Journal of Computers Vol. 28, No. 2, 2017, pp. 119-133
doi:10.3966/199115592017042802009

Scale-Free Topology Evolution Model Based on Invulnerability Optimization for Wireless Sensor Networks

Chun-Meng Hu, San-Yang Liu, and Zhao-Hui Zhang

School of Mathematics and Statistics, Xidian University, Xi'an 710126, Shaanxi, China
hcm_19920518@163.com, liusanyang@126.com, zhangzhaohui005@163.com

Received 19 April 2016; Revised 10 May 2016; Accepted 12 August 2016

Abstract. Topologies with energy-efficient and strong invulnerability has become an important issue in the development of Wireless Sensor Networks (WSNs). In this paper, we propose a Poisson-growth model based on regulated attractiveness function to build a WSN with scale-free topology, named PSFBRA. In the model, adjustable parameters are introduced for balancing connectivity and energy consumption in WSNs. Then a mathematical optimization model which based on the endurable probability and the topology structure entropy is established. Through analyzing the values of the topologic parameters, the optimal scaling exponent of the PSFBRA topology is obtained. Finally, simulation results show that PSFBRA topology is more in line with the practical application of WSNs, maintains the fault tolerance of scale-free network under random failures, improves the network invulnerability under intentional attacks and effectively enhances the communication efficiency.

Keywords: endurable probability, invulnerability, topology evolution, topology structure entropy, wireless sensor network

1 Introduction

Wireless sensor networks have gained enormous attention for their wide range of applications such as environmental monitoring, military surveillance, health care, and disaster management [1]. However, WSNs are vulnerable to energy depletion because of battery drain. In addition, natural disaster and deliberate attack will lead to WSNs being collapsed easily. Therefore, constructing the topology which has good communication quality, high energy utilization efficiency and strong invulnerability is one of the most important challenges for WSNs [2-5].

It is important that WSNs are able to continue functioning in the face of node failure or intrusion, a feature known as invulnerability [6]. Hashmi presented an analytical model of cluster reliability in cluster-based WSNs [7]. When the cluster head dies, backup cluster head node takes over the responsibility and continues to work as a new cluster head and facilitates the cluster reliability. Fu, Li and Giancarlo used two layout schemes based on super wires and super nodes for enhancing network invulnerability [8]. Both stationary and mobile relay nodes are used. Through the increase of the number of relay nodes, the robust connectivity and the balanced traffic load can be ensured [9]. A novel energy efficiency routing with node compromised resistance (EENC) based on Ant Colony Optimization is proposed, which has high performance in energy-efficient and combating inside attack from the compromised nodes[10]. An energy efficient failures-tolerant topology is constructed [11]. By building k-connectivity network, network connectivity can be still maintained under k-coverage strategy even if some nodes fail. Although the methods mentioned above which use redundancy mechanism to construct the survivability topology have many advantages, the increase of the use of hardware and software reduces the performance of the network. Moreover, a few studies analyze invulnerability from the perspective of topological evolution of scale-free network.

The discovery of scale-free networks characteristic is an important breakthrough in the development of complex network. Since scale-free networks can better exhibit the essential features of the real world and provide a reasonable model for us to construct a robust topology for WSNs. Considering the major constraints of WSNs is the limited energy sources, Zhu and Luo had proposed two scale-free models for wireless sensor networks, named energy-aware evolution model (EAEM) and energy-balanced evolution model (EBEM) which can organize the networks in an energy-efficient way [12]. Two topology evolutions were executed among cluster heads based on scale-free theory and residual energy, node saturation and communication radius were considered in the processes of topology evolution, which made the scale-free topology has a good robustness against energy exhaustion, random failures [13]. Wang et al. proposed a scale-free model (NLL-E) to enhance robust and energy efficiency in WSNs, using a link compensation mechanism [14]. Then, Qi, Wang and Zheng proposed a network evolution model DEDA on the basis of node degrees, residual energy and transmission distance, which had better invulnerability under deliberate attacks, but this model did not keep the power-law strictly [15]. An indicator of measuring the topological heterogeneity is obtained by utilizing the topology structure entropy [16-17]. But they did not take into account the scaling exponent's influence on the topological robustness. Further, there are more constraints being added on the scale-free topology to make it according with the characteristics of WSNs in varied applications [18-20], but these scale-free topologies don't optimize the capability of random failures and intentional failures simultaneously. So how to design and optimize the scale-free topology which have the strong capability of random failures and intentional failures simultaneously is particularly important.

Given all these considerations, an invulnerability optimization model of the Poisson-growth scale-free topology based on the attractiveness function is proposed. The topology construction is divided into two phases. In the first phase, a scaling exponent adjustable evolution model is proposed, and following conditions are considered when we design the evolution model: (1) We employ the homogeneous Poisson process to simulate the generation of network, which is more close to practical WSNs. (2) Considering the node localization, links between nodes depend on the transmission range. Therefore, nodes beyond local world cannot be directly connected. (3) Here, the attractiveness of the node is not a constant quantity. The residual energy and the distance are used to adjust the attractiveness of nodes and change the priority of connection to the new coming node. Nodes with greater e attractiveness have higher probability to be connected. (4) Adjustable parameters are introduced into our model. They can adjust the topology structure of the WSNs to make a balance between high connectivity and energy consumption of nodes. In the second phase, the endurable probability and the topology structure entropy are introduced to make quantitative measure the topological invulnerability. Through formulating and solving the multi-goals mathematic optimization model, the optimal parameters of the PSFBRA model are derived.

The remainder of this paper is organized as follows: Section 2 reviews the related work of scale-free network. In section 3, we show how to construct scale-free model based on the regulated attractiveness function, PSFBRA, and make a dynamic characteristic analysis. In section 4, constructs the optimized mathematical model about these properties of invulnerability under random failures and intentional attacks, then the effect of degree distribution characteristics on topological invulnerability is discussed in detail. In section 5, the simulation results are given and compared with the existing models. Finally, section 6 gives the conclusions of this paper.

2 Typical Scale-Free Network Models

2.1 The BA Evolving Network Model

Barabasi and Albert have proposed a canonical BA scale-free network model [21]. By including two evolving mechanisms, i.e., network growth and preferential attachment, the BA model makes a scale-free network with scaling exponent $\gamma = 3$.

The network generation algorithm of the BA scale-free model is as follows:

Step 1. Growth. Starting with a small number of m_0 nodes and l_0 edges. At every time step, we add a new node with $m\left(\le m_0\right)$ edges (that will be connected to the nodes already present in the network).

Step 2. Preferential attachment. When a new node comes into the network, it will choose the existing nodes to connect. We assume that the probability $\prod_i$ of a new node will be connected to node i depends on the connectivity k_i. And the formula of $\prod_i$ is

$$\prod_i = \frac{k_i}{\sum_j k_j} \quad \textbf{(1)}$$

where $\sum_j k_j$ is the total of the nodes' degree in the network.

2.2 The DMS Evolving Network Model

The DMS model is an extensional model of BA model proposed by Dorogovtsev, Mendes and Samukhin [22]. This linear increasing model introduces the concept of attractiveness. In other words, a new node will be connected to the existing node i depends on the degree and the attractiveness. The probability formula of preferential attachment is expressed as the follow:

$$\prod_i = \frac{k_i + A}{\sum_j (k_j + A)} \quad \textbf{(2)}$$

where A is the attractiveness of the node, and its value is a constant quantity. $\sum_j (k_j + A)$ is the sum of the other nodes' degrees and the attractiveness. According to the above probability formula to deduce further, we find that the network obeys the power-law distribution with the exponent of degree $\gamma(\gamma = 3 + A/m)$. When $a = 0$, the DMS model reverts to the BA evolving network model.

According to analysis on the evolutionary process of BA model and DMS model, we can find that there are some obvious diversities which make the scale-free model can't tally with the evolution process of the WSNs well. (1) The BA model and DMS model consider their generation rates of nodes as constant, but in practical situation, all nodes in WSNs keep changing over time. (2) In the BA model and DMS model, when a new node is coming into the network, it must know the connect information of every node. It's very hard for the sensor node limited by its communication ability and energy. (3) The degree of the node in the BA model has a close relation with the age of the node, the longer the age is, and the greater the degree will be. The "young" node will have a low degree or even become an isolated node. And the DMS model makes the link of node not only depends on the age of the node, but also relate to the node's attractiveness used to reflect some own characters. But the attractiveness is an equivalent constant, and once imported node into the network, its value won't be changed. This neither embodies the individual difference between the nodes in WSNs, nor dynamically adjusts along with the evolution of WSNs.

With these in mind, we propose a Poisson-growth model based on local-world and regulated attractiveness function, to build a WSNs scale-free topology with adjustable power exponent in the next chapter.

3 Topology Evolution Model Based on Scale-Free Networks

3.1 PSFBRA Topology Evolution Mechanism

Based on these issues, we then show a novel model based on the Poisson process, which also considers both the node degrees and attractiveness of node. The algorithm of PSFBRA model is as follows:

Step 1. Initialization. Starting with a small number $(m_0 - 1)$ of nodes and one sink node as a network, in which each node connects to its neighbors. And initial energy value E_0 enters into the existing network.

Step 2. Poisson-growth. At per unit time, newly added nodes are coming by the rate at λ according to the Poisson process. For each new node, $m(\le m_0)$ edges are connected to the existing nodes.

Step 3. Selection of the local world. At per unit time, select direct neighbor nodes of new node from the existing network as the local world Ω.

Step 4. Preferential attachment. When a new node comes into the network, it will choose m nodes in its local world Ω to form the new edges with a probability $\prod_{j\to i}$ proportional to their degree, residual energy and the distance with the new node, such that

$$\prod_{j\to i} = (\beta_1 \frac{k_i}{\sum_{l\in\Omega_j} k_l} + \beta_2 \frac{\varphi(E_i,L_i)}{\sum_{l\in\Omega_j} \varphi(E_l,L_l)}) \bullet P(d_{ij} < R) \tag{3}$$

The definition of attractiveness is:

$$\varphi(E_i,L_i) = \frac{E_i}{L_i} \tag{4}$$

where Ω_j is the local world of a new coming node j, d_{ij} is the Euclidean distance between nodes i and j, R is the maximum communication radius of nodes. E_i is the residue energy of sensor node i, L_i is the distance between the new node and the node i. β_1 is the connectivity adjustable parameter, β_2 is the attractiveness adjustable parameter and $\beta_1 + \beta_2 = 1$.

Considering the fact that every link to node i will consume some energy of node i, we simply suppose

$$E_i = E_0 - \alpha k_i \tag{5}$$

where E_0 is initial energy value, k_i is node degree. We define a as the ratio of k_i to energy consumption.

Step 5. Termination. When the number of nodes in the network reaches the desired network size, it stops growing.

We can find that from the Equation (4), the attractiveness of the sensor node is adjusted by E_i and L_i. When the residue energy of the node i is more and the distance to the new node is nearer, the value of $\varphi(E_i,L_i)$ is larger, and the probability of the node i is connected to the new node j is greater. So the growth of nodes degree in our mechanism is restricted and balanced.

3.2 Dynamic Characteristics Analysis of Topology Evolution Model

The network which has power law distribution can better exhibit the essential features of the real world. In the section, in order to find whether degree distribution of the proposed model has the characteristics of power law or not, we will make a dynamic characteristics analysis for evolution model PSFBRA with mean-field theory [23].

Theorem 1. The degree distribution of PSFBRA model follows a power law distribution.

Proof. Assuming that the nodes were distributed uniformly, when the new node j comes into the network, it will choose some nodes in its local world Ω_j to connect. So the probability that new node j connects with the node i in its local world is associated with the proportion of area value, this can be approximated as

$$P(d_{ij} < R) \approx \frac{\pi R^2/2}{\pi R_t^2} = \frac{R^2}{2R_t^2} \tag{6}$$

where R_t is the entire network radius at time t, R is the maximum communication radius of new added node j. And Equation (3) is approximate to Equation (7),

$$\begin{aligned} \prod_{j\to i} = (\beta_1 \frac{k_i}{\sum_{l\in\Omega_j} k_l} + \beta_2 \frac{\varphi(E_i,L_i)}{\sum_{l\in\Omega_j} \varphi(E_l,L_l)}) \bullet P(d_{ij} < R) &\approx \frac{R^2}{2R_t^2} \left(\beta_1 \frac{k_i}{N(\mathrm{t}) \frac{R^2}{2R_t^2} \langle k \rangle_t} + \beta_2 \frac{\varphi(E_i,L_i)}{\frac{R^2}{2R_t^2} \varphi\left(\langle E \rangle_j, \langle L \rangle_j\right) \langle k \rangle_t} \right) \\ &\approx \beta_1 \frac{k_i}{\lambda t \bullet 2m} + \beta_2 \frac{\varphi(E_i,L_i)}{\lambda t \bullet \varphi\left(\langle E \rangle_j, \langle L \rangle_j\right)} \end{aligned} \tag{7}$$

In the local world of each new node, we have $\sum_{l\in\Omega_j} k_l = N(\mathrm{t})\frac{R^2}{2R_t^2}\langle k\rangle_t$ and $\sum_{l\in\Omega_j}\varphi(E_l,L_l)$ $=\frac{R^2}{2R_t^2}\varphi\left(\langle E\rangle_j,\langle L\rangle_j\right)\langle k\rangle_t$, where $N(\mathrm{t})=\lambda t$ is the number of nodes in entire network at time t, λ is the distribution parameter of the Poisson process, $\langle k\rangle_t$ is the average degree of each node at time t. $\langle E\rangle_j$ and $\langle L\rangle_j$ are used to indicate the average of the residual energy and the average of the distance between new node and its local world nodes respectively.

By the mean-field theory, the increasing rate of k_{ij} satisfies the dynamical equation:

$$\frac{\partial k_{ij}(t)}{\partial t}\approx m\lambda[\Pi(k_i)],(t\gg t_i) \tag{8}$$

after substituting Equation (7) into Equation (8), we get:

$$\frac{\partial k_{ij}(t)}{\partial t}\approx m\lambda\left[\beta_1\frac{k_i}{\lambda t\bullet 2m}+\beta_2\frac{\varphi(E_i,L_i)}{\lambda t\bullet\varphi\left(\langle E\rangle_j,\langle L\rangle_j\right)}\right] \tag{9}$$

solving Equation (9), we get:

$$\frac{\partial k_{ij}(t)}{\partial t}\approx\frac{m}{t}\left[\beta_1\frac{k_i}{2m}+\beta_2\Phi(E_i,L_i)\right] \tag{10}$$

Using the method of separation of variables can be obtained：

$$k_i(t)=C\bullet t^{\frac{\beta_1}{2}}-2m\Phi(E_i,\mathrm{L}_i)\frac{\beta_2}{\beta_1} \tag{11}$$

where $\Phi(E_i,\mathrm{L}_i)=\frac{\varphi(E_i,L_i)}{\varphi\left(\langle E\rangle_j,\langle L\rangle_j\right)}$.

Because the initial condition $k_i(t_i)=m$, solving Equation (11) can obtain:

$$k_i(t)=\left[m+\frac{2m\beta_2}{\beta_1}\Phi(E_i,\mathrm{L}_i)\right](\frac{t}{t_i})^{\frac{\beta_1}{2}}-2m\Phi(E_i,\mathrm{L}_i)\frac{\beta_2}{\beta_1},(t\gg t_i) \tag{12}$$

As the node arrival process is a Poisson process with parameter λ, so t_i is satisfied with Γ distribution

$$p(t_i\le x)=1-e^{-\lambda x}\sum_{l=0}^{i-1}\frac{(\lambda x)^l}{l!} \tag{13}$$

According to Equation (12),

$$
\begin{aligned}
p\left(k_i\left(t\right)\ge k\right)&=p\left(t_i\le\left[\frac{m+\frac{2m\beta_2}{\beta_1}\Phi}{k+\frac{2m\beta_2}{\beta_1}\Phi}\right]^{\frac{2}{\beta_1}}t\right),\left(t\gg t_i\right)\\
&=1-e^{-\lambda\left[\frac{m+\frac{2m\beta_2}{\beta_1}\Phi}{k+\frac{2m\beta_2}{\beta_1}\Phi}\right]^{\frac{2}{\beta_1}}\bullet t}\bullet\sum_{l=0}^{i-1}\frac{\left(\lambda\left[\frac{m+\frac{2m\beta_2}{\beta_1}\Phi}{k+\frac{2m\beta_2}{\beta_1}\Phi}\right]^{\frac{2}{\beta_1}}t\right)^{l}}{l!}
\end{aligned}
\tag{14}
$$

The partial derivatives by k is

$$
p\left(k_i\left(t\right)=k\right)\approx\frac{\partial p\left(k_i\left(t\right)<k\right)}{\partial k}
\tag{15}
$$

substituting Equation (14) into Equation (15), we have

$$
p\left(k_i\left(t\right)=k\right)\approx\frac{2}{\beta_1}\frac{\lambda t\left(m+A\right)^{\frac{2}{\beta_1}}}{\left(k+A\right)^{\frac{2}{\beta_1}+1}}\bullet e^{-\lambda\left[\frac{m+A}{k+A}\right]^{\frac{2}{\beta_1}}\bullet t}\bullet\frac{\left\{\lambda\left[\frac{m+A}{k+A}\right]^{\frac{2}{\beta_1}}t\right\}^{i-1}}{\left(i-1\right)!}
\tag{16}
$$

where $A=2m\frac{\beta_2}{\beta_1}\Phi$, then the steady state distribution is

$$
\begin{aligned}
p\left(k\right)&=\lim_{t\to\infty}\frac{1}{E\left(N\left(t\right)\right)}\bullet\sum_{i=1}^{\infty}p\left(k_i\left(t\right)=k\right)\\
&=\frac{1}{\lambda t}\frac{2}{\beta_1}\frac{\lambda t\left(m+A\right)^{\frac{2}{\beta_1}}}{\left(k+A\right)^{\frac{2}{\beta_1}+1}}\bullet e^{-\lambda\left[\frac{m+A}{k+A}\right]^{\frac{2}{\beta_1}}\bullet t}\bullet\lim_{t\to\infty}\sum_{i=1}^{\infty}\frac{\left\{\lambda\left[\frac{m+A}{k+A}\right]^{\frac{2}{\beta_1}}t\right\}^{i-1}}{\left(i-1\right)!}\\
&=\frac{2}{\beta_1}\frac{\left(m+A\right)^{\frac{2}{\beta_1}}}{\left(k+A\right)^{\frac{2}{\beta_1}+1}}
\end{aligned}
\tag{17}
$$

According to Equation (17), the degree distribution derived by PSFBRA model is obeying the power-law distribution with scaling exponent $\gamma=\frac{2}{\beta_1}+1$. And the scaling exponent γ can be changed within $\left[3,+\infty\right)$ by adjusting the parameter β_1. When $\beta_1\to1$, we can get $p\left(k\right)\propto k^{-3}$, then the degree distribution of PSFBRA model is closing in on the BA scale-free topology which has the good capability of invulnerability against random failures. When $\beta_1\to0$, the degree distribution of PSFBRA model is closing in on the random topology which has the good capability of invulnerability against intentional attacks. So it can be concluded that the PSFBRA model has the power-law distribution that keeps its robustness under random failures, meanwhile, a strong invulnerability under intentional attacks can also be obtained by adjusting the parameter β_1.

4 Mathematical Optimization Model of PSFBRA

In this section, we analyze the effect of degree distribution characteristics on topological invulnerability under random failures or intentional attacks, then find the optimal value β_1. Finally, an optimal PSFBRA scale-free topology is derived which keeps the topological invulnerability under random failures and maximizes the topological invulnerability under intentional attacks.

4.1 Invulnerability Index under Random Failures

In this paper, quantitative analysis is done to the network invulnerability. We introduce p_r represents random failures threshold, which can be used as the invulnerability strength criterion of the scale-free topology. When the removal ratio of random nodes is more than p_r the topology will be disrupted. It was presented by Cohen et al. with percolation theory [24]. The critical threshold value

$$p_r = 1 - \frac{1}{\kappa_0 - 1} \tag{18}$$

where $\kappa_0 = \langle k_0{}^2 \rangle / \langle k_0 \rangle$ is calculated from the original distribution before the random failures.

Since the scale-free topology has a power-law distribution

$$p(k) = ck^{-\gamma}, (k = k_{\min}, k_{\min} + 1, \ldots, k_{\max}) \tag{19}$$

where $k_{\min}$ and $k_{\max}$ are the minimum degree and the maximum degree, respectively. The coefficient c is obtained from (20)

$$\int_{k_{\min}}^{\infty} p(k)dk = \int_{k_{\min}}^{\infty} ck^{-\gamma}dk = 1,\ c = (\gamma - 1)k_{\min}{}^{\gamma-1} \tag{20}$$

$$\int_{k_{\max}}^{\infty} p(k)dk = \int_{k_{\max}}^{\infty} ck^{-\gamma}dk = \frac{1}{N},\ k_{\max} \approx k_{\min}N^{1/(\gamma-1)} \tag{20}$$

According Equation (21) the average degree $\langle k_0 \rangle$ and its second moment $\langle k_0{}^2 \rangle$ for the power-law distribution $p(k)$ can be expressed by

$$\langle k_0 \rangle = \int_{k_{\min}}^{k_{\max}} kp(k)dk \approx \frac{\gamma - 1}{2 - \gamma} k_{\min} \left(N^{\frac{2-\gamma}{\gamma-1}} - 1 \right) \tag{21}$$

$$\langle k_0{}^2 \rangle = \int_{k_{\min}}^{k_{\max}} k^2 p(k)dk \approx \frac{\gamma - 1}{3 - \gamma} k_{\min}{}^2 \left(N^{\frac{3-\gamma}{\gamma-1}} - 1 \right) \tag{22}$$

With Equation (22), Equation (23), κ_0 can be expressed as follows:

$$\kappa_0 = \langle k_0{}^2 \rangle / \langle k_0 \rangle = k_{\min} \left(\frac{2-\gamma}{3-\gamma} \right) \frac{N^{\frac{3-\gamma}{\gamma-1}} - 1}{N^{\frac{2-\gamma}{\gamma-1}} - 1} \tag{23}$$

substituting Equation (24) into Equation (18)

$$p_r = 1 - \frac{1}{k_{\min} \left(\frac{2-\gamma}{3-\gamma} \right) \frac{N^{\frac{3-\gamma}{\gamma-1}} - 1}{N^{\frac{2-\gamma}{\gamma-1}} - 1} - 1} \tag{24}$$

Fig. 1 displays the relationship between random failures threshold p_r and γ for different N when $k_{\min}$ is defined. We can see that with the increase of γ, p_r decreases, while the threshold value p_r becomes greater with the increase of network scale N.

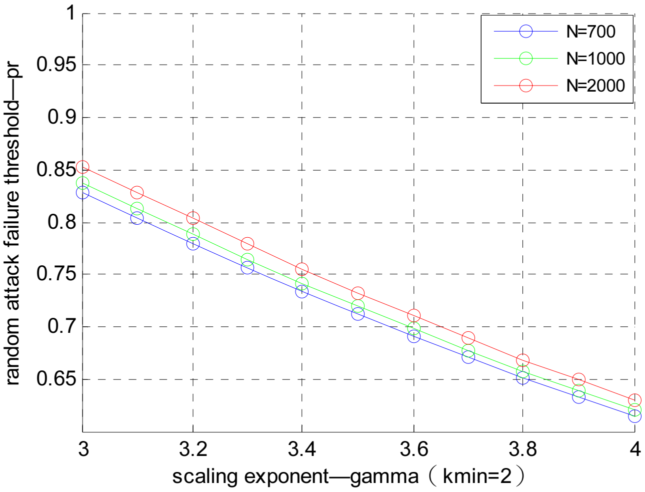

Fig. 1. The random failures threshold p_r

4.2 Invulnerability Index under Intentional Attacks

The heterogeneity of scale free topology leads to paralysis when the topology is confronted with the intentional attacks. In this section, we introduce the topology structure entropy [25] which can well measure the heterogeneity of topologies. The topology structure entropy is defined as follows [25]:

$$E=-\sum_{i=1}^{N} I_i \ln I_i \tag{25}$$

where $I_i = k_i \Big/ \sum_{i=1}^{N} k_i$ is an important degree of node i. k_i is the node degree of node i and N is the total number of nodes in the network.

When the network is completely uniform, $I_i = \frac{1}{N}$, the invulnerability of the topology is the strongest, the maximum value is

$$E_{\max} = -\sum_{i=1}^{N} \frac{1}{N} \ln \frac{1}{N} = \ln N \tag{26}$$

When the network is a star topology, all nodes are connected with a central node. At this time the invulnerability of the network is the worst. And $I_1 = \frac{1}{2}, I_j = \frac{1}{2(N-1)}, (j \neq 1)$, the minimal value is

$$E_{\min} = -\sum_{j=2}^{N} \frac{1}{2(N-1)} \ln\left(\frac{1}{2(N-1)}\right) - \frac{1}{2}\ln\frac{1}{2} = \frac{\ln 4(N-1)}{2} \tag{27}$$

Assuming r_i represents the serial number of the node i, the relationship between the node degree k_i and the serial number r_i is expressed by the function $k_i = f(r_i)$, and the degree-rank function is given by [24]:

$$f(r) = \left(\frac{\gamma-1}{Nc}\right)^{-\frac{1}{\gamma-1}} \left(r + \frac{cN^{2-\gamma}}{\gamma-1}\right)^{-\frac{1}{\gamma-1}} \tag{28}$$

substituting Equation (20) into Equation (29), we have

$$f(r)=k_{\min}N^{\frac{1}{\gamma-1}}\left(r+k_{\min}{}^{\gamma-1}N^{2-\gamma}\right)^{-\frac{1}{\gamma-1}} \quad \textbf{(29)}$$

Considering that the degree distribution of PSFBRA topology meets $\gamma > 3$, that is $k_{\min}{}^{\gamma-1}N^{2-\gamma} \approx 0$, and we get

$$f(r)=k_{\min}\left(\frac{N}{r}\right)^{\frac{1}{\gamma-1}} \quad \textbf{(30)}$$

With continuous approximation, the topology structure entropy E can be expressed as follows.

$$E=\frac{\int_1^N f(r)\ln f(r)dr}{\int_1^N f(r)dr}+\ln\left(\int_1^N f(r)dr\right) \quad \textbf{(31)}$$

Now, substituting Equation (31) into Equation (32), we have

$$E=\frac{\alpha N^{1-\alpha}\ln N}{N^{1-\alpha}-1}+\ln\frac{N^{1-\alpha}-1}{1-\alpha}-\frac{1}{1-\alpha},\ \alpha=\frac{1}{\gamma\text{-}1} \quad \textbf{(32)}$$

In Equation (33), the topology structure entropy E of scale-free topology can be expressed as the function of variables N and γ. When N and γ are constant, the topology structure entropy E can be used as the topology invulnerability strength criterion under intentional attacks. The greater E is, the more uniform the topology is, and the stronger invulnerability the topology is. This means topology structure entropy E should be maximized if the stronger invulnerability of PSFBRA scale-free topology is expected.

Fig. 2 displays the relationship between entropy E and scaling exponent γ for different N when the minimal connectivity $k_{\max}$ is defined. We know that with the increase of scaling exponent γ, the topology structure entropy increases, which makes the topology more uniform. So different scaling exponent γ brings the network a different topology of heterogeneity.

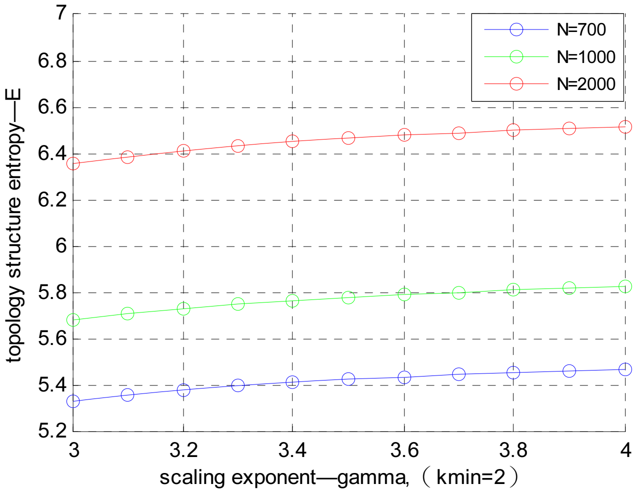

Fig. 2. The topology structure entropy function E

4.3 Mathematical Optimization Model of PSFBRA for Invulnerability

In order to improve the invulnerability under different attacks, a mathematical optimization model based on the random endurable probability p_r and the topology structure entropy E was proposed. By examining the relationship of random failures tolerance threshold, topology structure entropy and scaling exponent, we got the optimal value p_r and E. According to the above, this optimization problem of invulnerability can be transformed into the following:

$$\begin{cases} \max E(N,\gamma) \\ \max p_r(N,\gamma,k_{\min}) \\ s.t \\ \gamma > 3 \\ 1 \le k_{\min} \le N-1, k_{\min} \in Z^+ \end{cases} \Rightarrow \begin{cases} \max F = w_1 * E' + w_2 * p_r' \\ s.t \\ \gamma > 3 \\ 1 \le k_{\min} \le N-1, k_{\min} \in Z^+ \end{cases} \quad \textbf{(33)}$$

We convert the multi-objective problem to a single objective problem using the method of weighting aggregation. Then range method is used to standardize E and p_r obtain E' and p_r', and then entrusts with the weight of every indicator (w_1=0.3, w_2=0.7) according to the actual situation and the experimental results. Multi objective programming can be translated into right-hand of Equation (34), where F is the comprehensive network invulnerability.

By solving the programming problem, the optimal solutions γ and F are obtained for $k_{\min} = 2$. The results are shown in Fig. 3. We can see that the topology invulnerability achieves its maximum when $k_{\min} = 2$, $\gamma = 3.3606$. Combining $\gamma=\frac{2}{\beta_1}+1$, we can get $\beta_1 \approx 0.847$.

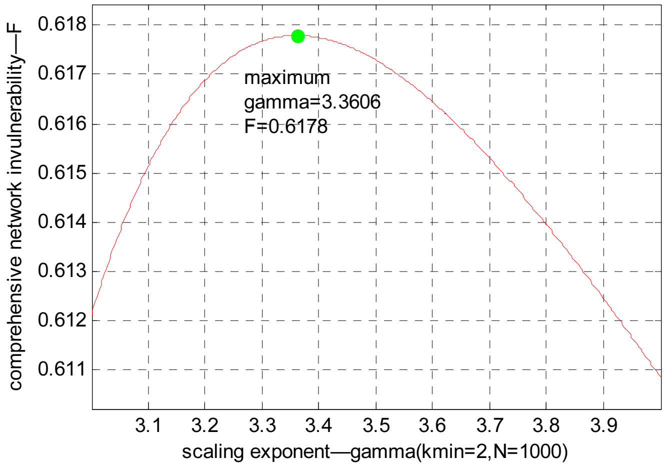

Fig. 3. The topology comprehensive invulnerability F

5 Simulation and Analysis

Under the condition of $k_{\min} = 2$, $\beta_1 \approx 0.847$, we use MATLAB to simulate the optimal PSFBRA topology process. For the sake of comparison, we also ran the energy-aware model (EAEM), the classic scale-free network model (BA). We compare several characteristics, i.e. degree distribution, average path length, maximal connected subgraph size [15]. Table 1 presents the parameters used in our simulation.

Table 1. Experimental parameters

Parameter	Value
Entire coverage region S	$400 \times 400m^2$
The networks size N	1000
Number of nodes in the initial state m_0	10
Links added in every time step m	2
Energy of nodes in the initial state E_0	$1J$
Each additional edge of the energy consumption α	$0.02J$
Transmission range R	$100m$

5.1 Degree Distribution

Fig. 4 represents the contrast of the theoretical value and actual value in the degree distribution of different topologies, the straight lines are the theoretical degree distribution. As can be seen, there are some nodes with high degree of WSNs in EAEM and BA, but the degree distribution of PSFBRA topology is relatively uniform. This is because the attractiveness of node is introduced into the design of PSFBRA, i.e. by control the energy of the node and the distance between the nodes, we can control degree growth rate of nodes which have already large degree. Therefore, the topology generated by model PSFBRA is very useful to avoid energy consumption.

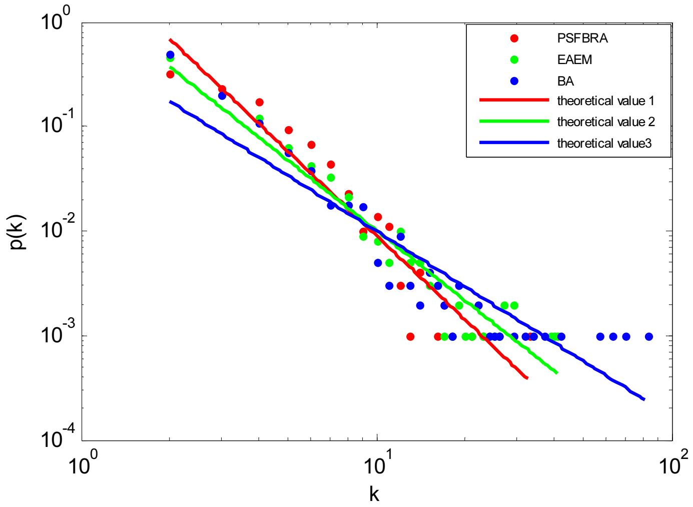

Fig. 4. Degree distribution of BA, EAEM and PSFBRA

5.2 The Experiments under Random Failures

Random failures mean that nodes in the network are randomly failed and at the same time the edges connecting with the failure nodes are also failed. Because of the low reliable hardware, the limited battery-power, and the harsh wilderness conditions, the sensor node failure often occurs in the practical application. Two metrics are also used to measure the topologies' invulnerability:

(1) Maximal connected subgraph size N' is the largest connected component remaining after the removal of some nodes which reflects the ability of network connectivity. The higher the connectivity is, the better the network invulnerability is.

(2) Average path length L is defined as the average number of distance along the shortest paths for all possible pairs of nodes in the maximal connected subgraph. It is a measurement of the efficiency of information. The definition is shown as

$$L = \frac{1}{N'\left(N'-1\right)/2} \sum_{1 \le i, j \le N'} d_{ij} \qquad \textbf{(34)}$$

where d_{ij} is the Euclidean distance between nodes i and j.

Fig. 5 (a) shows the maximal connected subgraph size N' for the increasing of the number of random failure nodes in different models. According to the simulation diagram, the PSFBRA model almost has the same invulnerability with the EAEM model and the BA model. This reflects that the PSFBRA model inherits the strong resistance to random failures of the scale-free topology.

Fig. 5 (b) shows average path length L of maximal connected subgraph under random failures. As the number of the failure nodes increases, the average path length of the three networks is also increased. The reason is that failure nodes make certain shortest paths broken. But L (PSFBRA) is shorter than L (EAEM) and L (BA). This is showed that PSFBRA network has robust topology, which can reach extreme efficiency in exchanging information for ubiquitous data-centric wireless sensor networks.

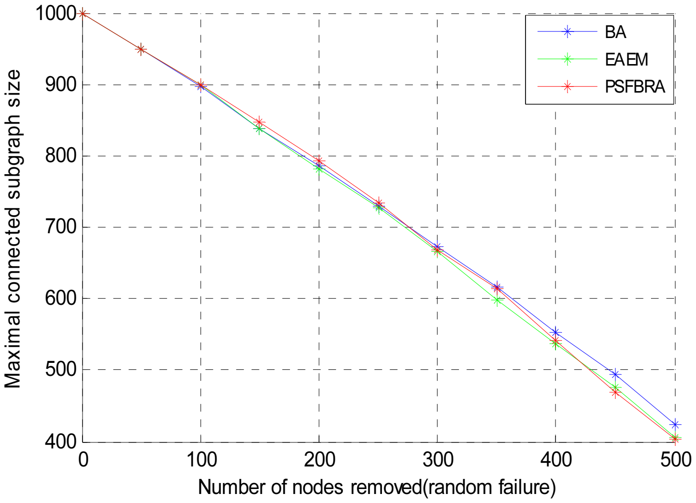

Fig. 5. (a) Comparison of maximal connected subgraph size (random attacks)

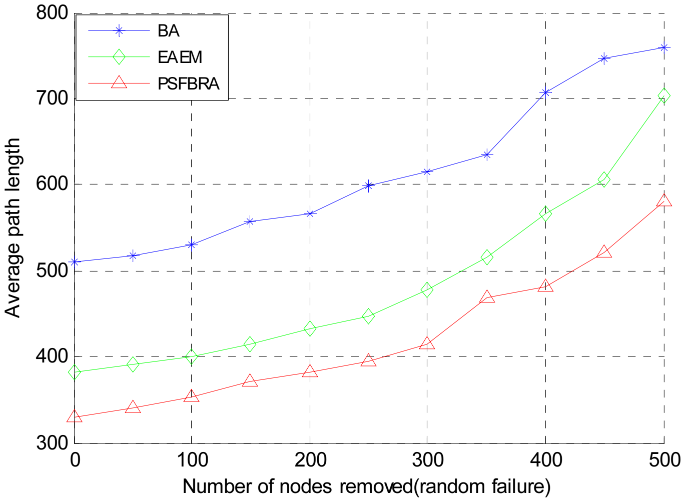

Fig. 5. (b) Comparison of average path length (random attacks)

5.3 The Experiments under Intentional Attacks

Intentional attack is another kind of accident for WSNs. Based on partial information of network, enemy can accurately attack the weakest parts and break down the whole system. So a network should have more robust topology to resist intentional attacks.

Fig. 6 (a) presents the maximal connected subgraph size under intentional attacks with high-degree nodes failed. From the three curves, we can observe that the BA and EAEM model can only tolerate 300 nodes and 400 nodes under intentional attacks respectively, while the PSFBRA model has more surviving nodes in the maximal connected subgraph, which means that PSFBRA model has stronger capability of maintaining connectivity and have a good invulnerability under intentional attack.

The average path length L against nodes' failure is shown in Fig. 6 (b). As shown in the figure, L(PSFBRA) is roughly shorter than L(EAEM) and L(BA). Moreover, when the number of failed nodes is more than 100 and 250, L(BA) and L(EAEM) curves present that have a rapid rise and fall, but the network topology optimized by PSFBRA model escapes this shake, showing stronger stability. The reason is that when the extent of destruction is large and the target network is distributed to many connection branches, the maximal connected subgraph will be diminished gradually and the average shortest path length will be a trend of being larger at first and smaller then. These results indicate that PSFBRA network has good invulnerability against nodes intentional attacks.

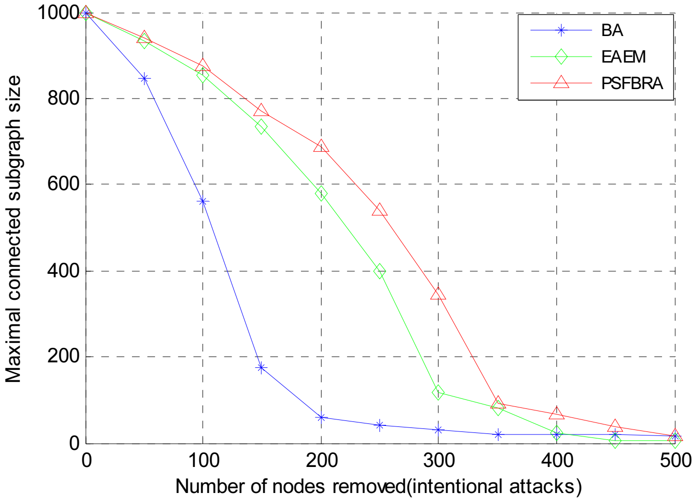

Fig. 6. (a) Comparison of maximal connected subgraph size (intentional attacks)

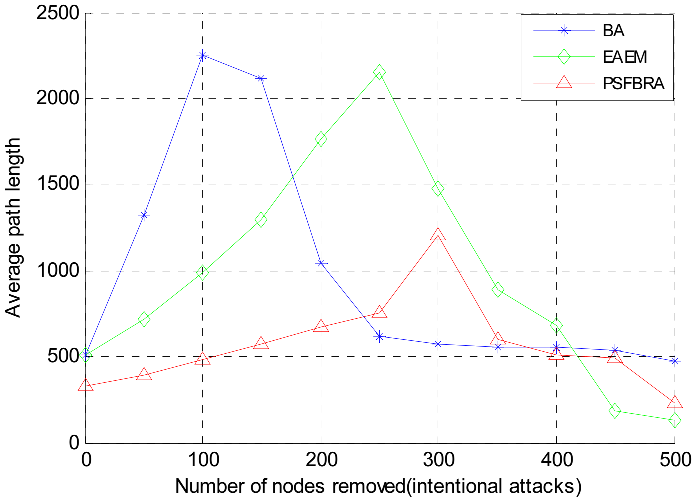

Fig. 6. (b) Comparison of average path length (intentional attacks)

6 Conclusion

Since scale-free networks can better exhibit the essential features of the real world and provide a reasonable model for us to construct a robust topology for WSNs. Firstly, based on the concept of attractiveness, we propose the Poisson-growth topology evolution model, which has the ability to change the power-law scaling exponent within [3,+∞) by adjusting its parameter. Then the endurable probability and the topology structure entropy are introduced to make quantitative measure the topological invulnerability. Through formulating and solving the multi-goals mathematic optimization model, the optimal parameter of the PSFBRA scale-free model is derived. Finally, both analysis and simulations reveal that the network topology generated by our proposed model and optimal parameter of the PSFBRA has a good invulnerability under random failures and intentional attacks, higher energy efficiency and can highly improve the network performance. WSNs is an application-oriented network, which is used differently in different environments, none topology structure can fit all conditions. It is believed that we provide some useful guidelines for the application of WSNs through introducing the scaling exponent adjustable model into the invulnerability of WSNs.

Acknowledgement

This work was supported by the National Nature Science Foundation of China (No.61373174), and the Fundamental Research Funds for the Central Universities (JB150716).

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, Wireless sensor networks: a survey, Computer Networks 38(4)(2002) 393-422.

[2] A. Bari, A. Jaekel., J. Jiang, Design of failures tolerant wireless sensor networks satisfying survivability and lifetime requirements, Computer Communications35(3)(2012) 320-333.

[3] S.G. Shen, R. Han, L. Guo, W. Li, Q. Cao, Survivability evaluation towards attacked WSNs based on stochastic game and continuous-time Markov chain, Applied Soft Computing 12(5)(2012) 1467-1476.

[4] S. Parvin, F.K. Hussain, J.S. Park, D.S. Kim, A survivability model in wireless sensor networks, Computers & Mathematics with Applications 64(12)(2012) 3666-3682.

[5] M. Chen, C.F. Lai, H. Wang, Mobile multimedia sensor networks: architecture and routing, EURASIP Journal on Wireless Communications and Networking 2011(1)(2011) 1-9.

[6] M. Alireza, A.H. Jahangir, Z. Taghikhaki, Survivability modeling of wireless sensor networks, in: Proc. Wireless Communication Systems, 2008. ISWCS'08. IEEE International Symposium on. IEEE, 2008.

[7] S.U. Hashmi, S.M.M. Rahman, H.T. Mouftah, N.D. Georganas, Reliability model for extending cluster lifetime using backup cluster heads in cluster-based wireless sensor networks, in: Proc. Wireless and Mobile Computing, Networking and Communications (WiMob), 2010 IEEE 6th International Conference on. IEEE, 2010.

[8] X.W. Fu, W.F. Li, F. Giancarlo, Empowering the invulnerability of wireless sensor networks through super wires and super nodes, in: Proc. Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium on. IEEE, 2013.

[9] V. Selvaraj, A.P. Renold, K-connected hybrid replay node placement in wireless sensor networks for restoring connectivity, ICTACT Journal on Communication Technology 5(2)(2014) 917-922.

[10] K. Lin, C.F. Lai, X. Guan, Energy efficiency routing with node compromised resistance in wireless sensor networks, ACM/Springer Mobile Networks & Applications (MONET) 17(1)(2012) 75-89.

[11] K. Lin, M. Chen, S. Zeadally, J.J.P.C. Rodrigues, Balancing energy consumption with mobile agents in wireless sensor networks, Future Generation Computer Systems 28(2)(2012) 446-456.

[12] H.L. Zhu, H. Luo, Complex networks-based energy-efficient evolution model for wireless sensor networks, Chaos, Solitons & Fractals 41(4)(2009) 1828-1835.

[13] G.Z. Zheng, Q.M. Liu, Scale-free topology evolution for wireless sensor networks, Computers & Electrical Engineering 39(6)(2013) 1779-1788.

[14] Y. Wang, E. Liu, X. Zheng, Z. Zhang, Y. Jian, X. Yin, F. Liu, Energy-aware complex network model with compensation, in Proc. IEEE Wi Mob, 2013.

[15] X. G. Qi, H. F. Wang, G. Z. Zheng, Study on evolution model of wireless sensor network invulnerability, Journal of software 25(1)(2014) 131-138.

[16] B. Wang, H. Tang, C. Guo, Z. Xiu, Entropy optimization of scale-free networks' robustness to random failures, Physica A:

Statistical Mechanics and its Applications 363(2)(2006) 591-596.

[17] Z. Feiyun, Entropy optimization of scale-free networks robustness to targeted attack, Information Technology Journal 12(9)(2013) 1868-1872.

[18] N. Jiang, F. Li, T. Wan, L. Liu, PDF: Poisson dynamics in fitness evolution model for wireless sensor networks, Journal of Ambient Intelligence and Humanized Computing 5(6)(2014) 919-927.

[19] N. Jiang, Y. Guo, Y. He, A local-world evolving model for WSNs with the self-regulating attractiveness, Journal of Networks 9(7)(2014) 1790-1797.

[20] X.W. Fu, W.F. Li., Clustering evolution model based on the local world for wireless sensor network, Journal on Communications, 36(9)(2015) 204-214.

[21] A. Barabasi, R. Albert, Emergence of scaling in random networks, Science 286(5439)(1999) 509-512.

[22] S.N. Dorogovtsev, J.F. FMendes, A.N. Samukhin, Structure of growing networks with preferential linking, Phys Rev Lett 85(21)(2000) 4633-4636.

[23] R. Albert, A.L. Barabasi, Mean-field theory for scale-free random networks, Physica A: Stat Mech Appl 272(1999) 173-87.

[24] R. Cohen, K. Erez, D. Ben-Avraham, S. Havlin, Resilience of the internet to random breakdowns, Physical Review Letters 85(21)(2000) 4626.

[25] J. Wu, Y.J. Tan, H.Z. Deng, D.Z. Zhu, Heterogeneity of scale-free network topology, System Engineering-Theory Practice 27(2007) 101-105.