Hindawi
Complexity
Volume 2018, Article ID 6386324, 14 pages
https://doi.org/10.1155/2018/6386324

Research Article

Analysis on Invulnerability of Wireless Sensor Network towards Cascading Failures Based on Coupled Map Lattice

Xiuwen Fu, Yongsheng Yang, and Haiqing Yao

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

Correspondence should be addressed to Xiuwen Fu; fuxiuwen1987@163.com

Received 21 August 2017; Revised 11 December 2017; Accepted 28 December 2017; Published 28 January 2018

Academic Editor: Ilaria Giannoccaro

Previous research of wireless sensor networks (WSNs) invulnerability mainly focuses on the static topology, while ignoring the cascading process of the network caused by the dynamic changes of load. Therefore, given the realistic features of WSNs, in this paper we research the invulnerability of WSNs with respect to cascading failures based on the coupled map lattice (CML). The invulnerability and the cascading process of four types of network topologies (i.e., random network, small-world network, homogenous scale-free network, and heterogeneous scale-free network) under various attack schemes (i.e., random attack, max-degree attack, and max-status attack) are investigated, respectively. The simulation results demonstrate that the rise of interference R and coupling coefficient ε will increase the risks of cascading failures. Cascading threshold values R_c and ε_c exist, where cascading failures will spread to the entire network when $R > R_c$ or $\varepsilon > \varepsilon_c$. When facing a random attack or max-status attack, the network with higher heterogeneity tends to have a stronger invulnerability towards cascading failures. Conversely, when facing a max-degree attack, the network with higher uniformity tends to have a better performance. Besides that, we have also proved that the spreading speed of cascading failures is inversely proportional to the average path length of the network and the increase of average degree $\langle k \rangle$ can improve the network invulnerability.

1. Introduction

Wireless sensor networks (WSNs) are usually made up of hundreds, even thousands, of distributed sensor nodes organized in ad hoc paradigm to monitor the environment. Since they can be easily deployed and self-organized, WSNs can cover a wide range of applications domains [1, 2]. As in most of the scenarios WSNs are expected to operate in unattended environments, the sensor nodes always suffer from the risks of energy depletion, hardware malfunction, or deliberate attacks [3, 4]. Failures of sensor nodes would split originally connected network topology, would reduce the coverage of the network, and might even lead to a global network paralysis. Therefore, how to establish an invulnerable WSN has been a hot research issue in recent years.

Most of current research on invulnerability of WSNs mainly focuses on the connectivity and availability of the network topology after removing a certain number of nodes or links. Although some promising progress has been made in building an invulnerable network topology, all this work fails to take into consideration the impacts of load redistribution on topology invulnerability. In real WSNs, the changes in network topology would give rise to the redistribution of data flow in the network, thus leading to the dynamic changes of network load. The capacity of a sensor node tackling or transmitting data is always limited due to the constrained hardware cost. When the real-time data load is beyond its capacity, it is highly likely to turn into failure. When a node fails, those nodes which transmit data via this failure node have to choose new paths to transmit data, thus leading to the load redistribution in the network. This load-redistribution process might make some new nodes fail due to capacity spilled and these failure nodes would lead to a new round of cascading failures. Consequently, more and more failure nodes are removed from the topology and this process will be repeated until there is no new node turning into failure. Therefore, the cascading process is a common phenomenon in WSNs, which is also a crucial factor to influence the network invulnerability [5, 6]. Especially with the wider application of wireless multimedia sensor

networks, the risks of overload in WSNs tend to be higher and the threats of cascading failures cannot be ignored anymore. But unfortunately, current research about cascading failures of WSNs is still rare.

Coupled map lattice (CML) is a dynamical system that models the behavior of nonlinear systems. As far as the network simulation is concerned, CML considers the network system as a time-discrete and space-discrete system. In the CML-modeling network system, by observing the interaction among nodes and the self-status changes of nodes, the dynamic behavior of the network can be well studied [7]. CML has been widely applied in the domain of complex networks due to its easy-modeling and high-computation efficiency advantages. The first CML model was proposed in [8] for the studies of spatiotemporal chaos. After that, many CML models have been developed for different applications. Leung et al. [9] developed a radial-based CML model for signal detection. Zhang and Wang [10] proposed a mixed linear-nonlinear CML model for image encryption. Konishi et al. [11] presented a car-following CML model for suppression of traffic congestion. Kohar et al. [12] used a quadratic CML method to research the role of network topology in noise reduction. For cascading failures, its inner essence is that a single node's failure is possible to spread to the entire network due to the coupled relationship with others. Considering the coupled feature of cascading failures, CML is a convincing theoretical tool to research it. Due to this reason, Wang and Xu [13] researched the cascading process of globally coupled networks based on CML. Cui et al. [14] studied the cascading failures of small-world networks. Di et al. [15] investigated the tolerance of edge cascades with CML method. Xu and Wang [16] researched the cascading process of scale-free networks.

But as WSN is a physical network featured by limited transmission radius, which is quite different from general complex network, its cascading process would demonstrate evident differences compared with other networks. Therefore, in this paper our goal is to investigate the invulnerability of various WSN topologies towards cascading failures with CML method. The contribution of this paper covers four aspects:

(1) We develop a cascading model of WSNs based on CML and propose four network topology construction methods (i.e., random network, small-world network, homogeneous scale-free network, and heterogeneous scale-free network) considering the limited transmission radius feature of WSNs.

(2) We analyze the degree distribution of the network topology generated by our methods theoretically. We prove that the generated scale-free network topologies are featured by pow-law degree distribution and the degree distributions of generated random network and small-world network are characterized by Poisson distribution.

(3) We design three attack schemes (i.e., random attack, max-degree attack, and max-status attack) as the trigger conditions for cascading process of WSNs. We investigate the cascading invulnerability under three attack schemes.

(4) Simulation results demonstrate that scale-free networks have stronger invulnerability when facing a random attack. Random network and small-world network perform better when facing a max-degree attack. Max-status attack can trigger cascading failures with less interference. The spreading speed of cascading failures is inversely proportional to the average path length of the network and increasing average degree can improve the network invulnerability.

The remainder of this paper is organized as follows. Section 2 describes the related work. Section 3 provides the cascading model of WSNs based on CML. Then, we give the topology construction methods of WSNs in Section 4 and give a theoretical analysis on their network characteristics from the perspective of degree distribution in Section 5. In Section 6, we propose the attack schemes and investigate the cascading failures invulnerability of WSNs under different attack schemes. Finally, we summarize our work and draw conclusions in Section 7.

2. Related Works

Current research about how to build an invulnerable WSN topology can be classified into three types: scale-free network, small-world network, and k-connectivity network. In scale-free networks, a few numbers of central nodes possess most of connections in the network, making the network invulnerable to random failures. In this area, Zhu et al. [17] proposed two scale-free evolution models EAEM and EBEM. In EAEM, the newly joined node prefers to connect the existing nodes with higher degree. In EBEM, the newly joined node is more likely to build connections with the existing nodes with higher degree and more remaining energy. Simulation results proved that both models are able to generate scale-free WSN topologies, but EBEM model is more energy-efficient. Luo et al. [18] proposed a scale-free model by introducing a link adding/deleting action. In Luo et al.'s model, besides adding new nodes into the network at each time round, the links between poor-energy nodes are likely to be removed and a new link might be built between a pair of rich-energy nodes. Since, in real WSNs, the failures of wireless links are more likely to occur than nodes failures, the scale-free topology generated by Luo et al.'s model is closer to the real scenario. The small-world network theory has also proved to be an effective tool to improve the network invulnerability. Helmy [19] firstly proved that, by introducing wired links as shortcuts into WSNs, the network can maintain relatively low average path length and high cluster coefficient. In our previous work [20], we found that when the number of shortcuts reaches 20% of the total number of nodes in the network, the fault tolerance of the network can be improved by 50%. Compared with scale-free network and small-world network, k-connectivity topology is the most common method in improving network invulnerability. The basic idea behind k-connectivity topology is to ensure each node in the network maintaining at least k paths towards other nodes. In this way, even if $k-1$ paths were cut off, the node can still deliver messages to other nodes successfully. Joshi and Younis [21] found that when the network size is large enough, k-connectivity network tends to be similar to random network, both of which degree distributions follow Poisson distribution. In WSNs, we can adopt two methods to achieve k-connectivity.

One is to introduce relay nodes into the network. Compared with the common nodes, relay nodes are equipped with more powerful batteries and transmission modules. Han et al. [22] proposed a relay node placement scheme PFRP. In this scheme, common nodes choose nearest relay nodes as their cluster heads and the backbone network that is composed of relay nodes are designed for k-connectivity. Another one is to adjust transmission power of sensor nodes to achieve k-connectivity. Since in WSNs the transmission radius of sensor nodes is always limited, network connectivity can only reach $k = 2$ or 3 in most cases. Lin et al. [23] firstly simplified the transmission power adjusting issue as the transmission range assignment issue and proved that this issue in two-dimensional space is NP-hard.

A thorough analysis and overview of invulnerability of WSNs can be found in [24]. Through analyzing existing solutions, one can conclude that existing topology construction methods mainly focus on the improvement of fault tolerance in a static point of view, but fail to consider the dynamic impacts of cascading process caused by load redistribution. Therefore, in order to understand the cascading process of WSNs and find out which topology structure tends to be more vulnerable against cascading failures, in what follows we investigate the cascading invulnerability of different network topologies under three attack schemes based on CML.

3. Cascading Model of WSNs Based on CML

Considering that the links between sensor nodes are bidirectional in most of WSNs, we use undirected graph $G = (V, E)$ to represent the topology of WSNs, where V is the collection of sensor nodes and E is the collection of links.

Based on the CML model proposed by Wang and Xu [13], we give a CML-based cascading model for WSNs:

$$x_i(t+1) = \left| (1-\varepsilon) f\left(x_i(t)\right) + \varepsilon \sum_{j=1, j\neq i}^{N} a_{ij}(t) \frac{f\left(x_j(t)\right)}{k_i(t)} \right|, \quad (1)$$

where $x_i(t)$ means the status of node i at time t and N is the total number of nodes in the network. If $x_i(t) \in (0, 1)$, node i is at the normal status, which means its real-time load is within its capacity. On the contrary, if $x_i(t) \geq 1$, node i is in failure status which means its real-time load has already been beyond its capacity. In this case, for any moment $m > t + 1$, $x_i(m) \equiv 0$ and the edges of node i would be also removed from the network. In this model, link status among N nodes is indicated by the adjacent matrix $A = [a_{ij}(t)]_{N\times N}$. If node i connects with node j at time t, $a_{ij}(t) = 1$. If no connection exists between nodes i and j, $a_{ij}(t) = 0$. $k_i(t)$ is the degree of node i at time t, which is equal to the sum of each element in i row of A. In WSNs, $k_i(t) = \sum_{j=1}^{N} a_{ij}(t)$ represents the number of adjacent nodes that node i has. $\varepsilon \in [0, 1]$ is the coupled coefficient, representing the coupled level between a pair of adjacent nodes. $\varepsilon = 0$ indicates that adjacent nodes cannot influence each other. With the increase of ε, the mutual influence tends to be more evident.

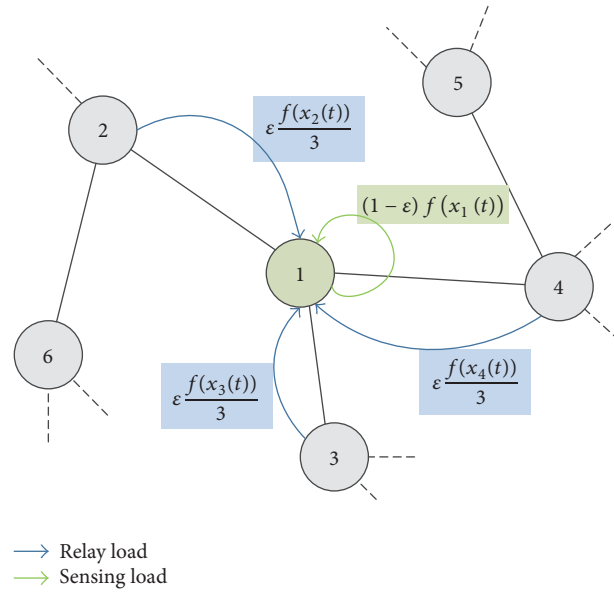


Figure 1: An example of load composition.

Nonlinear function $f(x)$ means the dynamic behavior of a sensor node in WSNs. Here we choose the logistics function $f(x) = 4x(1 - x)$. This function is often adopted in the network in which nodes can be easily affected by adjacent nodes [25]. As far as WSN is concerned, on the one hand, the capacity of sensor nodes is usually limited due to low-cost reason, making them sensitive to load change. On the other hand, sensor nodes in WSNs need to receive messages from last-hop nodes and relay them to next-hop nodes, meaning that sensor nodes are required to maintain frequent load-exchange with their adjacent nodes. Therefore, using logistics function to represent the dynamic behavior of WSNs is a reasonable choice. For logistics function, $f(x) \in [0, 1]$ when $x \in [0, 1]$.

Aiming to monitor the large area, WSNs deliver the environmental data to the base station via multihop relay. Therefore, the load of a sensor node consists of two parts: sensing load and relay load. For sensor node i, the sensing load is the load generated by its own sensing tasks, which is only related to its self-status function $f(x_i(t))$. The relay load is the load generated by relaying the data from its neighbors; thus it is only related to the status functions of its neighbors $\varepsilon \sum_{j=1, j\neq i}^{N} a_{ij}(f(x_j(t))/k(i))$. Coupled coefficient ε is to adjust the proportion between the sensing load and the relay load. By combining the sensing load and relay load, we can get the total load in (1). To state this more clearly, here we present an example on a simplified network topology shown in Figure 1.

Assume all the nodes can operate well at time t, since node 1 does not have connections with nodes 5 and 6, $a_{15}(t) = a_{16}(t) = 0$. According to (1), no data packets will be transferred from nodes 5 and 6 to node 1. For the nodes connecting to node 1, node 1 needs to help relay the data from them and thus their status would affect the status of node 1. Besides performing the relay tasks, node 1 needs to take the sensing load $(1-\varepsilon) f(x_1(t))$ generated by its own sensing tasks.

By combining all these loads, we can get the total load of node 1 at time $t + 1$ which is

$$x_1(t+1) = (1-\varepsilon) f(x_1(t)) + \sum_{k=1,2,3} \varepsilon \frac{f(x_k(t))}{3}. \quad (2)$$

In real WSNs, sensor nodes always fall into failure due to external factors (e.g., harsh environment or malicious attack) or internal factors (e.g., hardware/software breakdown or energy exhaustion). In CML-based cascading model, all these factors are defined as interference R. After imposing interference R at time t, the status of node i at time $t + 1$ can be expressed as

$$x_i(t+1) = \left| (1-\varepsilon) f(x_i(t)) + \varepsilon \sum_{j=1, j\neq i}^{N} a_{ij}(t) \frac{f(x_j(t))}{k_i(t)} \right| + R. \quad (3)$$

Obviously, in this case, the failure probability of node i will become higher with the increase of R. If $x_i(t + 1) \geq 1$, node i will fail at time $t + 1$. The adjacent nodes of node i will be influenced by the change of $x_i(t+1)$ and their status at time $t+2$ will update according to (1). If there are nodes whose updated status is larger than 1 at time $t + 2$, they would turn into failure immediately. In the same way, new failure nodes would result in a new round of failure spread. This spreading process would not stop until there is no new node turning into failure.

4. Topology Construction Methods of WSNs

In this section, aiming to investigate the invulnerability of different WSNs topologies towards cascading failures, we propose four topology construction methods: random network, small-world network, homogeneous scale-free network, and heterogeneous scale-free network.

4.1. Random Network. In Erdos-Renyi (E-R) random model [26], the initial network starts from N isolated nodes. Each pair of nodes in the network can be connected according to probability p. In E-R random model, the number of edges M is random, but its average value is $pN(N-1)/2$. The average degree $\langle k \rangle$ of the generated network topology is $p(N-1)$. But, for WSNs, since sensor node can only be allowed to connect with other nodes within its transmission radius, E-R random model is not appropriate for WSNs. Due to this reason, we design a topology construction method for random WSNs.

(1) Initialization. Randomly deploy N isolated sensor nodes. The transmission radius of sensor nodes is R_a. After that, each node is required to link to all the nodes within its transmission radius. Assume the total number of links in the network is M_s. In order to avoid creating separated topology, any node should have at least one effective path to any other nodes in the network.

(2) Link Deletion. Randomly choose M_d ($M_d \leq M_s$) as retained links and the remaining $M_s - M_d$ links are deleted from the initial network. We still need to ensure the generated topology is not separated.

After these two steps, we can obtain a random topology of which the average degree $\langle k \rangle$ is $2M_d/N$ and also conforming to the limited transmission radius feature of WSNs.

4.2. Small-World Network. As a transitive network type between random network and regular network, the small-world network was proposed in 1999 by Newman and Watts [27]. Although most of the nodes in the small-world network are not directly connected, the vast majority of nodes can be connected to each other only via a few hops. Hence, the small-world network exhibits a small average path length along with a large clustering coefficient. As far as WSNs are concerned, lowering relay hops from sensor nodes to the base station is the basic idea to improve the network performance in terms of lifetime and invulnerability. Thus, it is reasonable to expect that constructing WSNs topology with small-world effect is a feasible method to improve the network connectivity and reduce the network energy consumption. Helmy [19] firstly proved that small-world effect can also be applied in WSNs by introducing long-distance wired cables. In their solution, a certain amount of wired cables are deployed in the network and the cables can make the sensor nodes at their ends communicate with each other. Since the length of the deployed cables could be longer than the wireless transmission radius of sensor nodes, wired cables can play the same role of shortcuts. In this subsection, we use a similar way to build a small-world WSN by introducing wired cables.

(1) Initialization. According to the method mentioned in Section 4.1, we can get a random network topology with N nodes and M_d links.

(2) Random Reconnection. Reconnect links according to probability p_r. The link selected for reconnection would keep one endpoint unchanged and connect to a new node that is different from the previous one.

Through this method, the generated topology includes $p_r M_d$ shortcuts and its average degree is still $2M_d/N$.

4.3. Homogeneous Scale-Free Network. The most evident feature of scale-free network is that the degree distribution $P(k)$ of the network is in line with power-law distribution. Since in scale-free networks the high-degree nodes only account for a small proportion of the network, the failure probability of these nodes is at a relatively low level when facing random failures. By contrast, for the low-degree nodes that widely spread in the network, although these nodes have to take a much higher failure risk, the failures of these nodes have little effect on network performance. Due to this reason, scale-free networks demonstrate excellent survivability against random attacks. For WSNs, aiming to build a scale-free network topology that is closed to the practical case, besides the node degree, energy also should be taken into consideration due to its energy-sensitivity feature. Therefore, in this subsection we propose a homogeneous scale-free topology construction method considering the energy factor.

(1) Initialization. According to the method mentioned in Section 4.1, we can get a random network topology with m_0 nodes and e_0 links.

(2) Preferential Attachment. At each time step, a new node will join the network and connect to m_h ($m_h \leq m_0$) nodes that are within its transmission radius R_a. The probability $P_{ij}(t)$ of the new node i connecting to the existing node j at time t is proportional to the degree $k_j(t)$ and the energy $E_j(t)$.

$$P_{ij}(t) = \frac{k_j(t) E_j(t)}{\sum_{n=1}^{N(t)} \left(k_n(t) E_n(t)\right)}, \tag{4}$$

where $N(t)$ is the total number of the sensor nodes that are within the transmission radius of newly joined node i at time t. Therefore, if a node has more energy and links, it could have a higher probability to link with newly joined node. After t time steps, we can create a scale-free WSN topology with $m_0 + t$ nodes and $e_0 + m_h t$ links. Its average degree is $2(e_0 + m_h t)/(m_0 + t)$.

4.4. Heterogeneous Scale-Free Network. Since WSNs are featured by energy sensitivity, how to prolong the network lifetime is always a central topic in the studies of WSNs. Aiming to achieve this goal, in most cases clustering structure is introduced into the network to guarantee cost-effective data transmission via multiple hops. Clustering WSNs are composed of cluster heads and cluster members. Cluster members are responsible for collecting environmental data and transferring these data to the cluster heads that they belong to. The responsibility of cluster heads is to deliver these data to others via multiple hops. In this subsection, we propose a heterogeneous scale-free topology construction method considering the clustering structure of WSNs.

(1) Initialization. According to the method mentioned in Section 4.1, we can get a random network topology with m_0 nodes and e_0 links. All the nodes in the initial network are configured as cluster heads.

(2) Preferential Attachment. At each time step, a new cluster head or cluster member with m_h edges enters into the existing network with probability p_c or $1 - p_c$, respectively. The new node will join the network and connect to m_h ($m_h \leq m_0$) cluster heads that are within its transmission radius R_a. The probability $P_{ij}(t)$ of the new node i connecting to the existing cluster head j at time t is proportional to the degree $k_j(t)$ and energy $E_j(t)$.

$$P_{ij}(t) = \frac{\delta_j(t) k_j(t) E_j(t)}{\sum_{n=1}^{S(t)} \left(\delta_n(t) k_n(t) E_n(t)\right)}, \tag{5}$$

where $S(t)$ is the total number of cluster heads at time t and $\delta_n(t)$ is the degree saturation coefficient used for constraining the maximum number of connections a cluster head could have.

$$\delta_n(t) = \begin{cases} 1 & k_n(t) < k_{\max} \\ 0 & k_n(t) = k_{\max}. \end{cases} \tag{6}$$

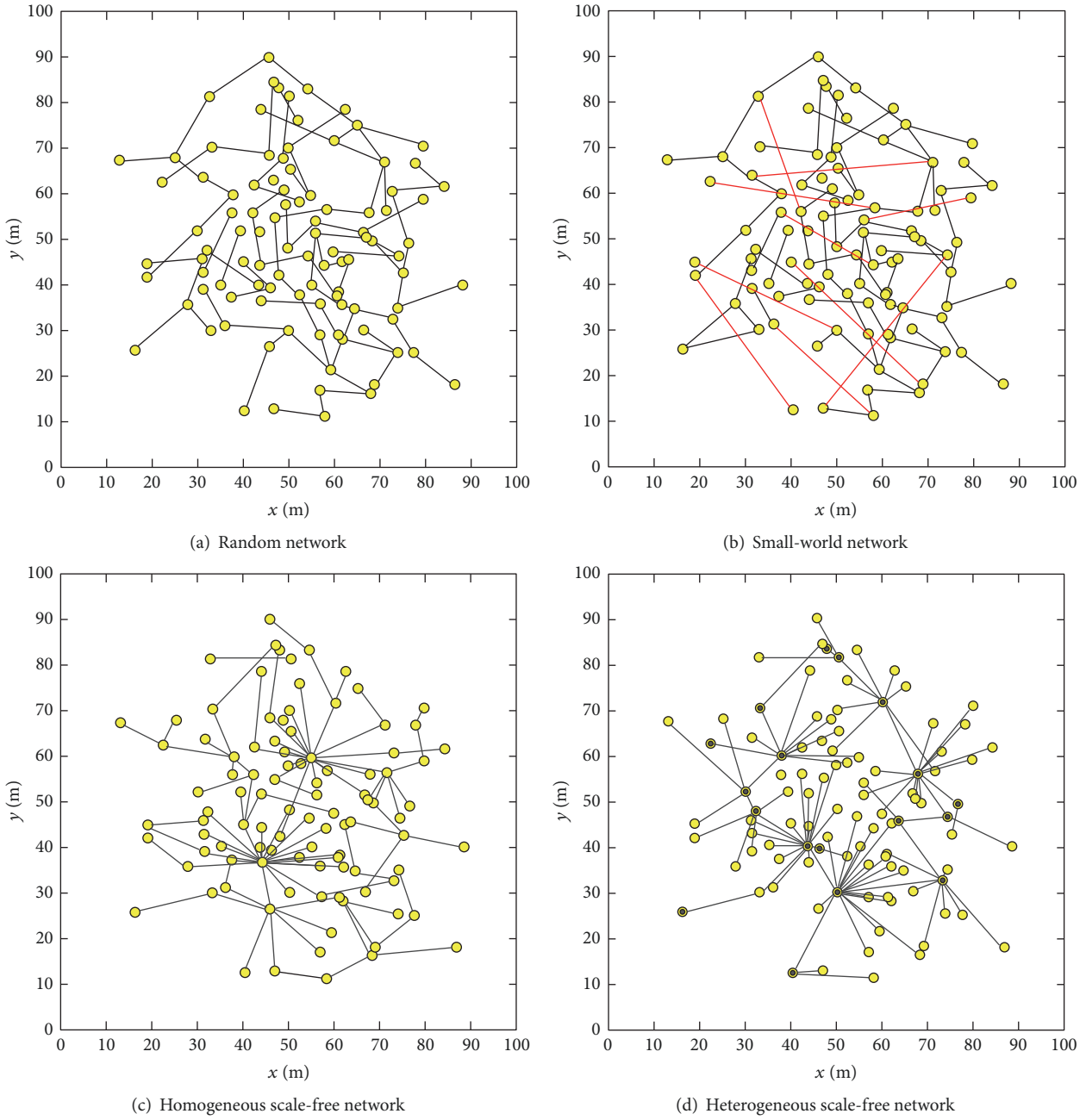
In most of the clustering WSNs, maximum number of connections that a cluster head could have is always fixed to ensure that cluster heads would not overload. Thus, in our model we use $k_{\max}$ to represent the upper limit of connections of cluster heads. If the degree (number of connections) of cluster head j reaches the degree saturation $k_{\max}$ at time t, $\delta_j(t) = 0$ and thus $P_{ij}(t) = 0$, which means that the cluster head j cannot have more connections if its degree achieves $k_{\max}$. Through this mechanism, we can ensure that the cluster heads with higher degree or with more energy are more likely to have new connections while they would not overload.

After t time steps, we can create a heterogeneous scale-free WSN topology with $m_0 + pt$ cluster heads and $(1 - p)t$ cluster members according to probability.

4.5. An Example of Network Topologies. Figure 2 is an example of the network topologies generated by our methods. The simulation area is 100 m × 100 m. The transmission radius R_a of sensor nodes is configured as 20 m. The total number of nodes $N = 100$. Aiming to ensure the generated topologies having the same average degree $\langle k \rangle$, we set the following: (1) for random network, the retained links $M_d = 100$; (2) for small-world network, reconnection probability $p_r = 0.05$; (3) for homogeneous scale-free network, the initial number of nodes $m_0 = 10$ and the initial number of links $e_0 = 10$; at each time step one new node will join the network and connect with $m_h = 1$ existing node. After 90 time steps, the network growth stops. For energy configuration, by referencing the parameter settings in [20], we configure the energy distribution E_i complying with the truncated normal distribution $N(2, 1)$ and the valid interval for E_i is $[0, 4]$. As the energy consumption during the topology construction phase can be ignored, here E_i is a static value; (4) for heterogeneous scale-free network, the initial network consists of 10 cluster heads and 10 links. The ratio of cluster heads $p_c = 0.2$. At each time step one new node will join the network and connect with $m_h = 1$ existing cluster head. The maximum number of connections that a cluster head could have $k_{\max} = 30$. Other configurations are the same as in homogeneous scale-free network. According to the above configurations, it is easy to get that the average degree $\langle k \rangle = 2$ in four generated topologies.

Figure 3 is the average degree distribution of random network and small-world network according to the configurations adopted in Figure 1 after 50 simulations. For easier description, here we use RN and SN as the abbreviations of random network and small-world network, respectively. From Figure 2, we can easily find that their degree distributions follow Poisson distribution, which is consistent with the general description of the random network and the small-world network. In these two kinds of networks, the degree of about 58% of nodes is 2 or 3. The degree of the remaining nodes is mainly distributed over 1 and 4.

Figure 4 shows the average degree distribution of homogeneous scale-free network and heterogeneous scale-free network after 50 simulations. For the convenience of description, here we use Homo-SFN and Heter-SFN as the abbreviations of homogeneous scale-free network and heterogeneous scale-free network, respectively. Different from random network



(a) Random network

(b) Small-world network

(c) Homogeneous scale-free network

(d) Heterogeneous scale-free network

Figure 2: A sample of four topology construction methods.

and small-world network, in heterogeneous scale-free network and homogeneous scale-free network the degree of most of the nodes is 1; the highest degree in two models is 23 and 28, respectively. From Figure 3, it can be easily observed that in log-log coordinates the degree distributions of heterogeneous scale-free network and homogeneous one demonstrate an evident power-law feature. It is worth noting that in heterogeneous scale-free network about 85% of newly joined nodes are determined to be cluster members, which means that all these nodes can only have one connection with their cluster heads. Therefore, the proportion of marginal nodes (i.e., the node whose degree is 1) in a heterogeneous scale-free network is higher than in a homogeneous one.

5. Theoretical Analysis on Degree Distribution

Degree distribution $P(k)$ is the probability that a randomly chosen node has k connections (or neighbors) and it can also be defined as the fraction of nodes in the network with degree k. It is considered as the most important property that could characterize a network structure. For random network and small-world network, their degree distributions are featured

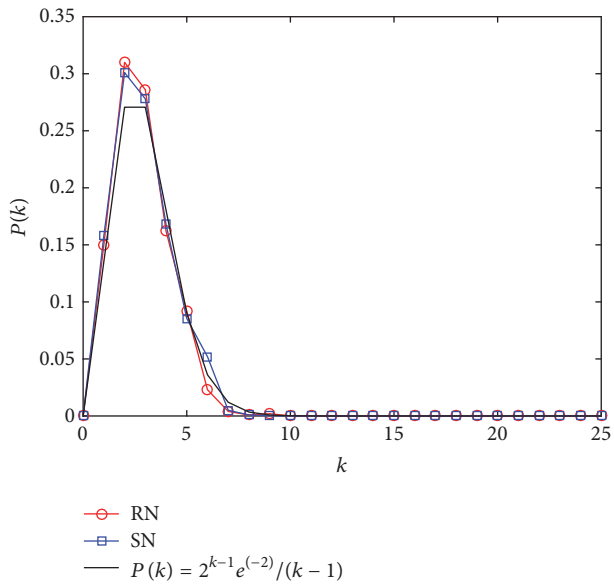


Figure 3: Degree distribution of random network and small-world network.

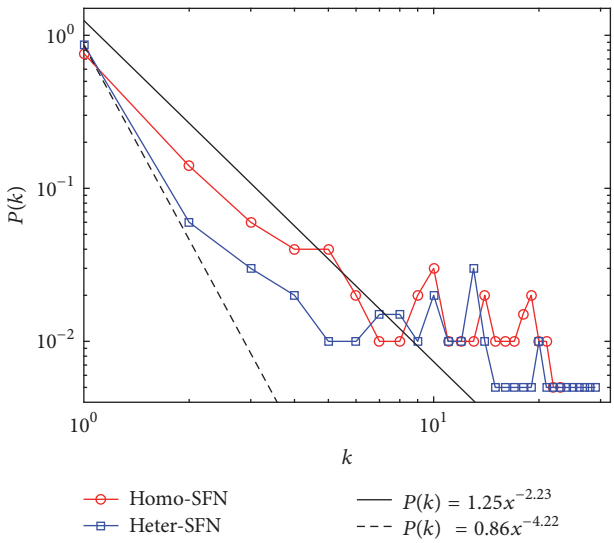


Figure 4: Degree distribution of homogeneous scale-free network and heterogeneous scale-free network.

by Poisson distribution. For scale-free networks, their degree distributions are characterized by power-law distribution. Therefore, aiming to further confirm the properties of our models, we carry out a theoretical analysis on their degree distributions $P(k)$ in this section.

5.1. Random Network and Small-World Network. In [26], for a E-R random network that consists of N nodes and where each edge is included with probability p, it has been proved that its degree distribution follows

$$P(k) = C_{N-1}^{k} p^{k} (1-p)^{N-1-k} \approx \frac{\langle k \rangle^{k} e^{-\langle k \rangle}}{k!}. \quad (7)$$

E-R random model allows isolated nodes to exist, which means the minimum degree in the network could be zero. But in our random network model, in order to ensure generated network topologies well-functioning, any nodes should maintain at least one path to others, which means that the minimum degree in the network should be at least one. Besides that, we have already known the average degree $\langle k \rangle$ in our random network model is $2M_d/N$. Therefore, through the translation process, we can easily get

$$P(k) \approx \frac{\langle k \rangle^{(k-1)} e^{-\langle k \rangle}}{(k-1)!} = \frac{(2M_d)^{k} e^{-2M_d/N}}{N^{k}(k-1)!}. \quad (8)$$

For small-world network model, since the number of existing links M_d is unchanged and the shortcuts reconnection process is still in a random way, its degree distribution is the same as in the random network model. When $N = 100$ and $M_d = 100$, we can get $P(k) \approx 2^{(k-1)}e^{-2}/(k-1)!$. As is shown in Figure 3, the simulation curves are quite closed to the theoretical curve. The correctness of $P(k)$ is further validated and the random feature of our models has also been validated by proving their degree distributions following Poisson distribution.

5.2. Heterogeneous Scale-Free Network and Homogeneous Scale-Free Network. As the homogeneous scale-free network is equivalent to a heterogeneous one when the ratio of cluster heads p_c is 100%, the homogeneous scale-free network can be deemed as a special case of the heterogeneous scale-free network. Therefore in this section, we firstly carry out a theoretical analysis on the degree distribution of heterogeneous scale-free network. In heterogeneous scale-free network model, as cluster members can be allowed to build m_h connections with the cluster heads that they belong to, their degree would always be m_h. But for cluster heads, their degree $k_j(t)$ would increase with the expanding size of the network. According to our topology construction method in Section 4.4, in step (2) the cluster head j connects to the newly joined node i according to the preferential attachment probability $P_{ij}(t)$. The growth rate of $k_j(t)$ can be described as

$$\frac{\partial k_j(t)}{\partial t} = m_h \frac{\delta_j(t) k_j(t) E_j}{\sum_{n=1}^{S(t)} [\delta_n(t) k_n(t) E_n]}, \quad (9)$$

where $S(t)$ is the total number of cluster heads at time t. We can easily get $S(t) = m_0 + p_c t$. In most cases, the degree $k_j(t)$ of most of cluster heads is much smaller than degree saturation $k_{\max}$; we can reasonably assume that $\delta_n(t) = 1$.

Since WSNs are mainly applied in the scenario requiring large-scale deployment, we can reasonably assume that, after experiencing a long-term evolution, the number of sensor nodes has reached a large enough size. Thus, we can get the following:

$$\sum_{n=1}^{S(t)} E_n k_n(t) = S(t) \langle k_h(t) \rangle \overline{E} \approx p_c t \langle k_h(t) \rangle \overline{E}, \quad (10)$$

where $\langle k_h(t) \rangle$ is the average degree of cluster heads at time t and $\overline{E}$ is the average energy expectation of sensor nodes in

the network. Assume $D(t)$ and $C(t)$ are total degree of nodes and cluster members, respectively; we can easily get $D(t) = 2(e_0 + m_h t)$ and $C(t) = (1 - p_c)m_h t$. Thus, $\langle k_h(t)\rangle$ can be calculated as

$$\begin{aligned}\left\langle k_h(t)\right\rangle &= \frac{D(t) - C(t)}{S(t)} = \frac{2m_0 + m_h t + p_c m t}{m_0 + p_c t} \\ &\approx \frac{m_h(1 + p_c)}{p_c}, \quad t \longrightarrow \infty.\end{aligned} \tag{11}$$

Substitute (10) and (11) into (9); then we can get

$$\frac{\partial k_j(t)}{\partial t} = \frac{k_j(t)E_j}{(1 + p_c)\overline{E}t}. \tag{12}$$

Via equivalent transformation of (12), we can get

$$\frac{\partial k_j(t)}{k_j} = \frac{E_j \partial t}{(1 + p_c)\overline{E}t}. \tag{13}$$

Given the generation rules of the network, each cluster head j has initial degree m_h. Consider this as the initial condition $k_j(t_j) = m_h$ for (13); we can solve it and get

$$k_j(t_j) = m_h\left(\frac{t}{t_j}\right)^{E_j/(1+p_c)\overline{E}}. \tag{14}$$

Equation (14) can be used to get the probability $P[k_j(t_j) < k]$

$$\begin{aligned}P\left[k_j(t_j) < k\right] &= P\left[t_j > t\left(\frac{k}{m_h}\right)^{-(1+p_c)\overline{E}/E_j}\right] \\ &= 1 - P\left[t_j \le t\left(\frac{m_h}{k}\right)^{(1+p_c)\overline{E}/E_j}\right].\end{aligned} \tag{15}$$

Generally assume that sensor nodes are added to the network at regular intervals, so t_j has equal probability density $P(t_j) = 1/(m_0 + t)$; then we can get

$$\begin{aligned}P\left[k_j(t) < k\right] &= 1 - \frac{t}{m_0 + t}\left(\frac{m_h}{k}\right)^{(1+p_c)\overline{E}/E_j} \\ &\approx 1 - \left(\frac{m_h}{k}\right)^{(1+p_c)\overline{E}/E_j}.\end{aligned} \tag{16}$$

Degree distribution $P(k)$ of the network can be calculated as

$$\begin{aligned}P(k) &= \frac{\partial P\left[k_j(t) < k\right]}{\partial k} \\ &= \frac{(1 + p_c)\overline{E}}{E_j} m_h{}^{(1+p_c)\overline{E}/E_j} k^{-[(1+p_c)\overline{E}/E_j + 1]}.\end{aligned} \tag{17}$$

It is obvious that the network degree distribution $P(k)$ of heterogeneous scale-free network model is in line with the general form of power-law distribution $P(k) \propto k^{-\gamma}$ and the power-law exponent $\gamma = (1 + p_c)\overline{E}/E_j + 1$. When $p_c = 1$, the entire network consists of cluster heads, which means the network is equivalent to a homogeneous scale-free network. At this point, we can get the degree distribution of homogeneous scale-free network

$$P(k) = \frac{\partial P\left[k_j(t) < k\right]}{\partial k} = \frac{2\overline{E}}{E_j} m_h{}^{2\overline{E}/E_j} k^{-[2\overline{E}/E_j + 1]}. \tag{18}$$

If we set $\overline{E}/E_j = 1$, $P(k) = 2m_h k^{-3}$ is totally the same as the general degree distribution $P(k) = 2mk^{-3}$ of B-A scale-free model [28]. Considering the impacts of energy factor on $P(k)$, (17) can be expressed as

$$\begin{aligned}P(k) &= \int_{E_{\min}}^{E_{\max}} P\left(k, E_j\right)\rho\left(E_j\right)dE_j \\ &= \int_{E_{\min}}^{E_{\max}} \frac{(1 + p_c)\overline{E}}{E_j} m_h{}^{(1+p_c)\overline{E}/E_j} k^{-[(1+p_c)\overline{E}/E_j + 1]}\rho\left(E_j\right)dE_j.\end{aligned} \tag{19}$$

According to the configurations in Section 4.4, energy E_i complies with truncated normal distribution $N(2, 1)$ and the valid interval $[E_{\min}, E_{\max}]$ for E_i is $[0, 4]$; we can easily get $\rho(E_j) = (1/0.9545\sqrt{2\pi})\exp[-(1/2)(x - 2)^2]$ and $\overline{E} = 2$. When $P_c = 1$, degree distribution of homogeneous scale-free network $P(k) \approx 1.25x^{-2.23}$ according to (18). When $P_c = 0.2$, degree distribution of heterogeneous scale-free network $P(k) \approx 0.86x^{-4.22}$. As is shown in Figure 4, the general trends of simulation curves and theoretical curves are similar. As in our theoretical analysis the basic assumption is that the network scale is large enough which our simulation can hardly satisfy, there is a deviation between simulation results and theoretical results. From the above analysis, the scale-free feature of our models has been validated by proving their degree distributions following a power-law distribution.

6. Invulnerability Analysis of WSNs

In this section, we analyze the invulnerability of various WSNs topologies with respect to cascading failures. In order to make the cascading process more active, we extend the network size. The total numbers of nodes and links increase to 300 and 600, respectively. Other configurations are the same as in Section 4.5. The initial status of node $x_i(0)$ follows truncated normal distribution $N(0.5, 0.1)$ over the effective interval $(0, 1)$. Here we design three attack schemes as trigger conditions for cascading process of WSNs.

(1) Random Attack. Select a node randomly from initial network and impose interference R.

(2) Max-Degree Attack. Select the node with highest degree from initial network and impose interference R.

(3) Max-Status Attack. Select the node with highest status from initial network and impose interference R.

Before analysis of invulnerability, we need to define a metric to evaluate the invulnerability of WSNs towards cascading failures at first. In our CML-based cascading model, the network is represented by graph $G = (V, E)$; then we can

get the definition of the connected subgraph and maximum connected subgraph.

Definition 1. For the network subgraph $G' = (V', E')$, if $V' \subseteq V$ and any two of the nodes in V' can maintain at least one effective path, then G' is one of the connected subgraphs of G.

Definition 2. For the network graph $G = (V, E)$ consisting of ω connected subgraphs which are $G'_1 = (V'_1, E'_1)$ and $G'_2 = (V'_2, E'_2), \ldots, G'_\omega = (V'_\omega, E'_\omega)$, if $V' \in \{V'_1, V'_2, \ldots, V'_\omega\}$ and $|V'| = \max\{|V'_1|, |V'_2|, \ldots, |V'_\omega|\}$, then $G' = (V', E')$ is the maximum connected subgraph of G.

$|V'|$ is the collection size of V'. Referencing the definition of availability of WSNs in [4], only the maximum connected subgraph $G' = (V', E')$ can be still functioning after removal of failure nodes or links. Therefore, we can reasonably consider $|V'|$ as the number of survival nodes. Considering the dynamic changes of WSN topology over time, we define that $|V'(t)|$ is the number of survival nodes at time t. As far as the cascading process of WSNs is concerned, initial network $G = (V, E)$ is well connected. If cascading failures occurred, the number of failure nodes is $|V| - |V'(t)|$ at time t. Through normalization processing, we can get the failure size

$$L(t) = \frac{|V| - \left|V'(t)\right|}{|V|}. \tag{20}$$

When no new nodes turn into failure, we can get the final failure size L. Obviously, the final failure size L can perfectly represent the damage level of cascading failures. Therefore, we select L as the invulnerability metric for cascading failures of WSNs.

6.1. Impacts of Interference R on WSNs Invulnerability. From Figures 5–7, it can be easily observed that, with the increase of interference R, the final failure size L is expanding. But the network performances are quite different when facing various types of attacks.

From Figure 5, when facing a random attack, the invulnerability of two scale-free networks is much stronger than that of the random network and the small-world network. By observing L-R relation curve, there is a cascading threshold R_c. In the case that $R \leq R_c$, imposing interference R has little impacts on final failure size L. But once $R > R_c$, a small change of R could make a great impact on L. For random network and small-world network, when $R > R_c = 1.2$, the cascading failures start to spread to the entire network rapidly. But for scale-free network, only when $R > R_c = 1.7$, the cascading process can be triggered. According to our CML-based cascading model, since a node with a higher degree means it having more neighboring nodes to share its load, its status would be more stable due to load-diversion effect. In other words, these high-degree nodes can be deemed as the "roadblocks" to stop spread of cascading failures. In scale-free networks, most of the sensor nodes have the minimum degree m_h and these "marginal" nodes always connect with "central"

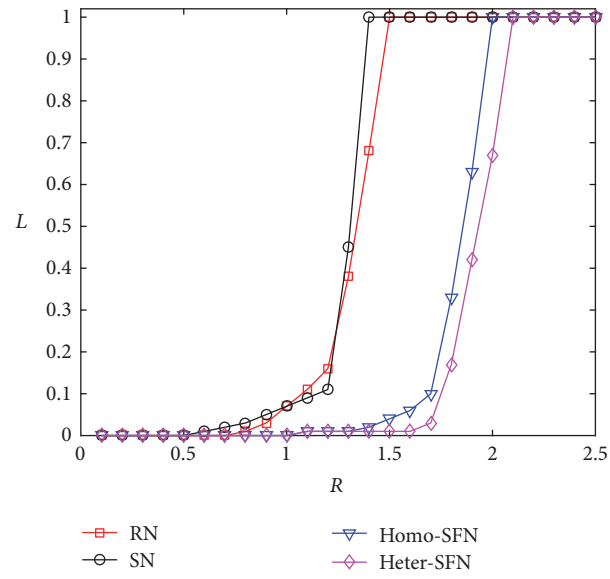


Figure 5: L-R relation curve under random attack ($\varepsilon = 0.6$).

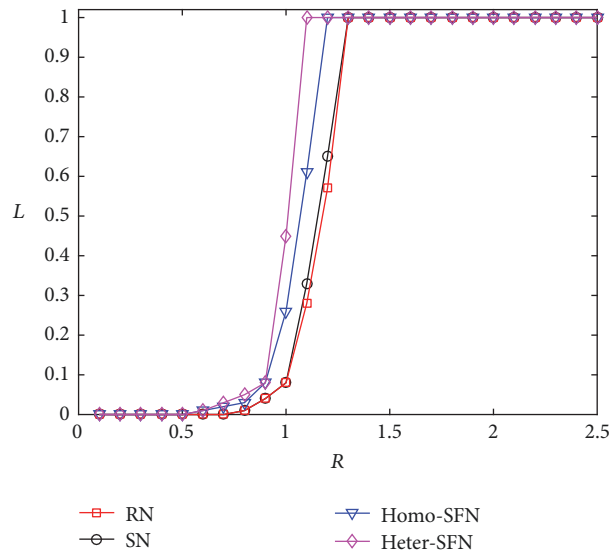


Figure 6: L-R relation curve under max-degree attack ($\varepsilon = 0.6$).

nodes (i.e., high-degree nodes) in a clustering way. When facing random attack, in most cases these marginal nodes would be attacked and then influence their neighbors by delivering failure status $x(i)$. When reaching central nodes, as the central nodes have stronger tolerance, then this spreading process will cease. This clearly explains why scale-free networks can have stronger invulnerability when facing random attack. Similarly, as heterogeneous scale-free network is more likely to generate high-degree nodes than homogeneous scale-free network, its invulnerability is slightly better.

From Figure 6, opposite to the case of random attack, random network and small-world network have stronger invulnerability than scale-free networks when facing max-degree attack. In fact, we can easily find that in the random

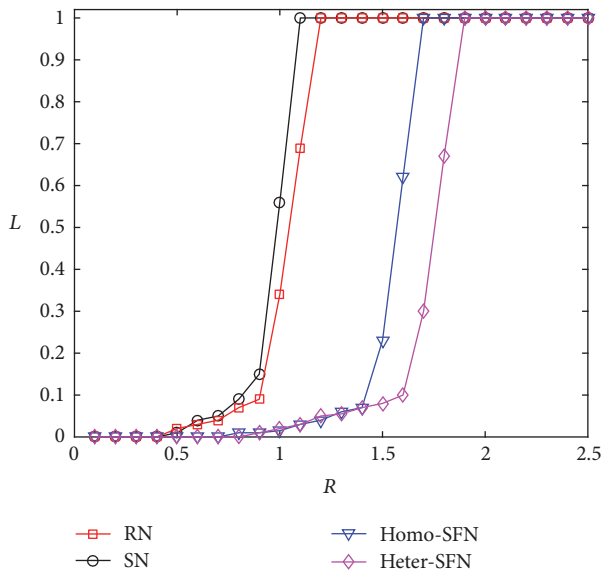


Figure 7: L-R relation curve under max-status attack ($\varepsilon = 0.6$).

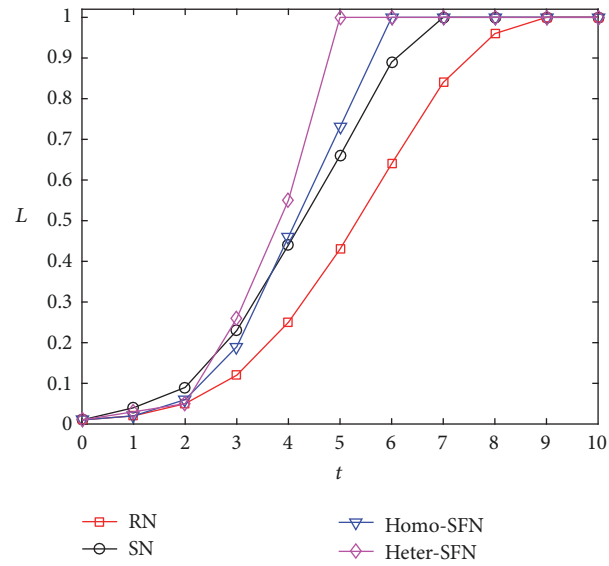


Figure 8: Cascading process under random attack ($\varepsilon = 0.6$).

network and the small-world network R_c values under max-degree attack slightly decrease compared to the values under random attack. As in these two kinds of networks the degree of nodes is distributed around the average degree $\langle k \rangle$, the attack objects selected by two attack schemes are not so different. But for scale-free networks, when facing a max-degree attack, as the node with highest degree is attacked, marginal nodes that connect with it would be influenced by its failure status and are highly likely to fall into failure due to the low-degree reason. Since the number of these marginal nodes is quite large, their failure status will spread rapidly and finally paralyze the entire network.

As is shown in Figure 7, the performance of various topologies when facing a max-status attack is similar to that under random attack, but the threshold R_c has been lowered by 0.4. Since the initial status of nodes $x_i(0)$ in the network follows a truncated normal distribution $N(0.5, 0, 1)$, in random attack scheme and attack max-status scheme the status of attack objects is always around 0.5 and 0.9, respectively. Therefore, compared with random attack scheme, the cascading process will be triggered much earlier by imposing R in max-status attack scheme.

6.2. Cascading Process of WSNs under Various Attack Schemes. According to the simulation results in the last subsection, we can easily get that the entire network would turn into failure when $\varepsilon = 0.6$ and $R = 2$. Therefore, in this subsection we adopt the same configurations to investigate the cascading process of WSNs under various attack schemes.

As is shown in Figure 8, when facing a random attack, the spread of cascading failures in heterogeneous scale-free network is the fastest, followed by homogeneous scale-free network and small-world network. Last is the random network. For heterogeneous scale-free network, the entire network will be collapsed over 4 time steps. By observing the topology structure of the heterogeneous scale-free network, we can discover that cluster members connect with cluster heads due to clustering mechanism and the backbone network consisting of cluster heads is well connected, making the average path length of the entire network quite short. Thus, in heterogeneous scale-free network, the cascading process always follows the following order: cluster member $\rightarrow$ cluster head $\rightarrow$ cluster head $\rightarrow$ cluster member. For homogeneous scale-free network, as the connectivity of the backbone network consisting of high-degree nodes is lower compared with scale-free heterogeneous network, its average path length tends be longer, thus making the failures spread slower. For random network and small-world network, the average path length is longer compared with scale-free networks due to their flat structures, helping the failure spread slow down. Due to the existence of shortcuts, the average path length in small-world network is much shorter than in random network, thus facilitating the spread of cascading failures.

From Figure 9, we can easily find that the max-degree attack scheme will significantly accelerate the cascading process, especially for scale-free networks. For instance, for heterogeneous scale-free network, the network will be entirely paralyzed after 3 time steps when facing a max-degree attack. Obviously, choosing the node with maximum degree will help the node influence adjacent nodes as many as possible and thus speed up the cascading process.

As is shown in Figure 10, the cascading process under max-status attack scheme is quite similar to that under random attack scheme. As analyzed in Section 6.1, when attack object is low-degree nodes, the cascading process is always slower as the interference R needs to go through multiple relays to reach every corner of the network. But if the attack object is central nodes with high-degree, the interference can be spread over the entire network in a few steps. Therefore, the spreading speed of cascading failures is closely related to the degree of attack objects. This also

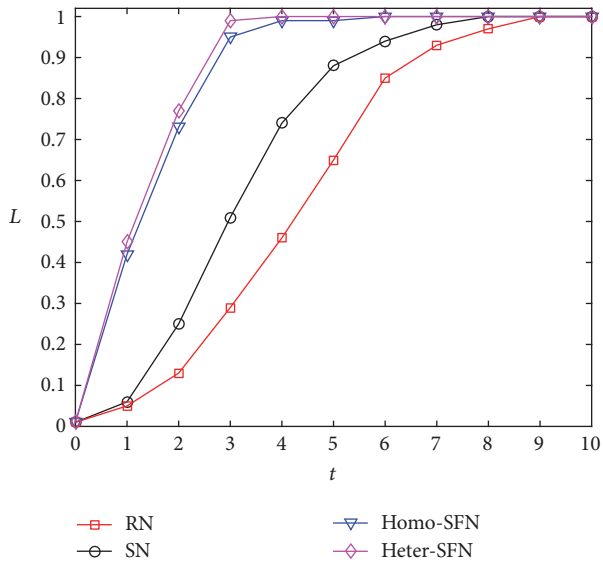


Figure 9: Cascading process under max-degree attack ($\varepsilon = 0.6$).

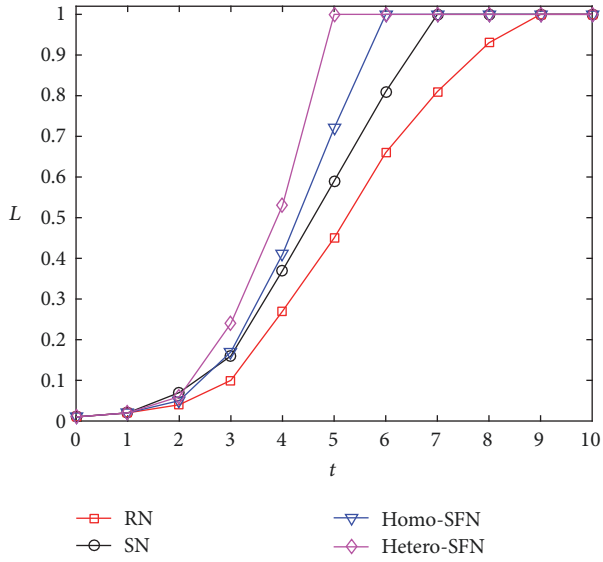


Figure 10: Cascading process under max-status attack ($\varepsilon = 0.6$).

explains why max-degree attack can significantly accelerate the spread of cascading failures. But for max-status attack scheme, the selection of attack object is only related to its initial status $x_i(0)$, but unrelated to its degree. Thus, its cascading process is similar to random attack scheme.

6.3. Impacts of Coupled Coefficient ε on WSNs Invulnerability. From Figures 11–13, it can be easily seen that, with the increase of coupled coefficient ε, the network invulnerability is gradually degrading. Obviously, when $\varepsilon = 0$, the sensor nodes work independently; nodes' failure behavior cannot influence their adjacent nodes. With the increase of coupled coefficient ε, the association among nodes is becoming closer, making the network featured by "injure one and you injure them all." Similar to L-R relation curve, there is a coupled threshold ε_c. When $\varepsilon > \varepsilon_c$, the cascading process begins.

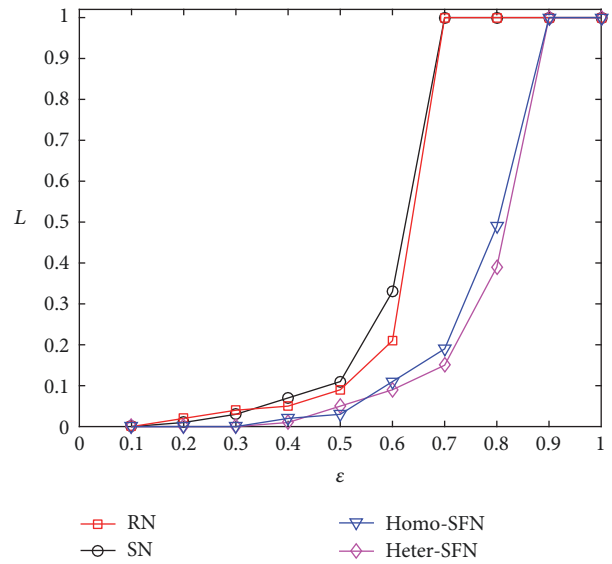


Figure 11: L-ε relation curve under random attack ($R = 1$).

From Figure 11, under random attack, scale-free networks have higher coupled threshold ε_c, which makes them survive in tight-coupling cases. This is because, when facing a random attack, in scale-free network low-degree nodes are highly likely to be attack objects and the impacts brought by the failures of these nodes would be stopped by the "roadblock" (i.e., high-degree nodes) due to the load-diversion effect. For random network and small-world network, since the degree distributions of these networks tend to be more uniform, cascading failures would be much easier to spread to the entire network.

As is shown in Figure 12, under max-degree attack, the tolerance of scale-free networks declines significantly. When $\varepsilon > \varepsilon_c = 0.4$, the networks would be collapsed soon. As in the max-degree attack scheme, the attack object would be the highest-degree nodes; the failure behavior of these nodes would make the marginal nodes connected with them turn into failure immediately. Since the number of these marginal nodes is relatively huge, their failures will spread rapidly and finally paralyze the entire network. But for random network and small-world network the degree difference of attack objects between random attack and max-degree attack is not as large as in scale-free networks; coupled thresholds ε_c under max-degree attack only slightly drop compared to under random attack.

As is shown in Figure 13, the network invulnerability under max-status attack scheme is similar to that under random attack scheme. The only difference is that the coupled threshold ε_c is lowered by 0.1. Under max-status attack scheme, the attack objects would be the nodes with highest status value $x_i(0)$. According to our CML-based cascading model, under this scheme the impacts that adjacent nodes would suffer could be more serious, thus enhancing their risks of cascading failures.

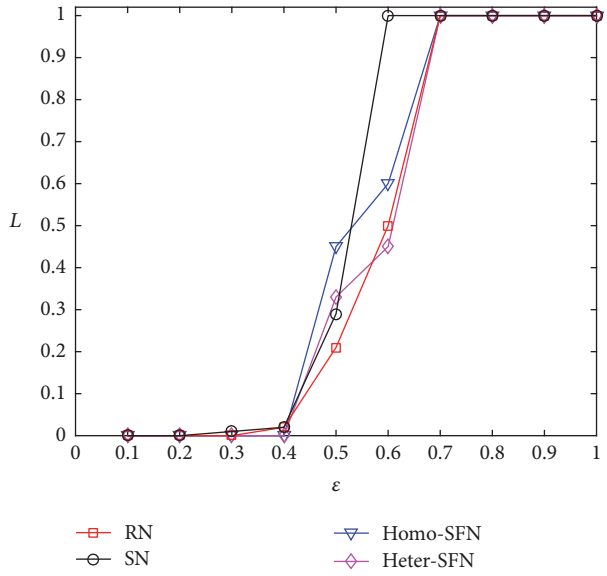


Figure 12: L-ε relation curve under max-degree attack ($R = 1$).

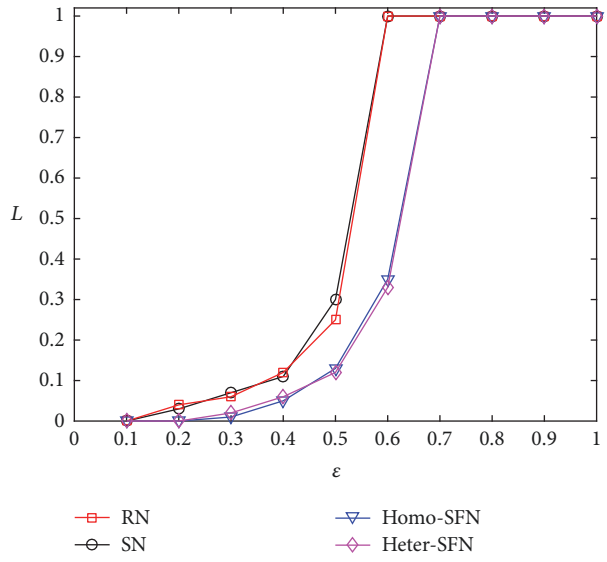


Figure 13: L-ε relation curve under max-status attack ($R = 1$).

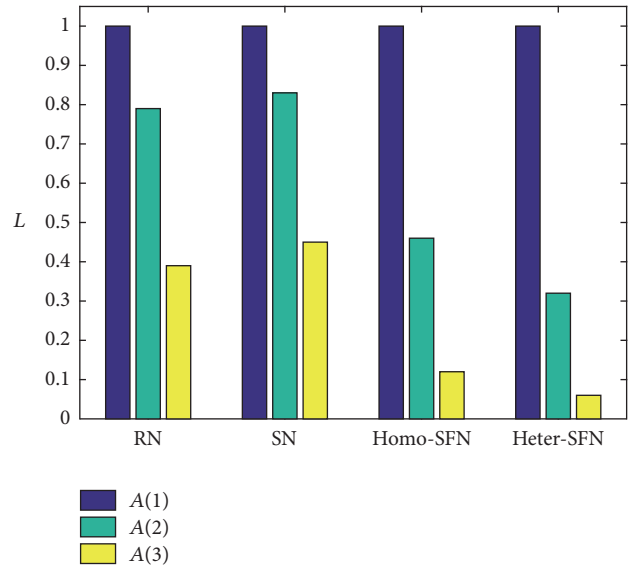


Figure 14: Failure size L with varying types of matrix A under random attack ($R = 2$, $\varepsilon = 0.6$).

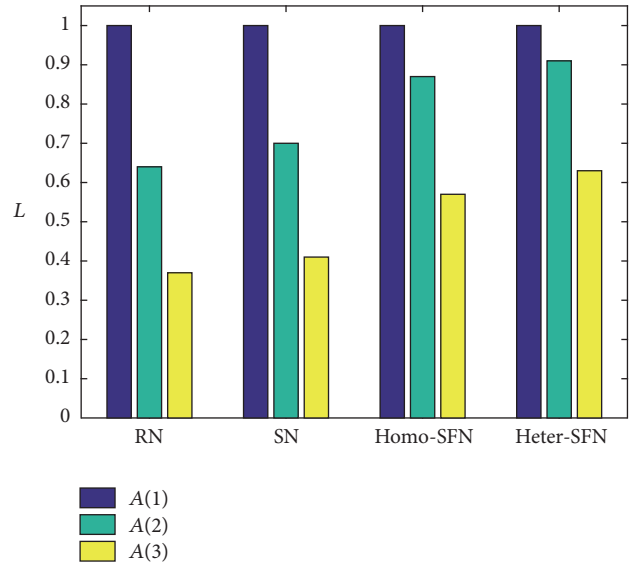


Figure 15: Failure size L with varying types of matrix A under max-degree attack ($R = 2$, $\varepsilon = 0.6$).

6.4. Impacts of Adjacent Matrix A on WSNs Invulnerability. In our CML model, the network topology is represented by adjacent matrix $A = [a_{ij}(t)]_{N\times N}$. Aiming to fully investigate the impacts of network topology on invulnerability, we design three types of matrix A for each network topology. For random network and small-world network, three types of matrix A are shown in Table 1. For homogeneous scale-free network and heterogeneous scale-free network, three types of matrix A are presented in Table 2. Other parameters remain the same as those in Section 4.5.

From Figures 14–16, we can easily observe that, even for the same type of network topology, the difference of matrix A could result in an evident difference in terms of network invulnerability. Moreover, the network failure size L would be significantly reduced when the matrix type is switched from $A(1)$ to $A(3)$. Taking the random network under the random attack as an example, when the network topology is constructed according to the matrix $A(1)$, the failure size is 100%, which means the entire network is paralyzed due to the cascading failures. When the matrix $A(2)$ is used to generate the random network topology, the failure size L decreases to 79%. By using $A(3)$, the failure size L can be further reduced to 39%. It is easy to understand that, for the network topology generated by the matrix $A(1)$, its average degree $\langle k\rangle = 2$, which means that the average number of neighbors owned by a sensor node in this topology is two; at this point, the load-diversion effect is not so obvious. When using the matrix $A(2)$ to generate the network topology, the average degree $\langle k\rangle$

Table 1: Types of matrix A for random network and small-world network.

Matrix types	Average degree $\langle k \rangle$	Number of retained links M_d	Number of sensor nodes N
$A(1)$	2	200	200
$A(2)$	3	300	200
$A(3)$	4	400	200

Table 2: Types of matrix A for homogeneous scale-free network and heterogeneous scale-free network.

Matrix types	Average degree $\langle k \rangle$	Number of new links at each time step M_h	Number of sensor nodes N
$A(1)$	2	2	200
$A(2)$	3	3	200
$A(3)$	4	4	200

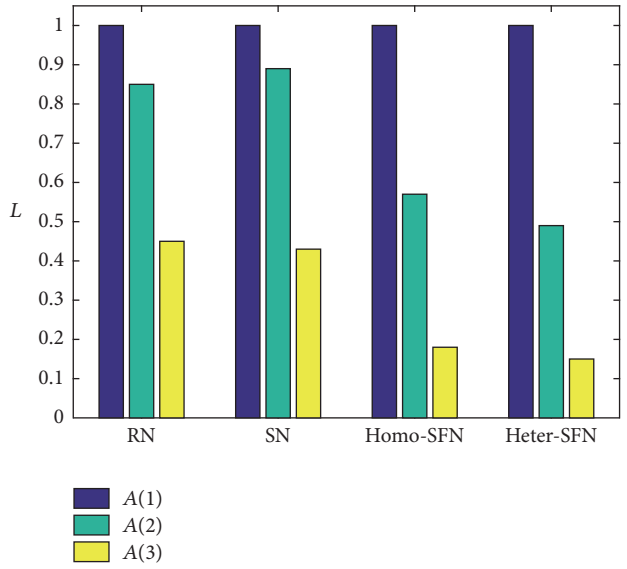


Figure 16: Failure size L with varying types of matrix A under max-status attack ($R = 2$, $\varepsilon = 0.6$).

increases to 3, the sensor node in this topology would have more neighbors to share its load compared to the case of $A(1)$, and its resilience to cascading failures tends to be stronger; thus the failure size L can be reduced. In the same way, the failure size L can be further reduced when using $A(3)$. This tells us that we can make sensor nodes have more neighbors in order to prevent cascading failures. To achieve this, we can increase the transmission radius of sensor nodes, but this way would consume more energy.

7. Conclusions

In this paper, we introduce a cascading model of WSNs based on CML and propose four network topology construction methods considering the limited transmission radius feature of WSNs. Then we analyze the invulnerability of various network topologies under three different attack schemes. The results show the following.

(1) The increase of interference R and coupled coefficient ε will increase the risks of cascading failures. There are cascading thresholds R_c and ε_c; when $R > R_c$ or $\varepsilon > \varepsilon_c$, the cascading process begins.

(2) When facing a random attack, the network with higher degree heterogeneity would be more invulnerable. Thus, the heterogeneous scale-free network performs the best, homogeneous scale-free network comes second, and random network and small-world network come last. When facing a max-degree attack, the network with more uniform degree distribution tends to perform better. Thus, the invulnerability of random network and small-world network is better than scale-free networks. The network performance under max-status attack is similar to that under random attack. But compared to random attack, max-status attack can make the cascading failures occur with imposing less interference R or in the case with low coupled coefficient ε.

(3) Regardless of which attack scheme is selected, the spreading speed of cascading failures in heterogeneous scale-free network is the fastest, followed by homogeneous scale-free network and small-world network. Last is the random network. Compared with other schemes, max-degree attack scheme could significantly accelerate the cascading process.

(4) Increasing the average degree $\langle k \rangle$ can improve the network resistance to cascading failures due to the load-diversion effect.

In the future work, we would like to research how to optimize the network in order to improve its invulnerability towards cascading failures. Given that the degree distribution is closely related to the network performance in terms of cascading failures, designing a topology construction method with reasonable degree distribution will be a meaningful issue. Moreover, dynamical entropy is an effective metric to indicate the variation speed in dynamical topology of networks [29, 30]. To have a better understanding of the inherent laws of cascading process in WSNs, it would also be worth discussing the cascading invulnerability of WSNs using the dynamical entropy.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work has been financially supported by the National Natural Science Foundation of China (61571336).

References

[1] M. Hammoudeh and R. Newman, "Adaptive routing in wireless sensor networks: QoS optimisation for enhanced application performance," *Information Fusion*, vol. 22, pp. 3–15, 2015.

[2] M. Younis, I. F. Senturk, K. Akkaya, S. Lee, and F. Senel, "Topology management techniques for tolerating node failures in wireless sensor networks: a survey," *Computer Networks*, vol. 58, no. 1, pp. 254–283, 2014.

[3] M. A. Mahmood, W. K. G. Seah, and I. Welch, "Reliability in wireless sensor networks: a survey and challenges ahead," *Computer Networks*, vol. 79, pp. 166–187, 2015.

[4] H. Bagci, I. Korpeoglu, and A. Yazici, "A distributed fault-tolerant topology control algorithm for heterogeneous wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 914–923, 2015.

[5] X. Fu and W. Li, "Cascading failures of wireless sensor networks," in *Proceedings of the 11th IEEE International Conference on Networking, Sensing and Control, ICNSC 2014*, pp. 631–636, USA, April 2014.

[6] X. Hu, W. Li, and X. Fu, "Analysis of Cascading Failure Based on Wireless Sensor Networks," in *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, SMC 2015*, pp. 1279–1284, Hong Kong, October 2015.

[7] N. Vasegh, "Spatiotemporal and synchronous chaos in accumulated coupled map lattice," *Nonlinear Dynamics*, vol. 89, no. 2, pp. 1089–1097, 2017.

[8] K. Kaneko, "Coupled map lattice," in *Chaos, order, and patterns (Lake Como, 1990)*, vol. 280 of *NATO Adv. Sci. Inst. Ser. B Phys.*, pp. 237–247, Plenum, New York, 1991.

[9] H. Leung, G. Hennessey, and A. Drosopoulos, "Signal detection using the radial basis function coupled map lattice," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 11, no. 5, pp. 1133–1151, 2000.

[10] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice," *Information Sciences*, vol. 273, pp. 329–351, 2014.

[11] K. Konishi, H. Kokame, and K. Hirata, "Decentralized delayed-feedback control of an optimal velocity traffic model," *The European Physical Journal B*, vol. 15, no. 4, pp. 715–722, 2000.

[12] V. Kohar, S. Kia, B. Kia, J. F. Lindner, and W. L. Ditto, "Role of network topology in noise reduction using coupled dynamics," *Nonlinear Dynamics*, vol. 84, no. 3, pp. 1805–1812, 2016.

[13] X. F. Wang and J. Xu, "Cascading failures in coupled map lattices," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 70, no. 5, Article ID 056113, 2004.

[14] D. Cui, Z. Gao, and X. Zhao, "Cascades in small-world modular networks with CML'S method," *Modern Physics Letters B*, vol. 21, no. 30, pp. 2055–2062, 2007.

[15] C. Di, G. Zi-You, and Z. Jian-Feng, "Tolerance of edge cascades with coupled map lattices methods," *Chinese Physics B*, vol. 18, no. 3, pp. 992–996, 2009.

[16] J. Xu and X. F. Wang, "Cascading failures in scale-free coupled map lattices," *Physica A: Statistical Mechanics and its Applications*, vol. 349, no. 3-4, pp. 685–692, 2005.

[17] H. Zhu, H. Luo, H. Peng, L. Li, and Q. Luo, "Complex networks-based energy-efficient evolution model for wireless sensor networks," *Chaos, Solitons & Fractals*, vol. 41, no. 4, pp. 1828–1835, 2009.

[18] X. Luo, H. Yu, and X. Wang, "Energy-aware topology evolution model with link and node deletion in wireless sensor networks," *Mathematical Problems in Engineering*, vol. 2012, Article ID 281465, 2012.

[19] A. Helmy, "Small worlds in wireless networks," *IEEE Communications Letters*, vol. 7, no. 10, pp. 490–492, 2003.

[20] X. Fu, W. Li, and G. Fortino, "Empowering the invulnerability of wireless sensor networks through super wires and super nodes," in *Proceedings of the 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing, CCGrid 2013*, pp. 561–568, Netherlands, May 2013.

[21] Y. K. Joshi and M. Younis, "Restoring connectivity in a resource constrained WSN," *Journal of Network and Computer Applications*, vol. 66, pp. 151–165, 2016.

[22] X. Han, X. Cao, E. L. Lloyd, and C.-C. Shen, "Fault-tolerant relay node placement in heterogeneous wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 5, pp. 643–656, 2010.

[23] S. Lin, J. Zhang, G. Zhou, L. Gu, J. A. Stankovic, and T. He, "ATPC: adaptive transmission power control for wireless sensor networks," in *Proceedings of the Proceeding of the 4th International Conference on Embedded Networked Sensor Systems (SenSys '06)*, pp. 223–236, New York, NY, USA, November 2006.

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

[25] C. Li, S. Li, X. Liao, and J. Yu, "Synchronization in coupled map lattices with small-world delayed interactions," *Physica A: Statistical Mechanics and its Applications*, vol. 335, no. 3-4, pp. 365–370, 2004.

[26] P. Erdös and A. Rényi, "On the evolution of random graphs," *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, vol. 5, pp. 17–61, 1960.

[27] M. E. Newman and D. J. Watts, "Renormalization group analysis of the small-world network model," *Physics Letters A*, vol. 263, no. 4-6, pp. 341–346, 1999.

[28] A.-L. Barabási, R. Albert, and H. Jeong, "Mean-field theory for scale-free random networks," *Physica A: Statistical Mechanics and its Applications*, vol. 272, no. 1, pp. 173–187, 1999.

[29] Y.-Q. Zhang, X.-Y. Wang, L.-Y. Liu, Y. He, and J. Liu, "Spatiotemporal chaos of fractional order logistic equation in nonlinear coupled lattices," *Communications in Nonlinear Science and Numerical Simulation*, vol. 52, pp. 52–61, 2017.

[30] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Applied Soft Computing*, vol. 26, pp. 10–20, 2015.