

Research on Invulnerability of Wireless Sensor Networks Based on Complex Network Topology Structure

<https://doi.org/10.3991/ijoe.v13i03.6863>

Zhigang Zhao

Zhejiang University of Media and Communications, Hangzhou Zhejiang, China
zhaozhig2006@126.com

Abstract—For real-world wireless sensor networks (WSNs), the invulnerability of the network is very critical, because a cascading failure would cause a serious effect on the whole network performance. Network survivability is closely dependent on the topology structure of a network. In this paper, [Note: If you use "firstly," you need to add "secondly," "thirdly,"... "finally" throughout this paragraph; I don't see a need for this here] we meticulously study the topology characteristics of WSNs based on the complex network theory. According to scale-free and small-world features of complex networks, the nodes of WSNs are divided into different types, including common node, super node, and sink node. From the point of view of invulnerability in complex networks, the influence of different types of nodes on the sensor networks' invulnerability is analyzed. Simulation experiments show that adding super nodes to the WSNs would significantly improve network survivability.

Keywords— Wireless sensor networks; Complex networks; Network Topology; Network survivability.

1 Introduction

WSNs are remotely located autonomous networks which consist of a great number of wireless sensors with wireless information transmission functions [1]. WSNs are widely used in the following domains: environmental monitoring, heat transfer, industrial process monitoring and control, traffic control, military, and so on [2, 3].

In general, WSNs consist of hundreds of wireless sensors which are connected with other sensors. Because they are battery-operated and remotely-deployed, sensor nodes in WSNs are prone to malware attacks [4]. Hence, how to ensure network survivability is one of the crucial problems in WSNs.

There are many realistic systems which can be described in terms of complex networks in nature and society [5], such as online social networks [6,7], protein-protein interaction networks [8], the Internet [9,10], and transportation networks [11,12]; therefore, a wide range of specialists have paid considerable attention to the topology structure characteristics of complex networks.

There are two well-known types of complex networks: scale-free networks [13] and small-world networks [14,15]. This discovery and definition of the two networks

indicate that the research of complex network topology has entered a new era. The scale-free networks are represented by node degree with power-law distribution. The small-world networks have special topological characteristics—short average path lengths and high clustering. However, with the growing importance and popularity of complex networks, a lot of other network topology characteristics have been proposed as well.

Recently, the study of complex networks has been expanded to network invulnerability. If those complex networks are robust enough, they become significantly more vulnerable to random failures and malicious attacks and exhibit cascading failures. The existing research on the invulnerability of WSNs has almost come to a standstill [16,17]. The impact of failure vertex on the other connected vertexes may not be taken into consideration. However, if a sensor node fails in WSNs, its load would be redistributed to its adjoining nodes. The continuously increasing load may go beyond the processing capacity of some nodes, leading the application to fail in these nodes as well, and a cascading problem in the whole network would eventually occur. This occurrence is called a cascading failure [18]. It seriously affects the performance of WSNs and can even cause the collapse of the entire network. Therefore, when designing the topology of WSNs, we should consider not only the network performance, but also controlling the cascading failure effectively.

Some empirical research shows that scale-free networks have strong survivability [19-22]. So the scale-free networks have become the mainstream topology of WSNs.

There have been numerous research findings about cascading breakdowns in complex networks over the past few years. Motter (2002) presented a cascading failure evolution model which revealed the causes of cascading effects [23]. Souza et al., (2014) further found that there were power-law features for the cascading breakdown of scale-free networks [24]. Some deductions about cascading breakdowns from the scale-free network topological structure are given by Deng et al., (2010) [25]. Meanwhile, Dobson et al., (2010) proposed an optimization algorithm on controlling cascading failure based on node importance [26]. Finally, Chen et al., (2013) proposed Souzaan optimal model suppressing cascading failure in weighted complex networks [27].

However, nearly all existing research depends on optimizing node performance to restrict cascading breakdowns instead of applying complex network topology. But the node performance of WSNs is fixed; therefore, we need to improve the invulnerability of WSNs through the topology characteristics of WSNs based on complex networks.

In this paper, we firstly analyze the topological characteristics of complex networks. Then we consider the influence of node distribution in the scale-free topology of WSNs on cascading failure before introducing a super node with higher performance, which will be connected with the sink node. On the basis of the above research, we put forward a cascading breakdown evolution model for WSNs with a scale-free topological structure.

The rest of this paper is organized as follows. Firstly, we explain how to build WSNs with a scale-free topological structure in Section 2. In Section 3, a cascading failure evolution model based on scale-free topological structure for WSNs is pro-

posed. In Section 4, simulation experiments and an analysis are given. Section 5 summarizes our findings.

2 WSN Models with Scale-free Topology

For large-scale WSNs, the critical problem is the resource limitation of the nodes. So the topology construction of WSNs should consider the types and distribution of nodes.

WSNs usually need to fix the relative position of sensors and a long-term link. The common WSNs' topology consists of N sensor nodes which are located symmetrically in a $U \times V$ rectangular scope; each sensor node is distributed at the intersection. The coordinate position is labeled as (u, v) , where $0 \leq u \leq U-1$, $0 \leq v \leq V-1$. The WSNs' topology presents the Mesh structure, which is shown in Figure 1.

For the purpose of constructing WSNs with scale-free nodes of one type, super nodes with higher performance are introduced. These nodes make direct long-distance communication between super nodes and sink nodes possible. Besides, super nodes can also communicate with the common nodes. So they are a suitable solution for introducing a "shortcut" in WSNs.

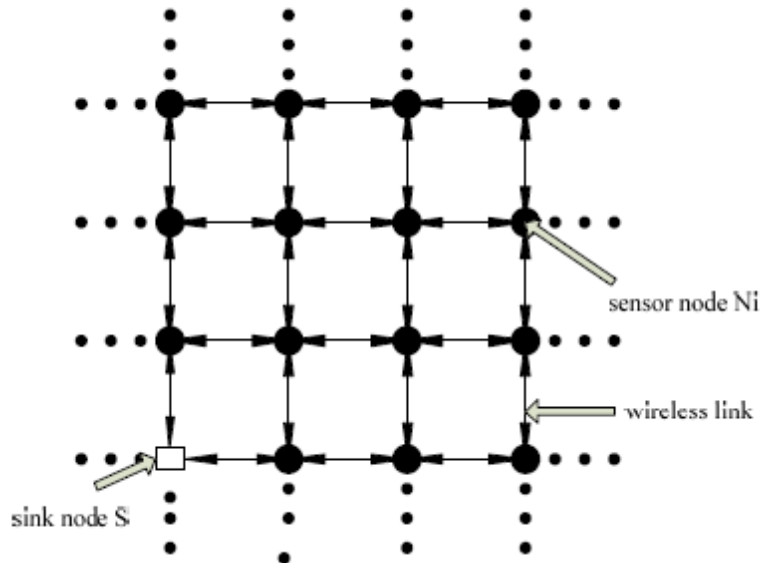


Fig. 1. The Mesh topology of WSNs

Assume that the coordinate position of the common node N_i is (u_i, v_i) , the position of another common node N_j is (u_j, v_j) , and their sink node is (u_s, v_s) . Firstly, we calculate the shortest distance between the common node N_i and N_j through the sink node without the super node.

$$D(N_i, S) = |u_i - u_s| + |v_i - v_s| \tag{1}$$

$$D(N_j, S) = |u_j - u_s| + |v_j - v_s| \tag{2}$$

As shown in Figure 2, if the common node N_i is far away from the sink node, we can add a super node N_i that can connect to the sink node through the super node.

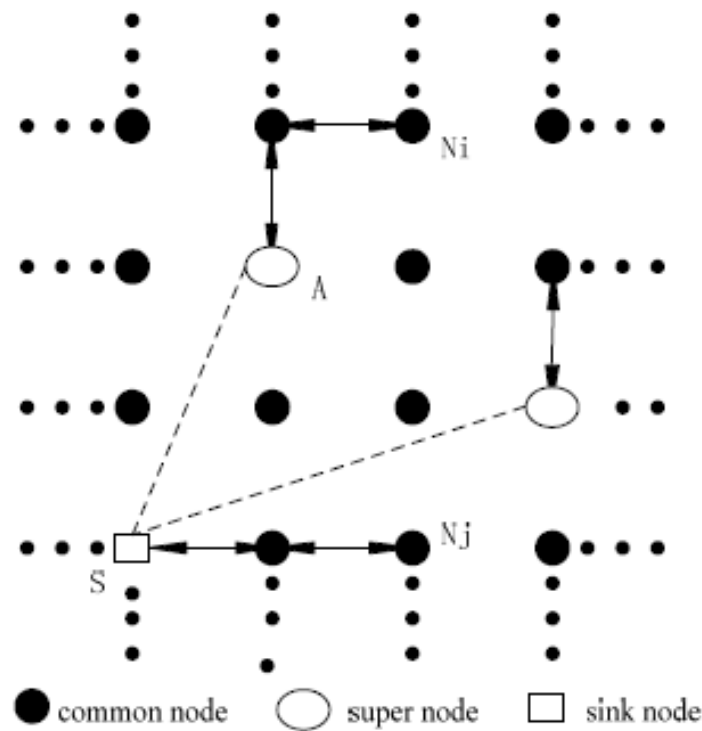


Fig. 2. The topology of WSNs after adding super nodes

The shortest distance for node N_i to the nearest super node is:

$$D'(N_i, S) = |u_i - u_A| + |v_i - v_A| \tag{3}$$

According to Eqs. (1), (2) and (3), we can know, when $D(N_i, S) \geq D'(N_i, S)$, the node will select a super node to add. On the contrary, when $D(N_i, S) < D'(N_i, S)$, the node N_j will not choose to add a super node.

Based on the topology of WSNs after adding a super node, the average path length of all nodes to super nodes or sink nodes in WSNs is shown as:

$$L_{average} = \frac{1}{n} \sum_{i=1}^n D_{i-sink} \quad (4)$$

where n represents the number of wireless sensors in WSNs, D_{i-sink} is the distance for node i from the super node to the sink node. So the shortest path for the common node i to the sink node in WSNs can be shown as:

$$D_{i-sink} = \min(D(N_i, S), D'(N_i, S)) \quad (5)$$

Assuming we add w super nodes to a WSN, the probability of the common nodes connecting to a super node is $\rho_{i,w}$, thus the average path length of the common node to the super node or sink node can be shown as:

$$L_{average}(w) = \frac{1}{n} \sum_{i=1}^n [\rho_{i,w} D'(N_i, S) + (1 - \rho_{i,w}) D(N_i, S)] \quad (6)$$

The initial value of the average path length is:

$$L_{average}(0) = \frac{1}{n} \sum_{i=1}^n D(N_i, S) \quad (7)$$

The ratio of the average path length of node to super node or sink node is defined as:

$$R_{average}(w) = \frac{L_{average}(w)}{L_{average}(0)} \quad (8)$$

3 Cascading Failure Model Based on Scale-free Topological Structure

In WSNs, the load of a node refers to the quantity of information on the node [28]. Based on the degree distribution of nodes in WSNs with scale-free topological structures, the load of node i can be defined as:

$$E_i = k_i^\beta \quad (9)$$

where E_i is the load of node i , k_i is the degree of node i , and β is a variable which can adjust the intensity of the node load.

Assume node i is a neighbour of node j in a WSN. If node j becomes invalid, the load of node j would be redistributed to its neighbours. Thus the load of node i would be altered. The load distribution equation is defined as:

$$\dot{E}_i = E_i + \Delta_{ij} = E_i + E_j/k_j \tag{10}$$

where \dot{E}_i represents the final load of node i , Δ_{ij} is a new increase load, and k_j is the degree of node j .

Because of limited resources, the node performance of WSNs with scale-free topological structures can be assumed a constant. The performance of each node can be defined as

$$p_i = p_0 \tag{11}$$

where p_i is the performance of node i , and p_0 is a constant value.

The cascading failure process of WSNs can be explained as follows: The failure of any vertex j would redistribute its own load to its neighbouring nodes. If the load of one neighbour vertex i after redistribution becomes greater than its performance p_0 , the vertex i would fail as well. The load of vertex i would be further spread to its neighbours, and so on in a vicious circle. The whole network would be down.

Based on complex network theory, the degree distribution of scale-free networks is $p(k) = ck^{-\lambda}$ ($c>0, \lambda>0$), and the degree distribution generation function could be shown as:

$$f_0(x) = \sum_{k=k_{min}}^{k_{max}} p(k)x^k \tag{12}$$

where k_{min} and k_{max} are the min and max node degrees in complex networks.

A node with degree k is chosen randomly, its failure probability is $q(k)$, and the generating function of the failure probability of a vertex whose degree is $k+1$ could be shown as:

$$f_1(x) = \sum_{k=k_{min}-1}^{k_{max}-1} q(k)x^k = \frac{\sum_{k=k_{min}}^{k_{max}} q(k)x^k}{x} \tag{13}$$

The failure probability $q(k)$ in Eq. (13) could be redefined as:

$$q(k) = \sum_{\tau=k_{min}}^{k_{max}} \theta_{\tau k} = \sum_{\tau=k_{min}}^{k_{max}} p_1(\tau)p_2(k)p_3(\tau k) \tag{14}$$

where $\theta_{\tau k}$ represents the probability that a common vertex with degree τ connected with a neighbour node with degree k , $p_1(\tau)$ is the probability of stochastically choosing a common node with degree τ , and $p_1(\tau) = p(\tau)$. $p_2(k)$ is the probability of randomly choosing an edge to a vertex with degree k . Then we can get

$$p_2(k) = \frac{k_p(k)}{\sum_{k=k_{\min}}^{k_{\max}} k_p(k)} \quad (15)$$

$p_3(k\tau)$ is the probability that a vertex with degree τ causes the failure of another vertex with degree k . As the total load of the vertex with degree τ is $E = \tau^\alpha$, the definition of $p_3(k\tau)$ is shown as

$$p_3(\tau k) = \frac{\tau^\alpha}{c_0 - k^\alpha}, \quad \alpha < \frac{\ln \frac{c_0}{1 + k_{\max}^{-1}}}{\ln k_{\max}} \quad (16)$$

where τ^α/τ is the new increase load of a vertex with degree k , and $c_0 - k^\alpha$ is the remaining performance of a vertex with degree k .

So $q(k)$ could be redefined as follows:

$$q(k) = \sum_{\tau=k_{\min}}^{k_{\max}} c\tau^{-\lambda} \frac{kck^{-\lambda}}{\sum_{k=k_{\min}}^{k_{\max}} kck^{-\lambda}} \frac{\tau^\alpha}{c_0 - k^\alpha} = \sum_{\tau=k_{\min}}^{k_{\max}} \frac{c(2-\lambda)\tau^{\alpha-\lambda-1}k^{1-\lambda}}{(k_{\max}^{2-\lambda} - k_{\min}^{2-\lambda})(c_0 - k^\alpha)} \quad (17)$$

According to Eq. (17), we could achieve the generation function for the remaining part of the network after cascading failure.

$$h_1(x) = xq(0) + xq(1)h_1(x) + xq(2)[h_1(x)]^2 + \dots = xf_1(h_1(x)) \quad (18)$$

According to Eq. (18), it can be seen that the generating function of the remaining network, except for the largest connected component, is shown as

$$h_0(x) = xf_0(h_1(x)) \quad (19)$$

Thus, according to Eqs. (13) and (17), we can get

$$f_1(h_1(x)) = \sum_{k=k_{\min}}^{k_{\max}} q(k)[h_1(x)]^{k-1} = \sum_{k=k_{\min}}^{k_{\max}} \sum_{\tau=k_{\min}}^{k_{\max}} \frac{c(2-\lambda)\tau^{\alpha-\lambda-1}k^{1-\lambda}}{(k_{\max}^{2-\lambda} - k_{\min}^{2-\lambda})(c_0 - k^\alpha)} [h_1(x)]^{k-1} \quad (20)$$

According to Eq. (18), we can get

$$h_1(1) = g_1(h_1(1)) = \sum_{k=k_{\min}}^{k_{\max}} \sum_{\tau=k_{\min}}^{k_{\max}} \frac{c(2-\lambda)\tau^{\alpha-\lambda-1}k^{1-\lambda}}{(k_{\max}^{2-\lambda} - k_{\min}^{2-\lambda})(c_0 - k^\alpha)} [h_1(1)]^{k-1} \quad (21)$$

According to Eq. (21), we can get $h_1(1) = w$, and according to Eq. (19), $h_0(1)$ can be defined as

$$h_0(1) = f_0(w) \tag{22}$$

Then based on Eq. (12), we can get

$$h_0(1) = \sum_{k=k_{\min}}^{k_{\max}} p(k)[w]^k \tag{23}$$

where w represents the min number of the following equation

$$w = \sum_{k=k_{\min}}^{k_{\max}} \sum_{\tau=k_{\min}}^{k_{\max}} \frac{c(2-\lambda)\tau^{\alpha-\lambda-1}k^{1-\lambda}}{(k_{\max}^{2-\lambda}-k_{\min}^{2-\lambda})(c_0-k^\alpha)} [w]^{k-1} \tag{24}$$

4 Simulation Experiments and Analysis

In the simulation, a 20×20 Mesh topology network is generated. The sink nodes are located in (0, 0) and (10m 10); Other common nodes are located in the crossing points of the Mesh topology. The network topology is shown in Figure 3.

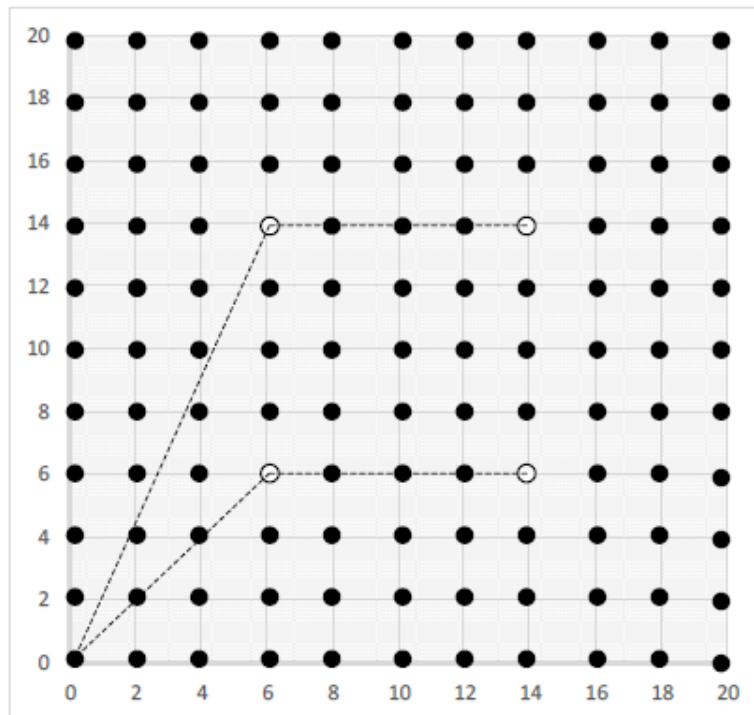


Fig. 3. The topology of simulation networks

In Figure 4, the relation between the number of super nodes added in the simulation network and the average path length (APL) is given. From Figure 4, we can see that the APL of these nodes connected to the sink nodes decreases fast after adding some super nodes to the network.

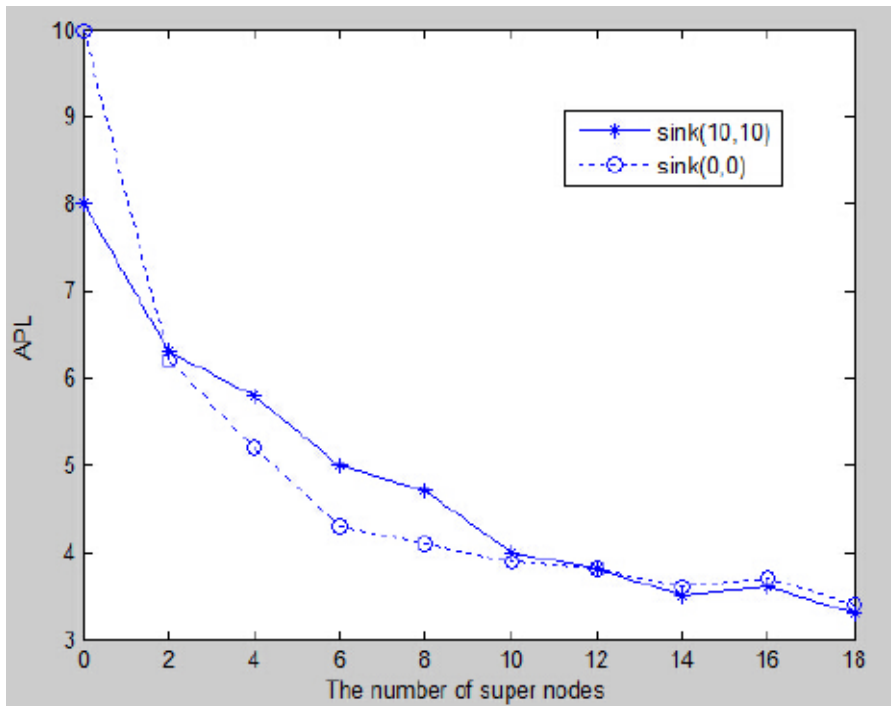


Fig. 4. APL with change [better: "addition"?] of super nodes

In order to test the validity of our cascading failure model, the topology structure before and after the network breakdown are compared. The topology change is shown in Figure 5.

Then we compare the lifetime of WSNs before prevention, after prevention and no cascading breakdown in Figure 6.

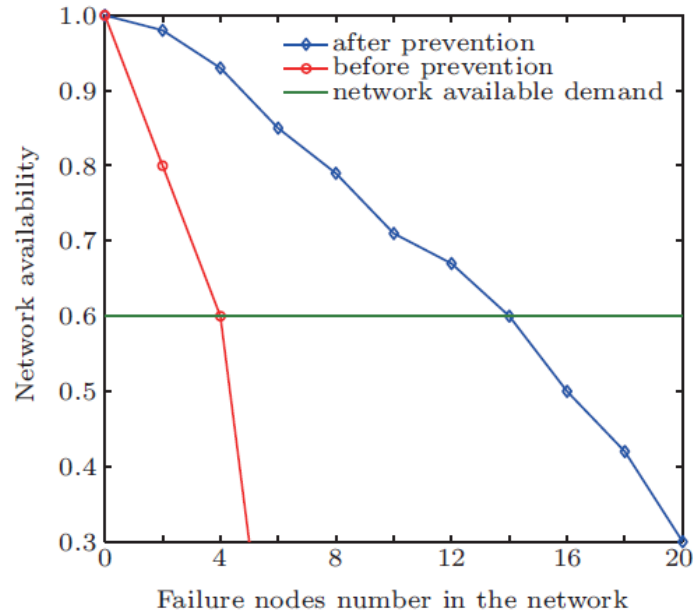


Fig. 5. The validity of our cascading failure model

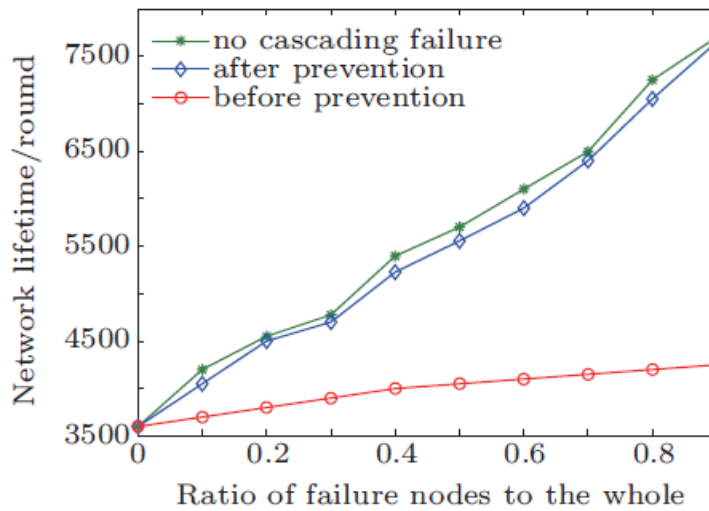


Fig. 6. Observation of the remaining network lifetime

From Figure 6, we can conclude that the lifetime of the network after prevention is far smaller than that without a cascading breakdown. This is because our cascading breakdown model greatly weakens the impact of a cascading breakdown on WSNs' capabilities.

Random failure is one of the most common problems in the real world. The random failure of the three situations is shown in Figure 7.

From Figure 7, we can know that the network topology with no cascading breakdown and after prevention is nearly the same when the equal amount of random failure nodes is deleted.

The change in the maximal connected graph with selected failure vertex for all situations is shown in Figure 8.

From Figure 8, we can see that when the same amount of nodes is deleted, the largest connected graph of the network with no cascading breakdown and after prevention is a bit larger than that before prevention.

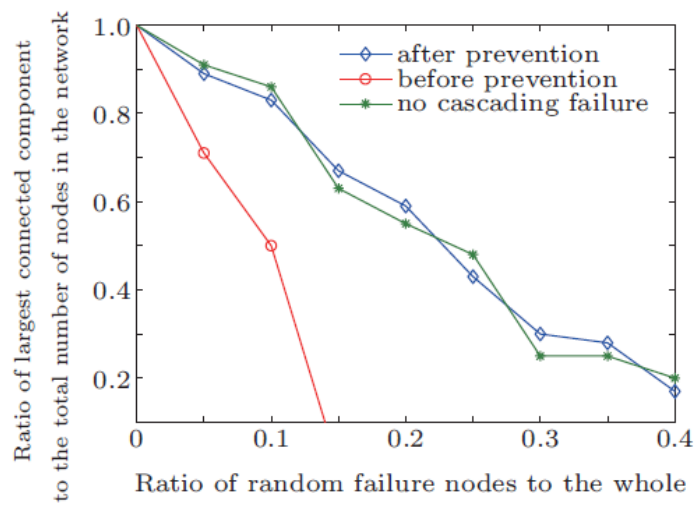


Fig. 7. Observation of the topology under random failure

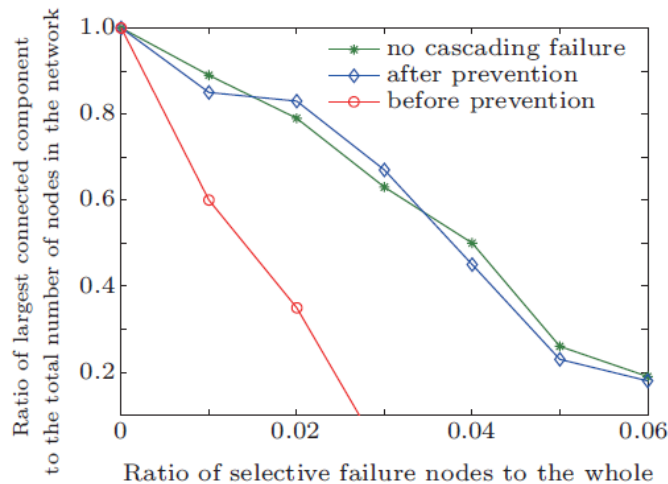


Fig. 8. Observation of the topology under random failure

5 Conclusions

In this paper, we start out by introducing the application of complex network theory in WSNs. Based on the topology characteristics of scale-free networks, we put forward high-performing super nodes which can communicate with the sink nodes to connect to the common nodes. A cascading breakdown evolution model based on the scale-free topological structure is proposed. Simulation experiments have shown the validity of our model.

6 References

- [1] Zhang, C. (2010). Cluster-based Routing Algorithms Using Spatial Data Correlation for Wireless Sensor Networks. *Journal of Communications*, 5(3), 232-238. <https://doi.org/10.4304/jcm.5.3.232-238>
- [2] Wang, J., Kim, J. U., Shu, L. (2010). A Distance-based Energy Aware Routing algorithm for wireless sensor networks. *Sensors*, 10(10), 9493-9499. <https://doi.org/10.3390/s101009493>
- [3] Fichera A., Frasca M., Volpe R. (2016). On energy distribution in cities: a model based on complex networks, *International Journal of Heat and Technology*, 34(4), 611-615. <https://doi.org/10.18280/ijht.340409>
- [4] Liu, B. (2014). Fault-tolerant topology in the wireless sensor networks for energy depletion and random failure. *Chinese Physics B*, 23(7), 343-349. <https://doi.org/10.1088/1674-1056/23/7/070510>
- [5] Cai, S., Zhou, P., Liu, Z. (2014). Synchronization analysis of directed complex networks with time-delayed dynamical nodes and impulsive effects. *Nonlinear Dynamics*, 76(3), 1677-1691. <https://doi.org/10.1007/s11071-014-1238-z>
- [6] Sun, G., Sheng, B., Zhou, Y. (2015). Big Data Analytics of Multi-Relationship Online Social Network Based on Multi-Subnet Compositated Complex Network. *International Journal of Database Theory & Application*, 8(5), 273-284. <https://doi.org/10.14257/ijdta.2015.8.5.24>
- [7] Zhang, W., Sun, G., Sheng, B. (2015). An Opinion Leaders Detecting Algorithm in Multi-relationship Online Social Networks. *International Journal of Hybrid Information Technology*, 9(5), 391-398. <https://doi.org/10.14257/ijhit.2016.9.5.33>
- [8] Chua, H. N., Ning, K., Sung, W. K. (2011). Using indirect protein-protein interactions for protein complex prediction. *Computational Systems Bioinformatics*, 6(3), 97-109.
- [9] Sánchezburillo, E., Duch, J., Zueco, D. (2012). Quantum Navigation and Ranking in Complex Networks. *Scientific Reports*, 2, 605-616.
- [10] Paparo, G. D., Müller, M., Comellas, F. (2013). Quantum Google in a Complex Network. *Scientific Reports*, 3, 127-132. <https://doi.org/10.1038/srep02773>
- [11] Tsiotas, D., Polyzos, S. (2015). Decomposing multilayer transportation networks using complex network analysis: a case study for the Greek aviation network. *Journal of Complex Networks*, 3(4), 642-670. <https://doi.org/10.1093/comnet/cnv003>
- [12] Shi, H. S. (2016). A Method of Automatic Detection of Fog Image Based on SVM Classification. *Revista de la Facultad de Ingeniería*, 31(9), 211-218.
- [13] Barabasi, A., Bonabeau, E. (2003). Scale-Free Networks. *Scientific American*, 5, 60-69. <https://doi.org/10.1038/scientificamerican0503-60>

- [14] Strogatz, S. H., Watts, D. R. (1998). Collective dynamics of 'small-world' networks. *Nature*, 393, 440-442. <https://doi.org/10.1038/30918>
- [15] Stanley, H. E., Amaral, L. N. (2000). Classes of small-world networks. *PNAS*, 21, 11149-11152.
- [16] Li, J., Wu, J. (2011). Optimal Attack Strategy in Random Scale-Free Networks Based on Incomplete Information. *Chinese Physics Letters*, 28(6), 068902. <https://doi.org/10.1088/0256-307X/28/6/068902>
- [17] Tan, S. Y., Wu, J. (2016). Efficient network disintegration under incomplete information: the comic effect of link prediction. *Scientific Reports*, 6, 22916. <https://doi.org/10.1038/srep22916>
- [18] Hu, K., Hu, T. (2010). Model for cascading failures with adaptive defense in complex networks. *Chinese Physics B*, 19(8), 65-71.
- [19] Albert, R., Jeong, H., Barabasi, A. (2010). Error and attack tolerance of complex networks. *Elsevier B.V.*, 10, 200-210.
- [20] Jalili, M. (2011). Error and attack tolerance of small-worldness in complex networks. *Journal of Informetrics*, 5(3), 422-430. <https://doi.org/10.1016/j.joi.2011.03.002>
- [21] Chekroun, S., Abdelhadi, B., Benoudjit, A. (2014). A New Approach Design Optimizer of Induction Motor Using Particle Swarm Algorithm, *Modelling, Measurement and Control A*, 87(2), 89-108.
- [22] Sehaba, K., Serna, A. (2014). Decoding Social Situations in Adolescents with Asperger through a Serious Game, *Modelling, Measurement and Control C*, 75(2), 234-247.
- [23] Motter, A. E., Lai, Y. C. (2002). Cascade-based attacks on complex networks, *Physical Review E Statistical Nonlinear & Soft Matter Physics*, 2, 065102. <https://doi.org/10.1103/physreve.66.065102>
- [24] Souza, R. M., Brummitt, C. D. (2014). Modeling Interdependent Networks as Random Graphs: Connectivity and Systemic Risk, *Understanding Complex Systems*, 7, 73-94.
- [25] Deng W., Zhu P. (2010). On Evaluating BGP Routing Stress Attack, *Journal of Communications*, 5(1), 39-47. <https://doi.org/10.4304/jcm.5.1.13-22>
- [26] Dobson, I., Kim, J. (2010). Testing branching process estimators of cascading failure with data from a simulation of transmission line outages, *Risk Analysis*, 30(4), 650-662. <https://doi.org/10.1111/j.1539-6924.2010.01369.x>
- [27] Chen, S. M., Pang, S. P. (2013). An LCOR model for suppressing cascading failure in weighted complex networks, *Chinese Physics B*, 22(5), 058901. <https://doi.org/10.1088/1674-1056/22/5/058901>
- [28] Cai, J. M., Yu, S. Z. (2013). An efficient management strategy for enhancing traffic capacity in scale-free networks, *Acta Phys. Sin.*, 62(5), 633-641.

7 Author

Zhigang Zhao is currently a lecturer at the School of New Media, Zhejiang University of Media and Communications, Hangzhou Zhejiang, China. He received his M.S. degree in software engineering from Zhejiang University in 2006. His research interests include computer applications, artificial intelligence, wireless sensor network, data mining and computer simulation. He is a member of CCF (zhaozhig2006@126.com).

Article submitted 06 February 2017. Published as resubmitted by the authors 20 March 2017.