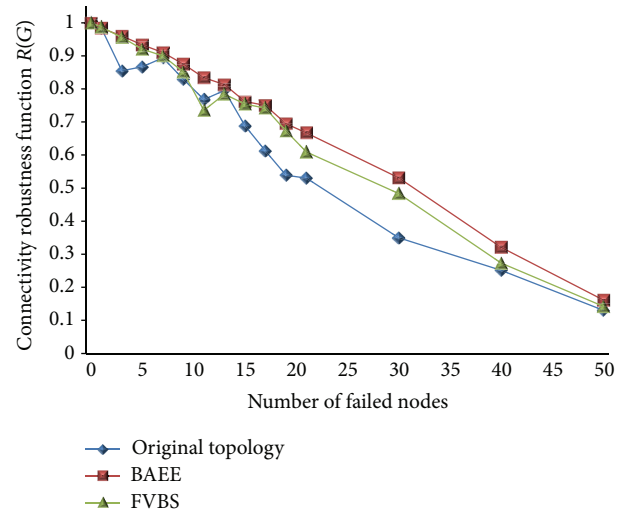

Figure 2: Connectivity robustness function versus the number of failed nodes under random failures.

which an average increasing rate is 31.41% for $E(G'_{\text{FVBS}})$ and 50.88% for $E(G)$. These results indicate that BAEE algorithm has obvious advantages against edges intentional attacks.

6. Conclusions

Because of the omnidirectional antenna, in WSNs, any two sensor nodes can connect if they are placed in each other's communication range. Therefore, the physical topology of WSNs is usually a strongly connected topology. Anyone should frequently receive and process data from the quantity of its neighbors, which will consume large amounts of energy. Shocking wireless channel collision also causes low throughput and high loss packets ratio in data transmission. To improve the WSNs transmission efficiency and save scarce

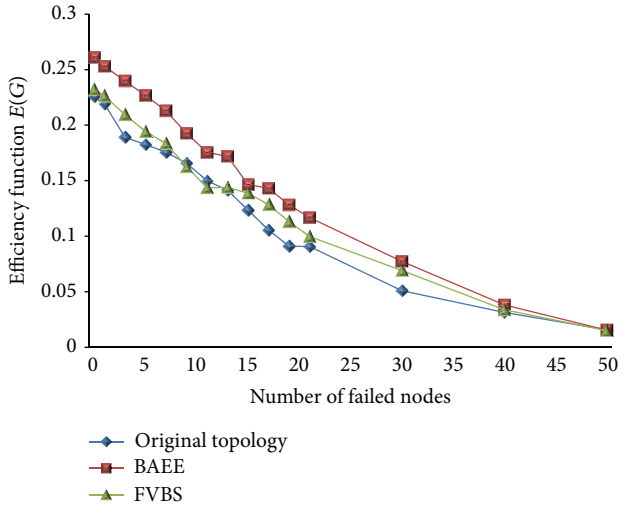

Figure 3: Efficiency function versus the number of failed nodes under random failures.

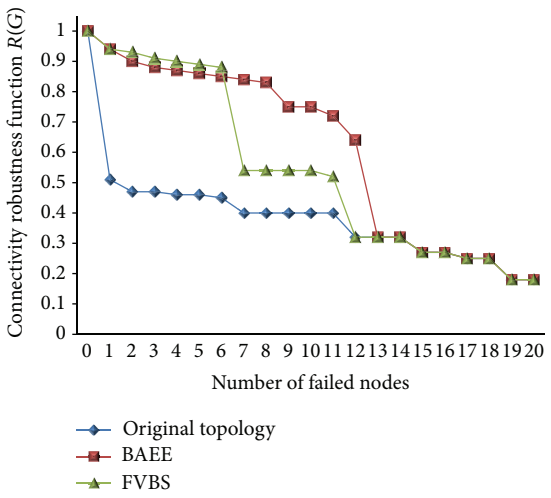

Figure 4: Connectivity robustness function versus the number of failed nodes under intentional attack.

energy, a logical topology generating from a physical one and further dynamic optimization are necessary for the self-organized wireless sensor networks.

With topology vulnerability analysis, this paper proposes one topology optimization control algorithm—BAEE. The algorithm calculates the vertex betweenness and expanded special edges with the minimum cost. Two metrics, the connectivity robustness function $R(G)$ and efficiency function $E(G)$, are utilized to measure the network performance. $R(G)$ is the metric to measure topology connectivity, and $E(G)$ is the metric to evaluate the network exchanging information capability. Detailed definitions are presented in this paper. Using numerical experimental simulations under various random failures and intentional attack scenarios, we measured the performance of BAEE and compared it with the Fiedler-vector-based strategy in TOC. Results were very

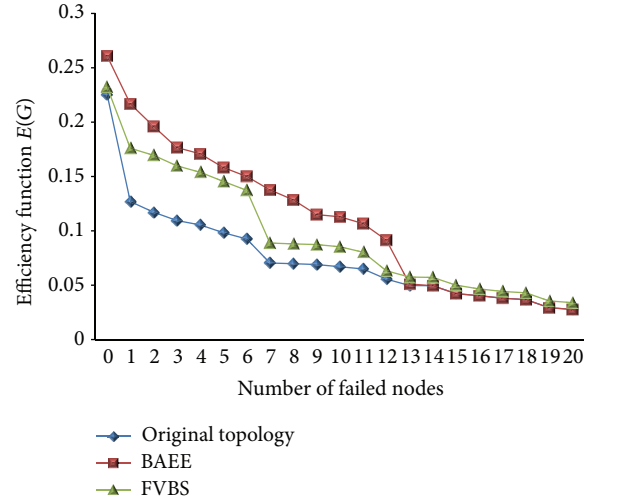

Figure 5: Efficiency function versus the number of failed nodes under intentional attack.

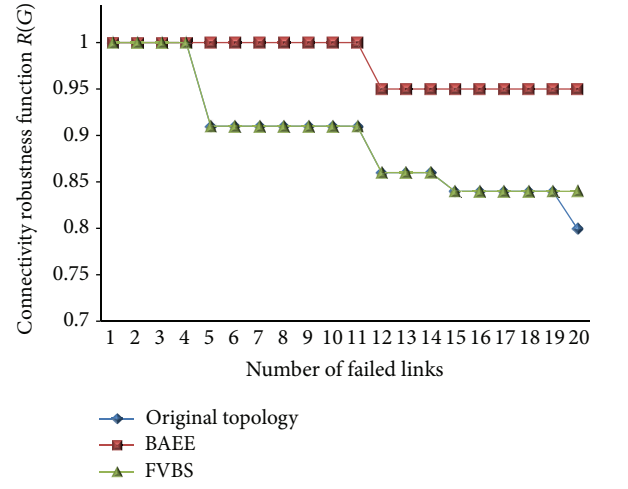

Figure 6: Connectivity robustness function versus the number of failed links under intentional attack.

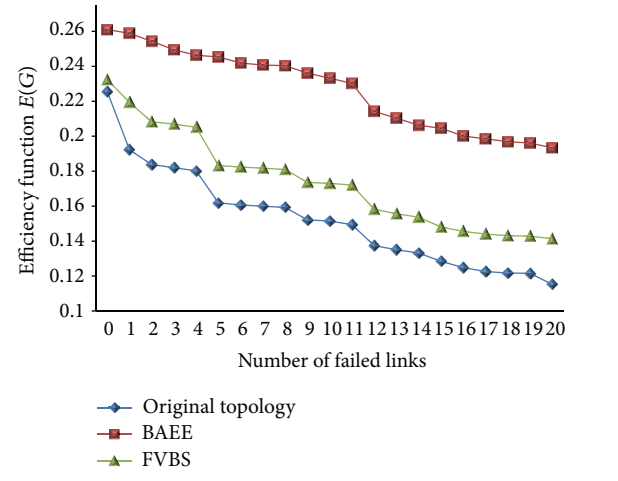

Figure 7: Efficiency function versus the number of failed links under intentional attack.

promising and showed that our novel algorithm's performance is much better than others in reaching high connectivity robustness function value and efficiency function value, which means that the optimized network by BAEE has robust connectivity and extremely efficient exchanging information capability.

Acknowledgments

This work was sponsored by the National Natural Science Foundation of China no. 61172014, the Natural Science Foundation of Tianjin no. 12JCZDJC21300, and the National Program of International S&T Cooperation no. 2013DFA11040.

References

[1] R. V. Kulkarni, A. Förster, and G. K. Venayagamoorthy, "Computational intelligence in wireless sensor networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 1, pp. 68–96, 2011.

[2] A. Alamri, W. S. Ansari, M. M. Hassan et al., "A survey on sensor-cloud: architecture, applications, and approaches," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 917923, 18 pages, 2013.

[3] N. Ababneh, "Performance evaluation of a topology control algorithm for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2010, Article ID 671385, 17 pages, 2010.

[4] W. Chen and N. Huang, "Strongly connecting problem on multihop packet radio networks," *IEEE Transactions on Communications*, vol. 37, no. 3, pp. 293–295, 1989.

[5] C. C. Shen and Z. Huang, "Topology control for Ad Hoc networks: present solutions and open issues," in *Handbook on Theoretical and Algorithmic Aspects of Sensor, Ad Hoc Wireless, and Peer-to-Peer Networks*, J. Wu, Ed., CRC Press, New York, NY, USA, 2005.

[6] W. Song, X. Li, O. Frieder, and W. Wang, "Localized topology control for unicast and broadcast in wireless ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 17, no. 4, pp. 321–334, 2006.

[7] M. Y. Aalsalem, J. Taheri, and A. Y. Zomaya, "A framework for real time communication in sensor networks," in *Proceedings of the 2010 ACS/IEEE International Conference on Computer Systems and Applications (AICCSA '10)*, pp. 1–7, May 2010.

[8] T. Yang, Y. Sun, J. Taheri, and A. Y. Zomaya, "DLS: a dynamic local stitching mechanism to rectify transmitting path fragments in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 306–315, 2013.

[9] V. Rodoplu and T. H. Meng, "Minimum energy mobile wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1333–1344, 1999.

[10] W. Ye, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," *IEEE/ACM Transactions on Networking*, vol. 12, no. 3, pp. 493–506, 2004.

[11] T. van Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," in *Proceedings of the International Conference on Embedded Networked Sensor System*, pp. 171–180, November 2003.

[12] G. Lu, B. Krishnamachari, and C. S. Raghavendra, "An adaptive energy-efficient and low-latency MAC for data gathering in wireless sensor networks," in *Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS '04)*, pp. 3091–3098, April 2004.

[13] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.

[14] S. Lindsey and C. S. Raghavendra, "PEGASIS: power-efficient gathering in sensor information systems," in *Proceedings of the IEEE Aerospace Conference*, vol. 3, pp. 1125–1130, 2002.

[15] Y. Ting and K. ChunJian, "An energy-efficient and fault-tolerant convergecast protocol in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 429719, 8 pages, 2012.

[16] N. Li, J. C. Hou, and L. Sha, "Design and analysis of an MST-based topology control algorithm," in *Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies (IEEE INFOCOM '03)*, vol. 3, pp. 1702–1712, April 2003.

[17] X. Li, Y. Wang, and W. Song, "Applications of κ-local MST for topology control and broadcasting in wireless Ad Hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 15, no. 12, pp. 1057–1069, 2004.

[18] M. X. Cheng, M. Cardei, J. Sun et al., "Topology control of ad hoc wireless networks for energy efficiency," *IEEE Transactions on Computers*, vol. 53, no. 12, pp. 1629–1635, 2004.

[19] A. Konstantinidis, Z. Qingfu, Y. Kun, and H. Ian, "Energy-aware topology control in sensor networks using modern heuristics," in *Proceedings of the Global Telecommunications Conference (IEEE GLOBECOM '06)*, pp. 1–5, December 2006.

[20] W. Guo, H. Gao, G. Chen, H. Cheng, and L. Yu, "A PSO-based topology control algorithm in wireless sensor networks," in *Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '09)*, pp. 3406–3409, September 2009.

[21] L. F. Liu and Y. Liu, "Topology control scheme based on simulated annealing algorithm in wireless sensor networks," *Tongxin Xuebao/Journal on Communications*, vol. 27, no. 9, pp. 71–77, 2006.

[22] R. Montemanni, L. M. Gambardella, and A. K. Das, "The minimum power broadcast problem in wireless networks: a simulated annealing approach," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '05)*, vol. 4, pp. 2057–2062, March 2005.

[23] Z. Huang and C. C. Shen, "Distributed topology control mechanism for mobile Ad Hoc networks with swarm intelligence," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 3, pp. 21–22, 2003.

[24] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 47–97, 2002.

[25] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Physical Review Letters*, vol. 87, no. 19, Article ID 198701, pp. 1–4, 2001.

[26] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, "Resilience of the Internet to random breakdowns," *Physical Review Letters*, vol. 85, no. 21, pp. 4626–4628, 2000.

[27] V. Latora and M. Marchiori, "Economic small-world behavior in weighted networks," *European Physical Journal B*, vol. 32, no. 2, pp. 249–263, 2003.

[28] H. Wang and P. V. Mieghem, "Algebraic connectivity optimization via link addition," in *Proceedings of the 3rd International Conference on Bio-Inspired Models of Network, Information and Computing Sytems (BIONETICS '08)*, pp. 1–8, 2008.