Ad Hoc Networks 93 (2019) 101900

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Cascading failures in wireless sensor networks with load redistribution of links and nodes

Xiuwen Fu*, Haiqing Yao, Yongsheng Yang

Institute of Logistics Science and Engineering, Shanghai Maritime University, Shanghai 201306, China

ARTICLE INFO

Article history:
Received 7 January 2019
Revised 24 April 2019
Accepted 24 May 2019
Available online 4 June 2019

Keywords:
Cascading failures
Wireless sensor networks
Load-redistribution scheme
Traffic metric

ABSTRACT

Existing cascading models for wireless sensor networks (WSNs) cannot correctly reflect the traffic feature of WSNs. In this work, we build a more practical cascading model for WSNs, in which the network load is defined according to two new traffic metrics "sink-oriented node betweenness" and "sink-oriented link betweenness" and the cascading process is jointly propelled by the load redistribution of sensor nodes and wireless links. In addition, load-redistribution schemes are designed according to the principle of "idle capacity". Simulation results show that the network invulnerability is positively related to the tolerance coefficient and negatively related to the exponential coefficient. The minimum costs needed to resist intentional node attacks are more expensive than the costs needed when facing intentional link attacks.

1. Introduction

In recent years, owing to the significance of network safety in our daily life, network invulnerability has attracted a large amount of interests from many researchers [1–3]. As an important part of the Internet of Things (IoTs), Wireless Sensor Networks (WSNs) have also received widespread attention about the network invulnerability because of their unattended deployment environment and vulnerability to node/link failures [4,5]. Since the earlier studies mainly focus on the static invulnerability from a topological perspective, recently cascading failures induced by the dynamic load redistribution in WSNs have been significantly concerned and widely investigated [6–10].

In existing works related to the cascading invulnerability of WSNs, they usually assumed that each sensor node takes a certain degree of traffic load due to data delivery tasks [11–15]. The traffic load is usually represented by degree or betweenness values. Due to the limited hardware costs, each sensor node can only have limited capacity to tackle its own load. If the real-time load is beyond its capacity, the sensor node is highly likely to fail due to buffer overflows or channel congestions. When a sensor node fails, those nodes who transmit data through it will choose a new path to accomplish the data delivery, further leading to the redistribution of the network load. We can easily discover that in existing cascading models the load-redistribution process can only spread from node to node and can only be triggered by node failures. It is natural for us to classify these models to the "cascading node failures" mode [16–21]. However, in a practical WSN, this mode can hardly reflect the practical traffic features of WSNs and cannot properly characterize the realistic cascading process. There are three major limitations in this mode:

1) It only considers the capacity of sensor nodes and fails to consider the capacity of wireless links. In WSNs, since the links are built via wireless transmission, their functions are constrained by bandwidth resources and channel resources. When the real-time load is beyond a link's capacity, the link-overload event will occur;

2) It assumed that the cascading process is only driven by node failures and fails to consider the load-redistribution process caused by link failures. In WSNs, when a link fails, the load it originally takes will be redistributed to other routes and the network load will be renewed accordingly. After this load-redistribution process, there might be some new nodes or links being overloaded, then the cascading failures will continue.

3) It only considers the traffic load in sensor nodes and does not have a traffic metric to depict the traffic load taken by links. Moreover, existing traffic metrics are oversimplified as they ignore the impacts of the sink node on the distribution of the network load.

In the research of cascading failures for other network systems (e.g., power grid network), the concepts of "link load" and "link failure" have been well studied [22–25], but these research results cannot be applied to WSNs. This is because these studies only consider the impacts of link load on the network cascading process, but ignoring the impacts of node load. In addition, their models cannot reflect the sink-convergence feature of WSNs. From

* Corresponding author.
E-mail address: xwfu@shmtu.edu.cn (X. Fu).

https://doi.org/10.1016/j.adhoc.2019.101900
1570-8705/

the above discussion, we can easily find that cascading failures in WSNs are a result of the overload behaviors of nodes and links affecting jointly. To research the cascading invulnerability, the cascading model for WSNs should switch from the "cascading node failures" mode to the "cascading node-link failures" mode.

Therefore, the aim of this paper is to construct a realistic cascading model for WSNs considering the overload of nodes and links, and investigate the network invulnerability under different attack schemes. In this model, considering the sink-convergence feature of WSNs, new traffic metrics are presented to depict the traffic load on sensor nodes and wireless links. The load-redistribution schemes are designed according to the principle of "idle capacity", which is closer to the practical routing protocols. We numerically find some interesting and important results, such as, during the cascading process the majority of failed nodes are caused by isolation and more costs are needed to resist intentional node attacks than resisting intentional link attacks. Our findings can be useful in further studies on how to build an invulnerable WSN.

The rest of this paper is organized as follows: in Section 2, we describe the traffic metrics on nodes and links in detail. In Section 3, we present the cascading models. In Section 4, we analyze the network invulnerability against cascading failures. Finally, conclusions and the future work are given.

2. Traffic metrics

2.1. Problem statements

In this section, before giving the new traffic metrics, we firstly discuss the rationality of using degree or betweenness value as the traffic metric to measure the network load. We present a network topology referencing [15] (shown in Fig. 1). The network topology consists of 300 sensor nodes.

Fig. 2 shows the normalized network traffic distribution generated by LEACH [26], we can easily observe that sensor nodes closer to the sink node tend to take a heavier traffic load. In fact, this phenomenon has been discovered by many researchers and they call it the "sink hole issue" [27–31]. In WSNs, sensor nodes have two tasks: transmitting the data packets created by their own sensing tasks and help relay the data packets from other sensor nodes. Because all the data packets will be collected at the sink node eventually, the nodes closer to the sink node will take heavier relay tasks than "edge" nodes, thus leading to a higher traffic load.

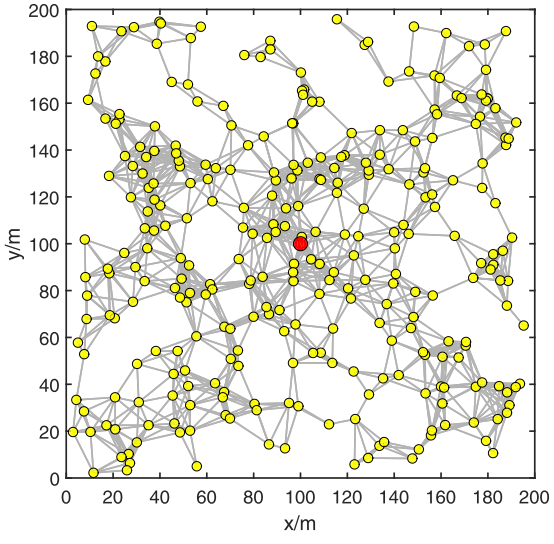


Fig. 1. network topology (consisting of 300 sensor nodes and the sink node is marked red).

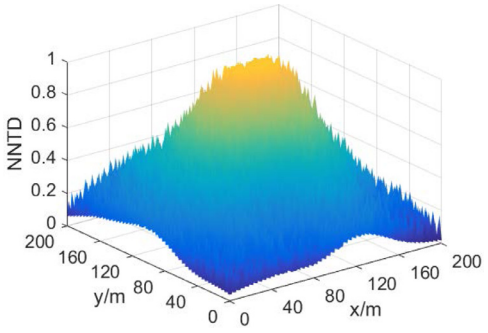


Fig. 2. Normalized network traffic distribution (NNTD) generated by LEACH.

Fig. 3 shows the normalized network traffic distribution created by degree and betweenness respectively. In Fig. 3(a), the more connections the sensor node has, the heavier its load tends to be. We can easily discover that the traffic distribution created by nodes' degree to some extent, can only reflect the traffic exchange in neighboring areas. In Fig. 3(b), the node who holds a larger number of shortest paths between each pair of sensor nodes in the network, will take heavier load. In the betweennss-based load model, data packets are simply assumed to be delivered from one sensor node to another sensor node, rather than from the origin sensor node to the sink node. Compared with the traffic distribution shown in Fig. 2, neither degree nor betweenness can create a similar traffic distribution, because they fail to take into account the sink-convergence feature of WSNs.

According to the above discussion, when used in WSNs, there are some obvious problems in the existing degree-based or betweenness-based traffic metrics.

1) They cannot properly reflect the sink-convergence feature of WSNs, which makes the obtained distribution of the network load far from the reality

2) They can only be used to measure the traffic load on nodes, but fail to indicate the load on links, which makes the load-redistribution process far from the practical cascading process in WSNs.

2.2. Sink-oriented betweenness

To properly reflect the traffic feature of WSNs, we propose two traffic metrics: sink-oriented node betweenness (SNB) and sink-oriented link betweenness (SLB), which are to measure the load on sensor nodes and wireless links respectively.

SNB is defined as follow:

$$D_i(t) = \frac{\sum_{j \in V} g_{ij}(t)/g_j(t)}{N}, \tag{1}$$

where $g_{ij}(t)$ is the number of the shortest paths from node j to the sink node which pass through node i at time t. $g_j(t)$ is the number of the shortest paths from node j to the sink node at time t. V is the node collection except the sink node. N is the number of sensor nodes except the sink node. The most extreme situation for SNB is that each of the shortest path from any sensor nodes to the sink node will pass through node i. At this point, $D_i(t)$ will be the maximum value 1. When node i is at the border of the network and no nodes require it to relay data packets, the load it takes is only its self-generated data packets. At this point, $D_i(t)$ will be the minimum value $1/N$.

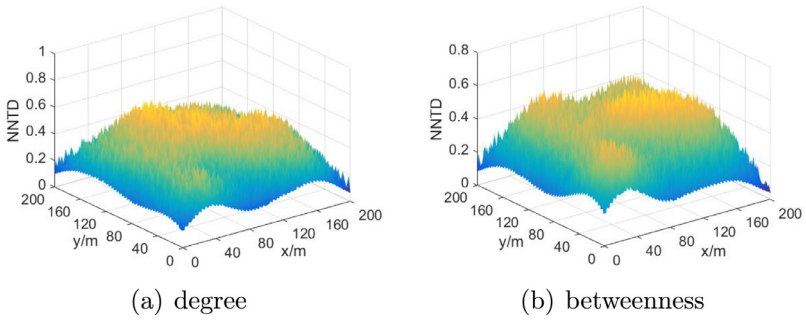


Fig. 3. Normalized network traffic distribution (NNTD) generated by various traffic metrics.

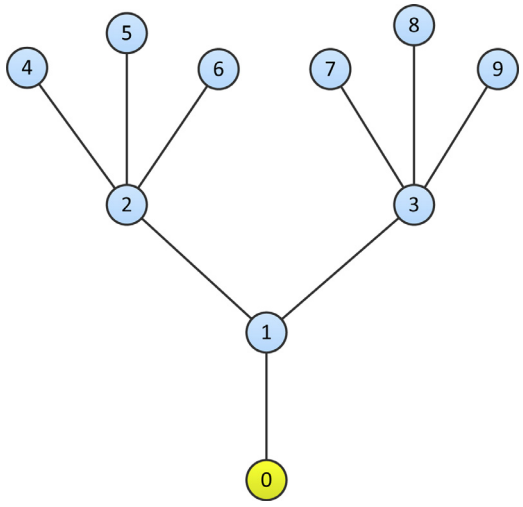


Fig. 4. Clustering structure of WSNs (node 0 is the sink node and other nodes are common sensor nodes).

SLB is defined as follow:

$$D_{e_{jk}}(t) = \sum_{i \in V} \frac{g_{i,e_{jk}}(t)/g_i(t)}{N}, \tag{2}$$

where $g_{i,e_{jk}}(t)$ is the number of the shortest paths from node i to the sink node which pass through the edge e_{jk} at time t. The most extreme situation for SLB is that each of the shortest path from any sensor nodes to the sink node will pass through edge e_{jk}. At this point, $D_{e_{jk}}(t)$ will be the maximum value 1. When edge e_{jk} is at the border of the network and only its endpoints (i.e., the sensor nodes at the both ends of the edge) require it to relay data packets, e_{jk} will be the minimum value $1/N$.

Without loss of generality, we choose the most commonly-used network structure in WSNs (i.e.,cluster topology) to evaluate the reasonability of SNB and SLB (shown in Fig. 4). In this network topology, each node must go through node 1 to reach the sink node. Thus, we can reasonably consider that the entire network traffic will pass through node 1. In addition to the self-generated data packets, node 2 and node 3 are also required to relay the data packets from 3 nodes respectively. Thus, we can reasonably consider that almost half of the network traffic will pass through node 2 and node 3. For remaining sensor nodes, they do no take relay tasks and the only load they take is the self-generated load. From Table 1, we can clearly find that SNB perfectly depicts the above traffic distribution feature. By contrast, neither degree nor betweenness is able to reflect this feature. In a similar way, we can find that the entire network traffic will pass through edge e_{01}. Almost half of the network traffic will pass through edge e_{12} and edge e_{13}. For remaining edges, the only load they take is from their endpoints. According to Table 2, SLB can indicate the traffic load on each links reasonably.

Table 1
Comparison of multiple traffic metrics.

Node	Degree	Betweenness	SNB
1	0.176	0.615	1
2-3	0.235	0.641	0.444
4–9	0.058	0	0.111

Table 2
SLB in clustering WSN.

Edge	SLB
e_{01}	1
e_{12}, e_{13}	0.444
e_{24}, e_{25}, e_{26}, e_{37}, e_{38}, e_{39}	0.111

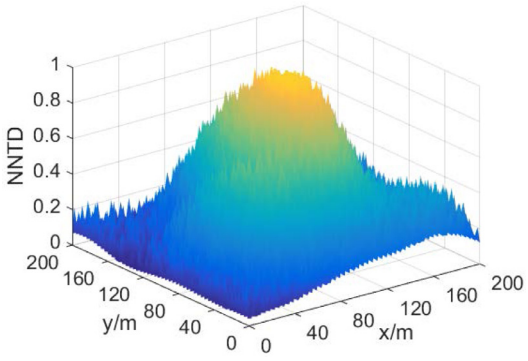


Fig. 5. Normalized network traffic distribution (NNTD) jointly created by SNB and SLB.

Fig. 5 shows the network traffic distribution jointly created by SNB and SLB. In this figure, we can find that the sink-convergence feature in WSNs is clearly presented. The traffic distribution in Fig. 5 is quite similar with that in Fig. 2. The reasonability of SNB and SLB is further validated.

3. Cascading model

3.1. Load and capacity

As discussed in last section, in practical WSNs the initial load of sensor nodes and wireless links is closely related to the number of shortest paths from all the other sensor nodes to the sink node that pass it in the network, so it is reasonable to define the initial load as a function of the sink-oriented betweenness. For this consideration, we define the initial load of node i and the initial load

of link e_{jk} as follows

$$L_i(0) = D_i(0)^{\alpha}, \tag{3}$$

$$L_{e_{jk}}(0) = D_{e_{jk}}(0)^{\alpha}, \tag{4}$$

where $\alpha \geq 0$ is the exponential coefficient that determines the distribution of the initial load. $D_i(0)$ and $D_{e_{jk}}(0)$ are the SNB and SLB in the initial network at time $t = 0$ respectively. We can easily observe that the initial load of each sensor node and link bears a linear relationship with its sink-oriented betweenness value when $\alpha = 1$. The configuration of α is closely related to the data type of WSNs. If the data type is the multimedia data, it means that the initial load will have a rapid growth in an exponential way with the increase of the sink-oriented betweenness value, thus α should be set a relatively large value. Otherwise, if the data type is the general text data, α can be a small value. It is obvious that the introduction of α can provide a high flexibility for our model to apply to different types of WSNs.

In most literature, the nodes' capacity is set to be positively correlated with their initial load, as shown in (5).

$$W_i = (1 + \beta)L_i(0), \tag{5}$$

where β is the tolerance coefficient. However, in WSNs, this setting is far from the practical situations. Unlike power grids in which the nodes' capacity can be customized according to the practical demands, the nodes' capacity in WSNs are always the same. Therefore, in this work, the sensor nodes' capacity is defined as

$$W_N = (1 + \lambda_n)L_n(0) = (1 + \lambda_n)\frac{\sum_{i \in V} L_i(0)}{N}. \tag{6}$$

where λ_n is the node tolerance coefficient to adjust the node capacity. According to (6), each sensor node has the same capacity, which is positively correlated with the average load of the initial network. It is easy to understand that the network designer tends to give more capacity to sensor nodes when the initial network faces greater load. In a similar way, the links' capacity is defined as

$$W_L = (1 + \lambda_l)L_l(0) = (1 + \lambda_l)\frac{\sum_{e_{ij} \in E} L_{e_{ij}}(0)}{M}. \tag{7}$$

where λ_l is the link tolerance coefficient to adjust the link capacity and E is the link collection consisting by the wireless links in the network. M is the number of links in the initial network.

3.2. Load-redistribution schemes

In the traditional "cascading node failures" mode, cascading failures can only spread via the node-to-node interaction. When a node fails, its load will be distributed to its neighboring nodes. However, in practical WSNs, on the one hand the links are characterized by limited capability, on the other hand, the link failures can also cause the redistribution of the network load. Therefore, in our model, the load-redistribution schemes should cover two cases: 1) load redistribution after a node failure; 2) load redistribution after a link failure. It is worth noting that in existing load-redistribution schemes, the load from the failed node will be assigned to the neighboring nodes evenly. In nowadays, with the advancement of routing technologies in WSNs, in most of routing protocols, sensor nodes can have the real-time state information about their neighbors and they usually assign the load according to the idle capacity the neighbors have. Therefore, in order to approach as close as possible the practical routing process in WSNs, in our model the load-redistribution schemes are designed according to the principle of "idle capacity".

3.2.1. Load redistribution after a node failure

This case is to describe the load-redistribution process after a node failure. If node i fails at time t, its neighboring node j can receive extra load $\Delta_{ji}(t)$ as follows

$$\Delta_{ji}(t) = \frac{W_N - L_j(t)}{\sum_{k \in \Omega_i(t)} [W_N - L_k(t)]} L_i(t), \tag{8}$$

where $\Omega_i(t)$ is the node collection consisting by the neighbors of node i at time t. According to (8), we can easily obtain that under the idle-redistribution scheme, the node with more idle capacity can be assigned more load from the failed node.

After the load-redistribution process, the load of neighboring nodes will increase at the next time step. It is easy to understand that an increase in the load of the endpoint node will result in an increase in the load of the link it connects. Thus, when a node j receives extra load $\Delta_{ji}(t)$ from the neighboring failed node i, the load of its link e_{jk} will also increase by $\Delta_{e_{jk},j}(t)$.

$$\Delta_{e_{jk},j}(t) = \frac{\Delta_{ji}(t)}{L_j(t)} L_{e_{jk}}(t), \tag{9}$$

where $\Delta_{ji}(t)/L_j(t)$ indicates the ratio of the newly received load of node j to its original load and $L_{e_{jk}}(t)$ is the load of link e_{jk} at time t. According to (9), the ratio of the newly received load of link e_{jk} to its original load is the same as the ratio of the newly received load of endpoint node j to its original load.

To illustrate the load-redistribution process after a node failure more clearly, we present an example on a simplified network topology (show in Fig. 6). Assuming that node j fails at time t, the original load it takes will transfer to its neighboring nodes a, b and c according to the load-redistribution scheme. The increase of load in nodes a, b and c will lead to the increase of load on their links e_{ad}, e_{aj}, e_{bj}, e_{cj} and e_{bc}. At time $t + 1$, the real-time load of nodes a, b, c and the links e_{ad}, e_{aj}, e_{bj}, e_{cj}, e_{bc} will update according to (10) and (11) respectively.

$$\begin{cases} L_a(t+1) = L_a(t) + \Delta_{aj}(t) \\ L_b(t+1) = L_b(t) + \Delta_{bj}(t) \\ L_c(t+1) = L_c(t) + \Delta_{cj}(t) \end{cases} \tag{10}$$

$$\begin{cases} L_{e_{ad}}(t+1) = L_{e_{ad}}(t) + \Delta_{e_{ad},a}(t) \\ L_{e_{aj}}(t+1) = L_{e_{aj}}(t) + \Delta_{e_{aj},a}(t) \\ L_{e_{bj}}(t+1) = L_{e_{bj}}(t) + \Delta_{e_{bj},b}(t) \\ L_{e_{cj}}(t+1) = L_{e_{cj}}(t) + \Delta_{e_{cj},c}(t) \\ L_{e_{bc}}(t+1) = L_{e_{bc}}(t) + \Delta_{e_{bc},b}(t) + \Delta_{e_{cb},c}(t) \end{cases} \tag{11}$$

It is worth noting that the extra load received by e_{bc} is affected by nodes b and c at the same time, thus its load at time $t + 1$ will increase by $\Delta_{e_{bc},b}(t) + \Delta_{e_{cb},c}(t)$.

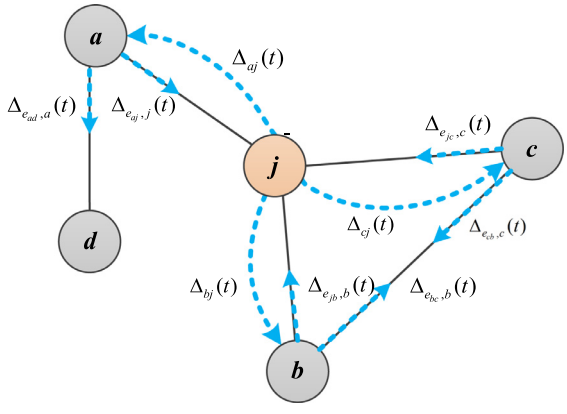


Fig. 6. An example of load redistribution after a node failure.

3.2.2. Load redistribution after a link failure

This case is to describe the load-redistribution process after a link failure. If link e_{ij} fails at time t, its neighboring link e_{jk} can receive extra load $\Delta_{e_{jk},e_{ij}}(t)$ as follows

$$\Delta_{e_{jk},e_{ij}}(t)=\frac{W_L-L_{e_{jk}}(t)}{\sum\limits_{a\in\Omega_i(t)}[W_L-L_{e_{ia}}(t)]+\sum\limits_{b\in\Omega_j(t)}[W_L-L_{e_{jb}}(t)]}L_{e_{ij}}(t). \tag{12}$$

According to (12), the link with more idle capacity can be assigned more load from the failed link.

When a link e_{jk} receives extra load $\Delta_{e_{jk},e_{ij}}(t)$ from its neighboring link e_{ij}, the load of its endpoint node k will also increase by $\Delta_{k,e_{jk}(t)}$.

$$\Delta_{k,e_{jk}}(t)=\frac{\Delta_{e_{jk},e_{ij}}(t)}{\sum\limits_{a\in\Omega_k(t)}L_{e_{ka}}(t)}L_k(t) \tag{13}$$

where $\sum\limits_{a\in\Omega_k(t)}L_{e_{ka}}(t)$ is the sum of the load taken by all links of node k (i.e., the sum of the link load taken by node k) and $\frac{\Delta_{e_{jk},e_{ij}}(t)}{\sum\limits_{a\in\Omega_k(t)}L_{e_{ka}}(t)}$ indicates the ratio of the newly received link load of node k to the sum of its original link load. According to (13), the ratio of the newly received load of node k to its original load is the same as the ratio of its newly received link load to the sum of its original link load.

To illustrate the load-redistribution process after a link failure more clearly, we present an example on a simplified network topology (show in Fig. 7). Assuming that link e_{ij} fails at time t, the original load it takes will transfer to its neighboring links e_{ai}, e_{bi}, e_{cj} and e_{dj} according to the load-redistribution scheme. The increase of load on these links will lead to the increase of load in their endpoint nodes a, b, c and d. At time $t+1$, the real-time load of the links e_{ai}, e_{bi}, e_{cj}, e_{dj} and the nodes a, b, c, d will update according to (14) and (15) respectively.

$$\begin{cases}L_a(t+1)=L_a(t)+\Delta_{a,e_{ai}}(t)\\ L_b(t+1)=L_b(t)+\Delta_{b,e_{bi}}(t)\\ L_c(t+1)=L_c(t)+\Delta_{c,e_{cj}}(t)\\ L_d(t+1)=L_d(t)+\Delta_{d,e_{dj}}(t)\end{cases} \tag{14}$$

$$\begin{cases}L_{e_{ai}}(t+1)=L_{e_{ai}}(t)+\Delta_{e_{ai},e_{ij}}(t)\\ L_{e_{bi}}(t+1)=L_{e_{bi}}(t)+\Delta_{e_{bi},e_{ij}}(t)\\ L_{e_{cj}}(t+1)=L_{e_{cj}}(t)+\Delta_{e_{cj},e_{ij}}(t)\\ L_{e_{dj}}(t+1)=L_{e_{dj}}(t)+\Delta_{e_{dj},e_{ij}}(t)\end{cases} \tag{15}$$

If $L_i(t+1)>W_N$, $i\in\{a,\ b,\ c,\ d\}$ or $L_{e_{mn}}(t+1)>W_L$, $e_{mn}\in\{e_{ai},\ e_{bi},\ e_{cj},\ e_{dj}\}$, another round of node failures or link failures will be triggered. This cascading process will not stop until the load of remaining nodes or links is within their capacity.

3.3. Cascading mechanism

In most of the existing cascading models, sensor nodes have two states: normal and overloaded. According to their assumptions, if the node's load is beyond its capacity, then it will be removed from the network permanently. This assumption is reasonable in the network like power grids. However, in WSNs, this assumption is far from the fact. Different with the electricity overload in power grids, the overload of data packets in WSNs will not cause physical damages of sensor nodes. Sensor nodes will reboot rather than fail permanently when overloaded. When the reboot is completed, it will join the network again and function normally. Thus, in our model, the node at overloaded state will be given a recovery time Δt. Within Δt, this node cannot receive, process and transmit data packets. When Δt is expired, the node will become "normal" again. In fact, Δt can be considered as the time that the overloaded node's reboot needs. In addition to "normal" and "overloaded", sensor nodes can also be "isolated". For a sensor node, if the routing paths to the sink node are cut off due to the overload of neighboring nodes or links, even if its load is still within the capacity range, it will be "isolated", because its message-forwarding service is no longer working. Isolated nodes can be repaired when some of its neighboring nodes or links recover from overload and an effective path to the sink node appears. Fig. 8 depicts the state transitions of sensor nodes in cascading process.

4. Analysis on the invulnerability of WSNs

4.1. Simulation settings

We use Matlab to implement our simulations and introduce GUROBI optimizer to accelerate the simulation process. In the simulations, the network size is set to 300 and sensor nodes are randomly deployed in the simulation area. The wireless transmission radius of sensor nodes is set to 20 m. The sink node is placed at the center of the simulation area. To better investigate the invulnerability of WSNs against cascading failures, we focus on two simple targeted attacks in our cascading model. The first one is to attack the nodes with the highest load (NH). The removal rule is to attack the first q% nodes in the descending order of the initial load. The second one is to attack the links with the highest load (LH). The removal rule is to attack the first q% links in the descending order of the initial load. In this work, the attack ratio q% is set to 10%. To ensure that the cascading failure is triggered by targeted attacks, each node and link in the initial network before attacks is at the normal state. We use the proportion of normal nodes $H_n(t)$

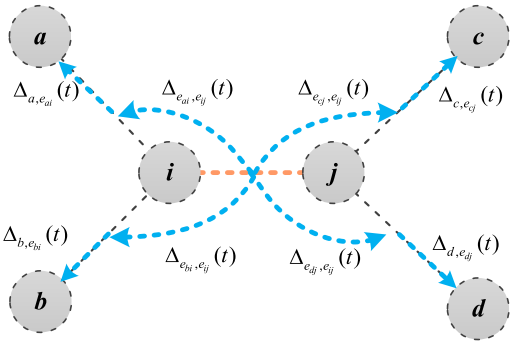


Fig. 7. An example of load redistribution after a link failure.

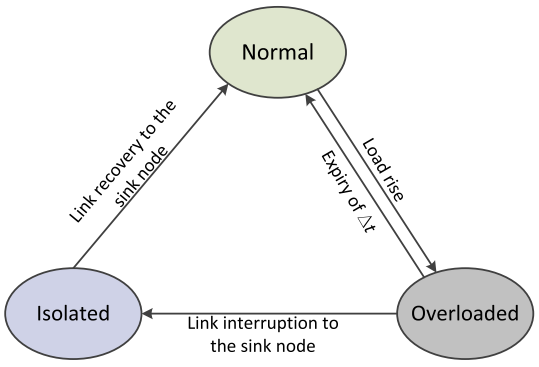
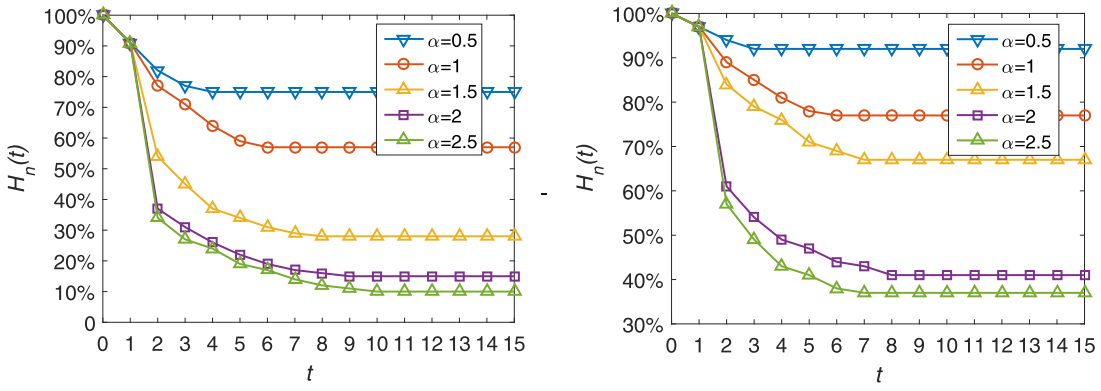
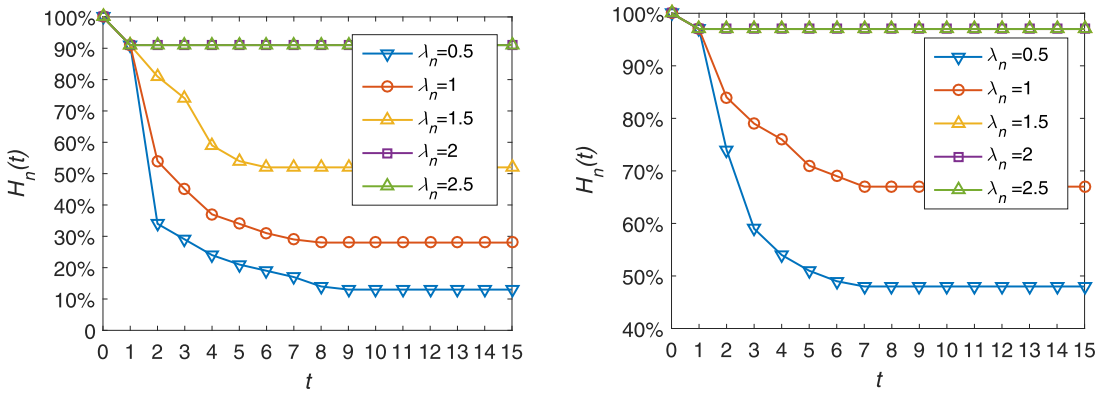


Fig. 8. State transitions of sensor nodes in cascading process.



(a) NH attack scheme (b) LH attack scheme

Fig. 9. Proportion of normal nodes $H_n(t)$ with varying α ($\lambda_n = \lambda_l = 1, \Delta t = \infty$).



(a) NH attack scheme (b) LH attack scheme

Fig. 10. Proportion of normal nodes $H_n(t)$ with varying λ_n ($\alpha = \lambda_l = 1, \Delta t = \infty$).

to measure the network invulnerability against cascading failures. To be fair, $H_n(t)$ under NH attack scheme and LH attack scheme can be calculated by (16) and (17) respectively.

$$H_n(t) = \frac{N_n(t)}{N(1-q\%)}, \tag{16}$$

$$H_n(t) = \frac{N_n(t)}{N}, \tag{17}$$

where $N_n(t)$ is the number of normal nodes at time t respectively. Here we use $H_n(\infty)$ to represent the proportion of normal nodes when the network reaches the steady state respectively.

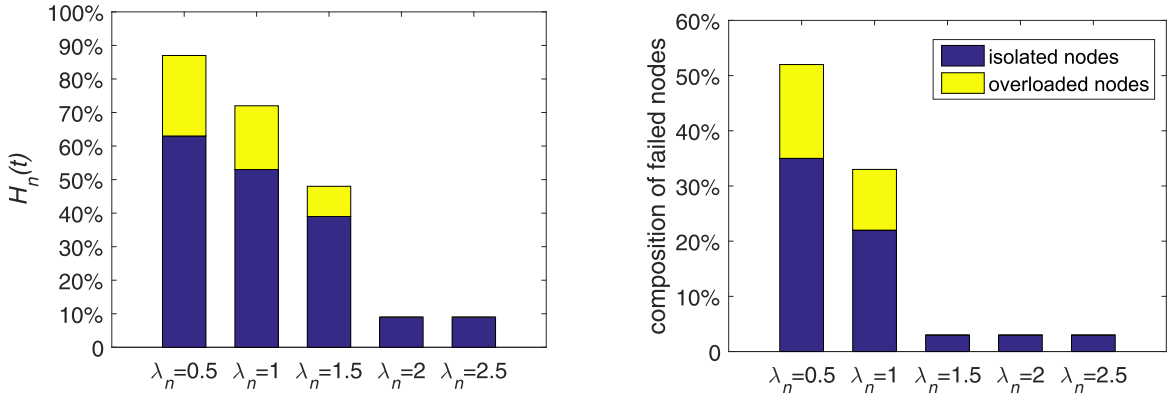
Because of the limited hardware costs in WSNs, we prefer the stronger invulnerability with a smaller cost, where the cost e is defined as follows

$$e = \lambda_n \lambda_l, \tag{18}$$

According to our cascading model, λ_n and λ_l denote the resources invested for the capacity expansion of nodes and links respectively. The product of λ_n and λ_l can naturally reflect the costs for network invulnerability.

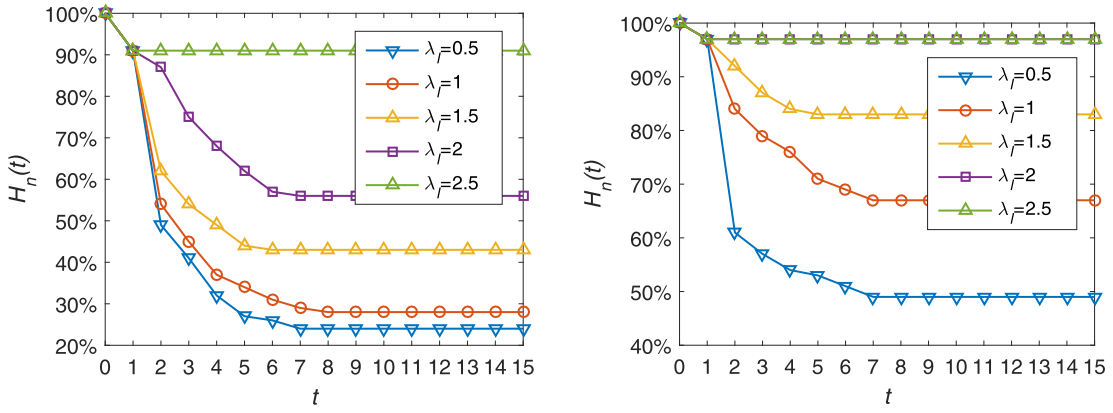
4.2. Simulation results

As is shown in Fig. 9, we can easily find that with the increase of α, the proportion of normal nodes $H_n(t)$ tends to decrease and the cascading process will reach the steady state earlier. For example, under NH attack, when $\alpha = 0.5$, $H_n(t)$ will reach the steady state 75% at time $t = 4$. When α rises to 2.5, $H_n(t)$ will stabilize at 11% at time $t = 9$. It is easy to understand that the load taken by sensor nodes and links will increase much faster in an exponential way with the growth of α, which will lead to a more evident gap between low-load network components (i.e., nodes and links) and high-load network components. When the high-load network components are attacked, the low-load network components can hardly have enough capability to tackle the extra load transferred from failed components. From Fig. 10, we can obtain that the network invulnerability can be significantly improved with the increase of node tolerance coefficient λ_n. In our model, a higher λ_n means that sensor nodes can have more capacity to tackle the load. From Fig. 10(a), we can find that the cascading process under $\lambda_n = 2$ and $\lambda_n = 2.5$ is totally the same. Thus, this is surely a threshold λ_n^* within [1.5,2]. When $\lambda_n \geq \lambda_n^*$, capacity expansion for nodes cannot improve the network invulnerability anymore. From Fig. 10(b), we can also find a similar threshold λ_n^*, which should be within [1,1.5]. Fig. 11 depicts the composition of failed nodes when the network reaches the steady state. We can clearly find that although the nodes being overloaded is the major reason that makes nodes isolated, the majority of failed nodes are isolated nodes. When facing NH attacks, in the case that $\lambda_n = 0.5$, isolated nodes are 63% and overloaded nodes are 24%. With the increase of λ_n, the ratio of overloaded nodes tends to be smaller. In the case that $\lambda_n = 2$ and $\lambda_n = 2.5$, there are no overloaded nodes in the network, which means the cascading process is not triggered. This result reasonably explains the existence of λ_n^*. When λ_n reaches λ_n^*, the cascading process can be avoided and the network invulnerability reaches the saturation point.



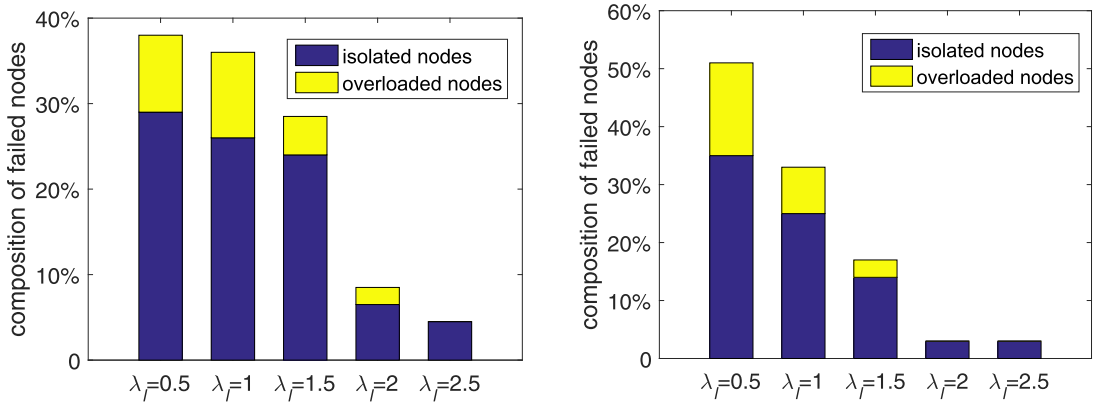
(a) NH attack scheme (b) LH attack scheme

Fig. 11. Composition of failed nodes with varying λ_n ($\alpha = \lambda_l = 1, \Delta t = \infty$).



(a) NH attack scheme (b) LH attack scheme

Fig. 12. Proportion of normal nodes $H_n(t)$ with varying λ_l ($\alpha = \lambda_n = 1, \Delta t = \infty$).



(a) NH attack scheme (b) LH attack scheme

Fig. 13. Composition of failed nodes with varying λ_l ($\alpha = \lambda_n = 1, \Delta t = \infty$).

According to Fig. 12, with the increase of link tolerance coefficient λ_l, $H_n(t)$ can be significantly increased. It is easy to understand that the increase of λ_l can bring the capacity expansion of links, thus reducing the overload risks of links. We also observe that when facing NH attacks, in the case that $\lambda_l = 2.5$, the network reaches the steady state at time $t = 1$, which means the cascading process is not triggered. Thus, we an easily conclude that there is a threshold λ_l^* within [2,2.5] that can protect the network from cascading failures. The results shown in Fig. 13 validate this conclusion.

Fig. 14 depicts the relationship between λ_l and λ_n. The existence of λ_n^* and λ_l^* is further validated. We can also observe that λ_n and λ_l can complement each other in ensuring the network invulnerability. With the increase of λ_n, the threshold λ_l^* will be lower, which means less capacity resources for links are needed. Conversely, with the increase of λ_l, the threshold λ_n^*

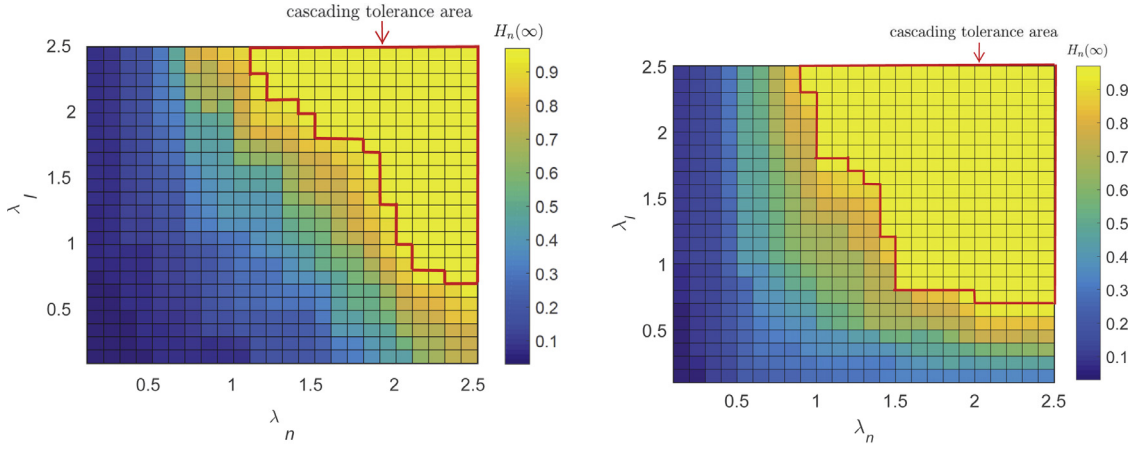


Fig. 14. Heatmap of $H_n(\infty)$ in the parameter space $[\lambda_n, \lambda_l]$.

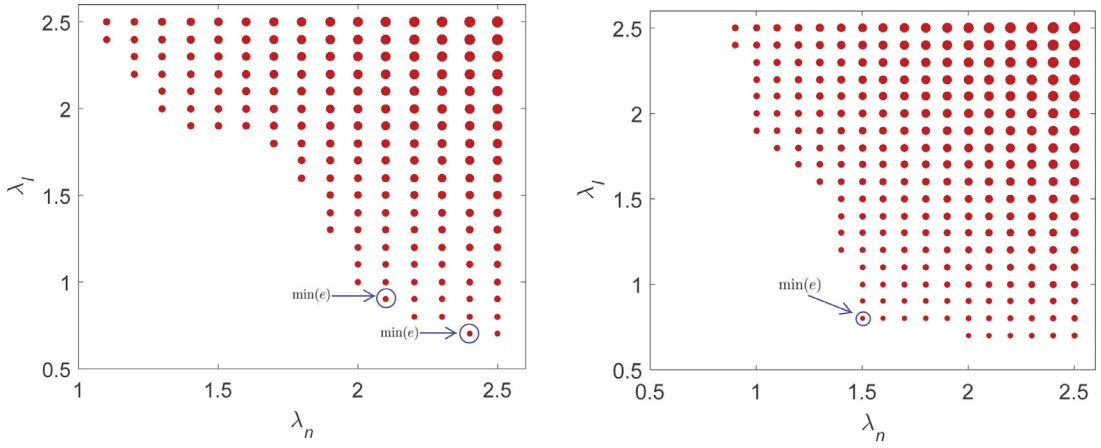


Fig. 15. Scatter diagram of cost e in the cascading-tolerance area (the point size represents the cost value e).

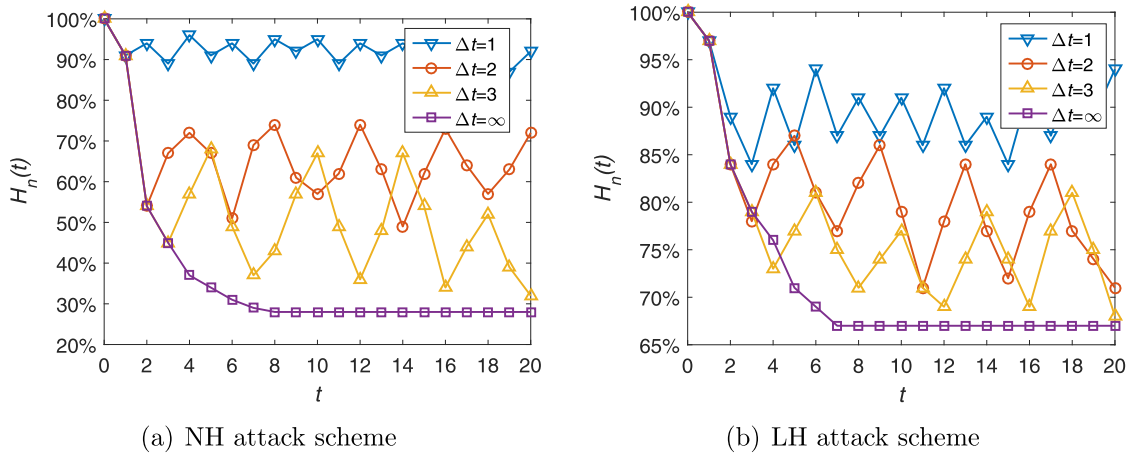


Fig. 16. Proportion of normal nodes $H_n(t)$ with varying Δt ($\alpha = \lambda_n = \lambda_l = 1$).

tends to be decreasing. Besides that, from Fig. 14, we can easily get a value area of (λ_n, λ_l) where the cascading process cannot be triggered. We call this area the "cascading-tolerance area".

Fig. 15 shows the cost curve e of the "cascading-tolerance area" under two different attack schemes. We obtain that the minimum e under NH attack scheme is 1.68, which is at the points (λ_n=2.4,λ_l=0.7) and (λ_n=2.1,λ_l=0.8) and the minimum e under LH attack scheme is 1.2, which is at the point (λ_n=1.5,λ_l=0.8). This tells us an important fact that the minimum costs needed to resist intentional node attacks is more expensive than the costs needed when facing intentional link attacks.

Fig. 16 depicts the impacts of recovery time Δt on the proportion of normal nodes $H_n(t)$. It can be easily observed that $H_n(t)$ tends to fluctuate more wildly as increasing Δt. When Δt=1, it means that the sensor nodes can recover from overload at the next time step, thus $H_n(t)$ fluctuates slightly. In this case, the loss caused by cascading failures can be minimized, but it can be hardly achieved in practice as sensor nodes need time to reboot. When $\Delta t = \infty$, sensor nodes loss the recovery ability and $H_n(t)$ decreases monotonically to a steady-state value.

5. Conclusions

In this paper, we developed a more practical cascading model for WSNs, in which the network load is defined according to two new traffic metric "sink-oriented node betweenness" and "sink-oriented link betweenness" and the overload behavior can occur in nodes and links. The load-redistribution schemes follow the principle of "idle capacity". The most significant advantage of this model is that it can properly reflect the traffic feature of WSNs and reasonably characterize the practical cascading process. The simulation results show that 1) network invulnerability is positively correlated with the tolerance coefficient and negatively correlated with the exponential coefficient; 2) although overload is the trigger condition of cascading process, overload is not the main cause of node failures. Most failed nodes are caused by isolation; 3) the minimum costs needed to resist intentional node attacks are more expensive than the costs needed when facing intentional link attacks; 4) the extension of recovery time will aggravate the fluctuation of cascading process. These results provide us some meaningful guidelines to build a more invulnerable WSN against cascading failures.

1) The network with high-volume data type is more vulnerable to cascading failures.

2) Improving the network connectivity to some extent can improve the network invulnerability against cascading failures.

3) Compared with the overload risks in wireless links, more capacity resources should be invested to protect sensor nodes from overload.

Cascading failures are essentially a load-transfer process along nodes or links. Thus, network topologies play an important role in the cascading process of WSNs. In the next step, we plan to develop a network topology construction method. In this method, the generated topology should be self-tuned according to the real-time load across the network. In addition, in this work, we only focus on one-sink WSNs. In the past few years, due to the outstanding advantages in energy saving and load balancing, the application of multi-sink WSNs is more and more extensive. The addition of multiple sink nodes can significantly change the network load distribution and bring significant differences to the cascading process of WSNs. Therefore, we believe that modeling and optimizing of cascading failures for multi-sink WSNs is a worthwhile research direction.

Declaration of Competing Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

Acknowledgment

This work is supported in part by the National Natural Science Foundation of China (NSFC) under grant nos. 61571336.

References

[1] R.R. Swain, P.M. Khilar, S.K. Bhoi, Heterogeneous fault diagnosis for wireless sensor networks, Ad Hoc Netw. 69 (2018) 15–37.
[2] A. Boukerche, P. Sun, Connectivity and coverage based protocols for wireless sensor networks, Ad Hoc Netw. 80 (2018) 54–69.
[3] S. Shriwastav, D. Ghose, Round-table negotiation for fast restoration of connectivity in partitioned wireless sensor networks, Ad Hoc Netw. 77 (2018) 11–27.
[4] X. Fu, G. Fortino, W. Li, P. Pace, Y. Yang, Wsns-assisted opportunistic network for low-latency message forwarding in sparse settings, Future Gen. Comput. Syst. 91 (2019) 223–237.
[5] X. Fu, Y. Yang, H. Yao, Analysis on invulnerability of wireless sensor network towards cascading failures based on coupled map lattice, Complexity 2018 (3) (2018) 1–14.
[6] Y. Duan, X. Fu, W. Li, Y. Zhang, G. Fortino, Evolution of scale-free wireless sensor networks with feature of small-world networks, Complexity 2017 (3) (2017) 1–15.
[7] B. Khalifa, Z.A. Aghbari, A.M. Khedr, J. Abawajy, Coverage hole repair in wsns using cascaded neighbor intervention, IEEE Sens. J. PP (99) (2017). 1–1
[8] X. Fu, H. Yao, O. Postolache, Y. Yang, Message forwarding for wsn-assisted opportunistic network in disaster scenarios, J. Netw. Comput. Appl. 137 (2019) 11–24.
[9] Y. Li, R. Yin, B. Liu, Cascading failure research on scale-free fault tolerant topology in wireless sensor networks, J. Beijing Univ. Posts Telecommun. 37 (2) (2014) 74–78.
[10] X. Fu, Y. Yang, H. Yao, Modeling and analyzing the cascading invulnerability of wireless sensor networks, IEEE Sens. J. 19 (11) (2019) 4349–4358.
[11] X. Hu, W. Li, X. Fu, Analysis of cascading failure based on wireless sensor networks, in: IEEE International Conference on Systems, Man, and Cybernetics, 2016, pp. 1279–1284.
[12] H.R. Liu, Y.L. Hu, R.R. Yin, Y.J. Deng, Cascading failure model of scale-free topology for avoiding node failure, Neurocomputing 260 (2017).
[13] X. Fu, H. Yao, Y. Yang, Exploring the invulnerability of wireless sensor networks against cascading failures, Inf. Sci. 491 (2019) 289–305.
[14] Z. Ye, T. Wen, Z. Liu, X. Song, C. Fu, Fault-tolerant scheme for cascading failure of scale-free wireless sensor networks, in: IEEE International Conference on Information and Automation, 2017, pp. 2006–2011.
[15] X. Fu, Y. Yang, O. Postolache, Invulnerability of clustering wireless sensor networks against cascading failures, IEEE Syst. J. PP (99) (2018) 1–12.
[16] A.E. Motter, Y.C. Lai, Cascade-based attacks on complex networks, Phys. Rev. E Stat. Nonlinear Soft Matter Phys. 66 (2) (2002) 065102.
[17] L. Tang, K. Jing, J. He, H.E. Stanley, Robustness of assembly supply chain networks by considering risk propagation and cascading failure, Physica A Stat. Mech. Appl. 459 (2016) 129–139.
[18] Y. Wang, F. Zhang, Modeling and analysis of under-load-based cascading failures in supply chain networks, Nonlinear Dyn. 92 (2) (2018) 1–15.
[19] P. Dey, R. Mehra, F. Kazi, S. Wagh, N.M. Singh, Impact of topology on the propagation of cascading failure in power grid, IEEE Trans. Smart Grid 7 (4) (2016) 1970–1978.
[20] Y. Zhu, J. Yan, Y.L. Sun, H. He, Revealing cascading failure vulnerability in power grids using risk-graph, IEEE Trans. Parallel Distrib. Syst. 25 (12) (2014) 3274–3284.
[21] J. Song, E. Cotilla-Sanchez, G. Ghanavati, P.D. Hines, Dynamic modeling of cascading failure in power systems, IEEE Trans. Power Syst. 31 (3) (2016) 2085–2095.
[22] C. Ding, H. Yao, J. Du, X. Peng, Z. Wang, J. Zhao, Cascading failure in interconnected weighted networks based on the state of link, Int. J. Mod. Phys. C 28 (03) (2017) 1750040.
[23] X. Peng, H. Yao, J. Du, Z. Wang, C. Ding, Load-induced cascading failures in interconnected networks, Nonlinear Dyn. 82 (1–2) (2015) 97–105.
[24] W.-X. Wang, G. Chen, Universal robustness characteristic of weighted networks against cascading failure, Phys. Rev. E 77 (2) (2008) 026101.
[25] J. Wang, C. Jiang, J. Qian, Robustness of interdependent networks with different link patterns against cascading failures, Physica A 393 (2014) 535–541.
[26] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy-efficient communication protocol for wireless microsensor networks, in: Hawaii International Conference on System Sciences, 2000, p. 8020.
[27] C. Qiu, H. Shen, K. Chen, An energy-efficient and distributed cooperation mechanism for k-coverage hole detection and healing in wsns, IEEE Trans. Mob. Comput. 17 (6) (2018) 1247–1259.
[28] S. Jannu, P.K. Jana, A grid based clustering and routing algorithm for solving hot spot problem in wireless sensor networks, Wirel. Netw. 22 (6) (2016) 1901–1916.
[29] X. Deng, Z. Tang, L.T. Yang, M. Lin, B. Wang, Confident information coverage hole healing in hybrid industrial wireless sensor networks, IEEE Trans. Ind. Inform. 14 (5) (2018) 2220–2229.
[30] J. Ren, Y. Zhang, K. Zhang, A. Liu, J. Chen, X.S. Shen, Lifetime and energy hole evolution analysis in data-gathering wireless sensor networks, IEEE Trans. Ind. Inform. 12 (2) (2016) 788–800.
[31] H. Huang, H. Yin, G. Min, X. Zhang, W. Zhu, Y. Wu, Coordinate-assisted routing approach to bypass routing holes in wireless sensor networks, IEEE Commun. Mag. 55 (7) (2017) 180–185.

Xiuwen Fu (Corresponding author). He received the B.S. degree in mechanical engineering from Henan University of Science and Technology, China, in 2009 and received M.S. and Ph.D. degrees in mechanical engineering from Wuhan University of Technology, china, in 2012 and 2016 respectively. Currently, he is a lecturer in Shanghai Maritime University. His research interests include wireless sensor networks, complex networks and Internet of things.

Haiqing Yao He received the B.S. and M.S. degrees in mechanical engineering from East China University of Science and Technology, Shanghai, China, in 2009 and 2011 respectively, and received Ph.D. degree in mechanical engineering from East China University of Science and Technology in 2015. Currently, he is a lecturer in Shanghai Maritime University. His research interests include fault detection, signal process and wireless sensor networks.

Yongsheng Yang He received the Ph.D. degree in mechanical engineering from Nanjing University of Aeronautics and Astronautics, China, in 1998. Currently, he is a professor in Shanghai Maritime University. His research interests include Internet of things and modeling of complex systems.