A random walk evolution model of wireless sensor networks and virus spreading*

Wang Ya-Qi(王亚奇)† and Yang Xiao-Yuan(杨晓元)

Network and Information Security Key Laboratory of the Armed Police Force, Department of Electronics Technology , Engineering University of the Chinese People's Armed Police Force, Xi'an 710086, *China*

(Received 16 April 2012; revised manuscript received 19 June 2012)

In this paper, considering both cluster heads and sensor nodes, we propose a novel evolving a network model based on a random walk to study the fault tolerance decrease of wireless sensor networks (WSNs) due to node failure, and discuss the spreading dynamic behavior of viruses in the evolution model. A theoretical analysis shows that the WSN generated by such an evolution model not only has a strong fault tolerance, but also can dynamically balance the energy loss of the entire network. It is also found that although the increase of the density of cluster heads in the network reduces the network efficiency, it can effectively inhibit the spread of viruses. In addition, the heterogeneity of the network improves the network efficiency and enhances the virus prevalence. We confirm all the theoretical results with sufficient numerical simulations.

Keywords: wireless sensor network, random walk, network efficiency, virus spreading

PACS: 05.90.+m, 05.65.+b, 05.70.Np **DOI:** 10.1088/1674-1056/22/1/010509

1. Introduction

In recent years, research on the complex network theory has received much attention and formed a new research field.[1,2] Many important results have been obtained, and the proposals of small-world[3] and scale-free models[4] have raised an upsurge of research on complex networks. With the further study of complex networks, the research for relevant applications is attracting more and more attention,[5] e.g., in wireless sensor networks (WSNs).[6] The WSN is a self-organized network system consisting of a large number of cheap sensor nodes deployed in the monitoring region that could freely communicate with each other through multi-hop routing protocols, and it combines sensors, modern networks, wireless communication, embedded computing technologies, etc. As the WSN has many potential applications in civil and military fields, it is recognized as one of the most important technologies in the 21st century.[7]

The sensor nodes are generally equipped with limited power, and bad detection environments make the battery replacement extremely difficult. Thus, sensor node failure caused by energy depletion often occurs, which greatly reduces the reliability and stability of the entire system.[8] The restriction on node energy seriously hinders the further application of the WSN. To solve this problem, several network routing protocols have been designed.[9–11] Those protocols prolong the life cycle of the WSN to a certain extent, but still cannot avoid the node failure problem caused by other factors such as virus attacks and hardware failures. In order to reduce the influence of node failure, the WSN should possess a stronger fault tolerance. Therefore, the research into a fault-tolerant mechanism for the WSN has important practical significance.[12]

With the rapid development of the complex network theory, researchers begin to use it to study the fault tolerance of a WSN. Based on the random graph theory, Ding and Guan[13] proposed a new WSN evolution model and analysed its performance. The analysis showed that the model obviously improved the fault tolerance in the WSN. By introducing the small-world model, Hawick and James[14] constructed a WSN model to enhance the network fault tolerance and extend the lifetime of the network. Based on the complex network theory, Zhu *et al*.[15] put forward two energy efficient WSN evolution models and discussed the performances of those two models. Considering two different types of sensor nodes, Li *et al*.[16] gave a local-world WSN evolution model, and analysed the influence of a few factors such as the local world scale on the network performance. However, almost all of the existing studies ignored the feature of multi-hop communication in a WSN and assumed that each sensor node covered the same number of communication nodes, which is obviously inconsistent with the real network. By means of complex network theory, Chen *et al*.[17] built a local world WSN evolution model with scale-free property in order to obtain a high fault tolerance, but the evolution mechanism did not take into account the effect of node degree on the network performance. Recently, we[18] considered the limitation of the maximum degree of each node and presented another local world WSN model among sink nodes. Nevertheless, the model ignored the exis-

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61103231 and 61103230) and the Innovation Program of Graduate Scientific Research in Institution of Higher Education of Jiangsu Province, China (Grant No. CXZZ11_0401).

†Corresponding author. E-mail: wjwangyq@126.com

© 2013 Chinese Physical Society and IOP Publishing Ltd

tence of ordinary sensor nodes.

Based on the above research, in the present paper, we propose a novel evolution model according to the random walk mechanism[19] to further investigate the fault tolerance of a WSN. In order to construct a complete WSN, both cluster heads (denoted by C-type) and sensor nodes (denoted by S-type) will participate in the whole evolution process of the network.[16] In view of the fact that the scale-free networks possess a strong robustness against random failure,[20] the WSN generated by our evolution model exhibits scale-free property, and the node degree distribution exponent of the network can change continuously with the density of C-type nodes. In the evolution mechanism, the preferential attachment is not only related to the residual energy of the WSN nodes, but also depends on the node degree. The research shows that the WSN generated by such an evolution model has a good fault tolerance and can dynamically balance the energy consumption of the network, which greatly improves the network performance and prolongs the life cycle of the network. We also find that increasing the density of C-type nodes extends the average path length of the network and reduces the network transmission efficiency. However, the heterogeneity of the network is able to improve the network efficiency.

In order to effectively deal with the growing severe security threats faced by WSNs, in this paper we investigate the spreading dynamical behavior of viruses in the evolution model by means of the propagation theory of complex networks. The virus transmission dynamic is one of the main research contents of the complex network theory.[21–24] When describing the propagation process of network viruses, it usually requires appropriate propagation models, such as susceptible-infected-susceptible (SIS)[25] and susceptible-infected-removed (SIR)[26] models. In the SIS model, each node has two possible discrete states: susceptible and infected. The susceptible state represents that the node is free of viruses but can be infected. The infected state means that the node has been infected and can pass viruses to other susceptible nodes. In this paper, we mainly adopt the SIS model to study the influences of C-type node density and network heterogeneity on virus propagation characteristics. The results show that both the virus propagation velocity and the virus prevalence decrease as the C-type node density increases, but the network heterogeneity increases the density of infected nodes. Finally, numerical simulations are used to verify these conclusions. We hope that our study will expand the application areas of WSNs and contribute to the prevention and control of viruses in a WSN.

The rest of this paper is organized as follows. Based on the random walk mechanism, a novel WSN evolution model is established in Section 2. In Section 3, the theoretical analysis of the evolution model is presented. Then in Section 4, numerical simulations are given to confirm the predictions obtained in Section 3. Finally, in Section 5, some conclusions are drawn from the present studies.

2. Novel evolution model of WSN

In this section, we propose an evolution model that can generate a scale-free WSN to enhance the fault-tolerant performance of the network. Considering the importance of consumption balance of node energy for the WSN, we use the preferential attachment mechanism that depends on the product of the node degree and the node's residual energy. In a WSN, the collected data can be transmitted between different C-type nodes and between C-type nodes and S-type nodes. However, data transmission is usually not allowed between different S-type nodes.[16,27] Based on this, our evolution model allows us to establish connections between C-type nodes and S-type nodes as well as between different C-type nodes, but does not allow connections between different S-type nodes. The node energy in the WSN is mainly used for collecting, processing, and transmitting data, wherein the data transmission consumes the most energy.[28] Therefore, we can assume that the residual energy of each node in the WSN remains unchanged in the evolution process. Based on the random walk strategy, the WSN evolution mechanism is described as follows.

(i) The network is initialized with a small number (m_0) of C-type nodes and one base station, and all m_0 C-type nodes are connected to the base station.

(ii) One C-type node or S-type node is randomly chosen as the starting point of the random walk.

(iii) At each step of the walk, the probability that a walker moves from the current node i to one of its C-type neighbors j is expressed as

$$\prod_{i\to j} = \frac{E_j k_j}{\sum\limits_{l\in\Lambda_i} E_l k_l}, \tag{1}$$

where E_j and k_j are the residual energy and the degree of node j, respectively, and Λ_i denotes the set of C-type neighbors of node i. If node j is not marked, then mark it, or else, randomly walk again. Repeat the random walk process until m different C-type nodes are marked.

(iv) A new C-type or S-type node is added to the network with probability (node density) α or $1-\alpha$, respectively, and connected to the m marked C-type nodes by undirected links.

(v) The whole process is repeated starting from step (ii), until the network size reaches up to N.

From the above evolution mechanism, we can see that the generation process of the WSN takes into account the evolution of both C-type nodes and S-type nodes. In the whole evolution process, only the degree of C-type node continuously increases, while the S-type node connectivity is always m, i.e.,

it remains unchanged. The probability that one C-type node is selected to establish a new link is not only related to its connectivity, but is also determined by its residual energy. For the same connectivity, the more residual energy a C-type node has, the bigger the probability that it will be selected to establish a new connection. Therefore, the evolution mechanism can keep the balance of residual energy of the entire network, so as to prolong the network life cycle and improve the whole performance of the network.

3. Analysis of the WSN evolution model

The node degree distribution is an important statistical parameter used to describe the topological structure of a complex network. In this section, we use the mean field theory to analyze the degree distribution of the proposed evolution model.[29] In the evolution process of the network, the connectivity of the S-type node always remains a constant, while the C-type node connectivity will continuously increase with the evolution time. So here we pay attention mainly to the degree distribution of C-type nodes.

Let $p(i)$ be the probability that node i is randomly selected from the network with N nodes $p(i) = 1/N$, and $p(j)$ be the probability that the walker arrives at one C-type neighbour j of node i by following one of the k_i links connected to node i. The expression of $p(j)$ can be derived by using the Bayes rule as[17]

$$p(j) = \frac{p(j/i)\,p(i)}{p(i/j)}, \tag{2}$$

where the conditional probability $p(j/i)$ denotes the probability that the walker moves from the starting node i to its C-type neighbor j. From the proposed evolution model, we know that $p(j/i)$ can be written as

$$p(j/i) = \prod_{i\to j} = \frac{E_j k_j}{\sum\limits_{l\in\Lambda_i} E_l k_l}. \tag{3}$$

Similarly, the conditional probability $p(i/j)$, i.e. the probability that the walker starts at j and arrives at i, is given by

$$p(i/j) = \prod_{j\to i} = \frac{E_i k_i}{\sum\limits_{l'\in\Lambda_j} E_{l'} k_{l'}}, \tag{4}$$

where Λ_j is the set of all C-type nodes in the neighborhood of node j.

To conveniently analyze the problems without losing rationality, here we suppose that $E_l = E_{l'} \approx \langle E' \rangle$ and $k_l = k_{l'} \approx \langle k \rangle$,[16] where $\langle E' \rangle$ is the mean value of residual energy of all C-type nodes in the network and $\langle k \rangle$ is the average degree of the network. From this, $\sum\limits_{l\in\Lambda_i} E_l k_l$ in Eq. (3) and $\sum\limits_{l'\in\Lambda_j} E_{l'} k_{l'}$ in Eq. (4) will become

$$\sum_{l\in\Lambda_i} E_l k_l \approx \alpha k_i \langle k \rangle \langle E \rangle, \tag{5}$$

$$\sum_{l'\in\Lambda_j} E_{l'} k_{l'} \approx \alpha k_j \langle k \rangle \langle E \rangle. \tag{6}$$

Furthermore, the starting node in the random walk process is chosen randomly. Thus, on average, k_i in Eq. (5) equals k_j in Eq. (6). Hence, we can obtain

$$\sum_{l\in\Lambda_i} E_l k_l = \sum_{l'\in\Lambda_j} E_{l'} k_{l'}. \tag{7}$$

Combining all the above equations, we can obtain

$$p(j) = \frac{\frac{k_j E_j}{\sum\limits_{l\in\Lambda_i} E_l k_l}}{\frac{k_i E_i}{\sum\limits_{l'\in\Lambda_j} E_{l'} k_{l'}} N} = \frac{E_j k_j}{E_i k_i N}. \tag{8}$$

According to the proposed WSN evolution mechanism, the evolution of network topology can be regarded as a dynamic growth process, i.e., at each time step there will be one new C-type or S-type node connected to m existing C-type nodes in the network. Thus, only the degree of the C-type node continuously increases with the network evolution. In order to utilize the mean field theory to analyze the performance of the evolving network, we assume that the network undergoes a long time evolution and k_j is a continuous parameter with time t. So the growth rate of k_j can be described as

$$\frac{\partial k_j}{\partial t} = \alpha m p(j) = \alpha m \frac{E_j k_j}{E_i k_i N}. \tag{9}$$

In order to simplify Eq. (9), Nk_i can be expressed as[30]

$$Nk_i = N\langle k \rangle = \sum_i k_i. \tag{10}$$

The summation over the degrees of all existing C-type nodes during the time step from 0 to t can be calculated as

$$\sum_i k_i = 2m_0 + (1+\alpha)mt. \tag{11}$$

Substituting Eqs. (9) and (10) into Eq. (11) gives

$$\frac{\partial k_j}{\partial t} = \frac{\alpha m E_j k_j}{E_i k_i N} = \frac{\alpha m E_j k_j}{E_i\,(2m_0 + (1+\alpha)mt)}, \tag{12}$$

that is,

$$\frac{\mathrm{d}k_j}{k_j} = \frac{\alpha m E_j}{E_i} \cdot \frac{\mathrm{d}t}{2m_0 + (1+\alpha)mt}, \tag{13}$$

which yields the solution

$$k_j(t) = C\,(2m_0 + (1+\alpha)mt)^{\frac{\alpha f(E)}{1+\alpha}}, \tag{14}$$

where

$$f(E) = \frac{E_j}{E_i}. \tag{15}$$

The $f(E)$ is related to the residual energy distribution of C-type nodes, and the possible distributions usually include uniform distribution, power-law distribution, exponential distribution,[15] etc. For the uniform distribution, we have $f(E) = 1$.

At each time step, when one new C-type or S-type node enters into the network, m new links are established with m old C-type nodes. Thus, the initial condition can be obtained as

$$k_j(t_j) = m. \tag{16}$$

Then inserting Eq. (16) back into Eq. (14), we obtain

$$k_j(t) = m\left(\frac{2m_0+(1+\alpha)mt}{2m_0+(1+\alpha)mt_j}\right)^{\frac{\alpha f(E)}{1+\alpha}}. \tag{17}$$

Equation (17) shows that the degrees of all C-type nodes evolve in the same manner, namely, obeying a power-law distribution. The main difference is that due to the fact that the C-type nodes have different residual energies, the intercepts of the power functions are different from each other. Then, at time t the probability that one C-type node j has a connectivity $k_j(t)$ smaller than k is

$$\begin{aligned} &p(k_j(t)<k) \\ &= p\left(t_j > \frac{(2m_0+(1+\alpha)mt)\,m^{\frac{1+\alpha}{\alpha f(E)}}k^{-\frac{1+\alpha}{\alpha f(E)}}-2m_0}{(1+\alpha)m}\right). \end{aligned} \tag{18}$$

Suppose that one new C-type node with probability α enters into the network at equal time intervals, the probability density at time t_j is defined as

$$p(t_j) = \frac{1}{m_0+\alpha t}. \tag{19}$$

Combining Eqs. (18) and (19) yields

$$\begin{aligned} &p(k_j(t)<k) \\ &= 1-p\left(t_j \le \frac{(2m_0+(1+\alpha)mt)\,m^{\frac{1+\alpha}{\alpha f(E)}}k^{-\frac{1+\alpha}{\alpha f(E)}}-2m_0}{(1+\alpha)m}\right) \\ &= 1-\frac{(2m_0+(1+\alpha)mt)\,m^{\frac{1+\alpha}{\alpha f(E)}}k^{-\frac{1+\alpha}{\alpha f(E)}}-2m_0}{(1+\alpha)m}\frac{1}{m_0+\alpha t}. \end{aligned} \tag{20}$$

Thus, we can obtain the degree distribution $P(k)$ from Eq. (20)

$$\begin{aligned} P(k) &= \frac{\partial p(k_j(t)<k)}{\partial k} \\ &= \frac{2m_0+(1+\alpha)mt}{\alpha f(E)(m_0+\alpha t)m}m^{\frac{1+\alpha}{\alpha f(E)}}k^{-1-\frac{1+\alpha}{\alpha f(E)}}. \end{aligned} \tag{21}$$

When $t\to\infty$, further simplifying Eq. (21), we can obtain

$$P(k) = \frac{1+\alpha}{\alpha^2 f(E)}m^{\frac{1+\alpha}{\alpha f(E)}}k^{-\gamma}, \tag{22}$$

where $\gamma = 1+(1+\alpha)/\alpha f(E)$ is the degree exponent.

From Eq. (22), we find that the WSN generated by our evolution model has the scale-free property, and thus a good fault tolerance can be achieved. Because in the preferential attachment mechanism the effect of the node residual energy is taken into account, the evolving network is able to keep the energy of the entire system dynamically balanced. Thereby, the life cycle of the network can be extended. Equation (22) also shows that the degree distribution exponent γ of C-type nodes in the network not only depends on the distribution of residual energy $f(E)$, but also changes continuously with the proportion of C-type nodes. Especially, when $\alpha = f(E) = 1$, $\gamma = 3$. In addition, the degree distribution exponent γ is not affected by the evolution time t, the minimum node degree m, and the initial number of nodes m_0. As the evolution model does not depend on the specific node distributed environment, it can be widely used in various large-scale deployed WSNs with multi-hop communication behavior.

4. Numerical simulations

In this section, by means of numerical experiments we further study the statistical properties of the proposed WSN evolution model, as well as the transmission dynamical behaviors of viruses in the evolution model. In the simulation, the parameters are chosen as follows: the total number of nodes of the network $N = 5000$, the initial number of C-type nodes $m_0 = 2$, and the minimum number of links attached to any node $m = 1,2,3$ respectively. In the evolution process, we assume that the residual energies of all C-type nodes follow a uniform distribution in $[0.5,1]$. When viruses begin to spread in the network, one C-type or S-type node is randomly selected as the infected node. We define the effective spreading rate of viruses as λ, the density and the relative density of infected nodes with given connectivity k at time t as $\rho(t)$ and $\rho_k(t)$, respectively. As viruses spread in the network, they will finally come to a steady state. The parameters ρ and ρ_k are defined as the steady state values (i.e., the virus prevalence) of $\rho(t)$ and $\rho_k(t)$, respectively, and $\rho = \sum_k P(k)\rho_k$.[31] All the following simulation results are obtained by averaging over 20 independent runs of the network model.

4.1. Statistical characteristics of the WSN evolution model

Figure 1 shows the corresponding relationship between the degree distribution $P(k)$ and the density of C-type nodes α in the WSN evolution model. From Fig. 1, it can be seen that when α has different values ($\alpha = 0.2, 0.5, 1$), the degree distribution of the evolution model obeys a power-law distribution, which indicates that the WSN generated by the proposed model can acquire a better fault tolerance. Figure 1 also implies that the result of the numerical simulation is consistent with the theoretical analysis from Eq. (22), which fully verifies the correctness of the theoretical analysis. It is noted that due to taking a reasonable approximation in the process of theoretical analysis, there is only a slight deviation between the coefficients of degree distributions $P(k)$ obtained from the above two methods.

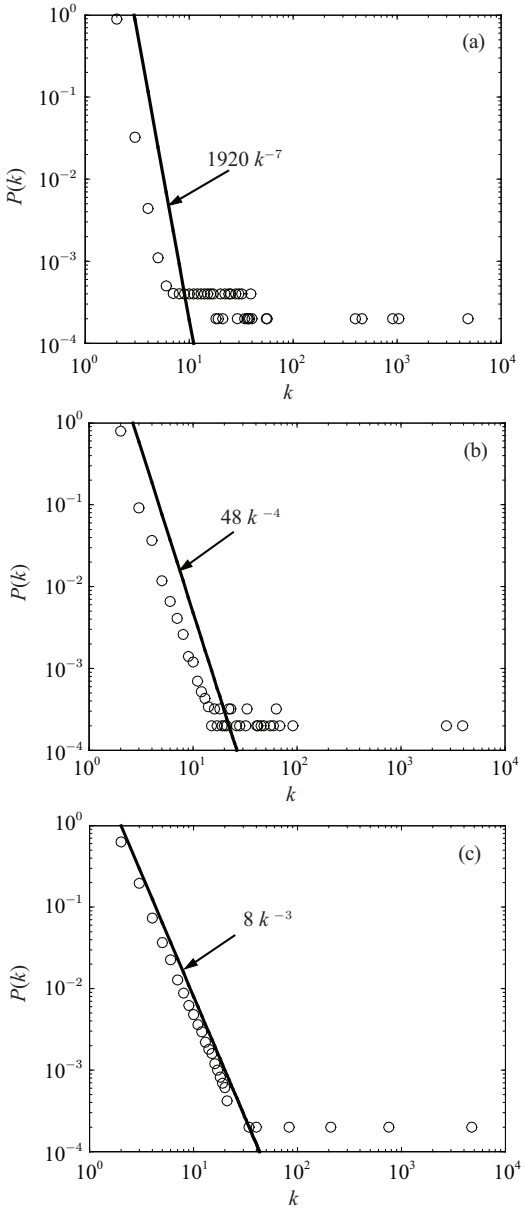


Fig. 1. Degree distribution $P(k)$ versus node degree k for three different values of α, i.e., $\alpha = 0.2$ (a), 0.5 (b), and 1(c).

In Fig. 2, we show the degree distribution $P(k)$ versus k for three different values of m in the WSN evolution model, where $\alpha = 0.5$. As shown in Fig. 2, when m changes ($m = 1, 2, 3$), the degree exponent of the evolution model γ remains unchanged, which fully illustrates that the scale-free feature of the proposed evolution model is not influenced by the value of m, and again verifies the rationality of the theoretical analysis. As m increases, the number of links of each node in the network will also increase, thereby enhancing the fault tolerance of the evolving network. However, a large m increases the node energy consumption. Therefore, in order to extend the life cycle of the entire network, we usually select a smaller m when using the proposed evolution model to construct a WSN.

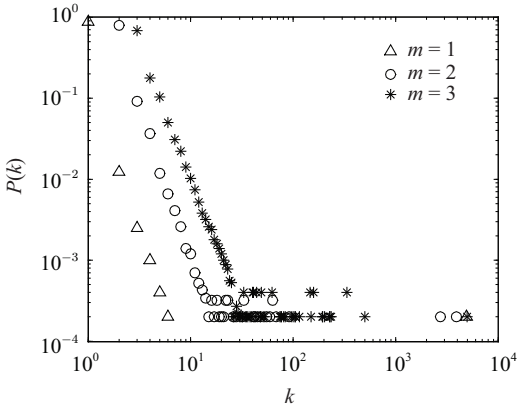


Fig. 2. Degree distribution $P(k)$ versus k for three different m.

In order to describe the data transmission performance of the evolving network, the average path length of the network L and the network efficiency η are introduced.[32] The former indicates the average number of hops among the network nodes for transmitting data. The latter measures how efficiently the network transmits data. The L and η are respectively defined as follows:[16,33]

$$L = \frac{1}{N(N-1)} \sum_{i \neq j} l_{ij}, \tag{23}$$

$$\eta = \frac{1}{N(N-1)} \sum_{i \neq j} \eta_{ij}, \tag{24}$$

where l_{ij} denotes the length of the shortest path between any two nodes i and j, and $\eta_{ij} = 1/l_{ij}$ is the efficiency between any two nodes i and j.

Figure 3 illustrates the average path length of the evolving network L versus the density of C-type nodes α for two different values of m. We observe that for a given m, L increases as α increases, which means that the larger the number of C-type nodes in the network, the more hops the data transmission experiences. Therefore, in order to accelerate the data transmission in the network, the proportion of C-type nodes should be appropriately reduced. From Fig. 3, it can also be seen that for a given α, L decreases with the increase of m, which shows that the increase of heterogeneity level of the network will be favorable for data transmission in the network.

In Fig. 4, we plot the network efficiency η versus C-type node density α for two different values of m. As shown in Fig. 4, η significantly decreases as α increases, which indicates that the reduction in the number of C-type nodes can improve the efficiency of data transmission in the network. The main reason for this is that the decrease of α can lower L. Moreover, when α remains invariant, η increases as m increases. This is because the larger the value of m, the more alternative paths can be used to transmit data in the network. Thus, the probability that a smaller L exists increases, and the network efficiency is also improved.

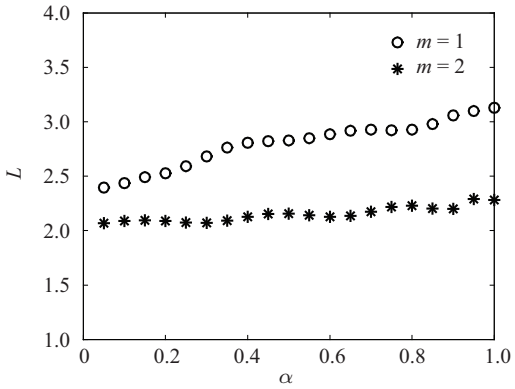


Fig. 3. Average path length of the network L versus α for two different values of m.

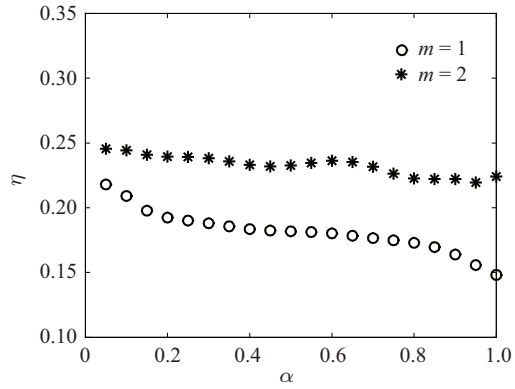


Fig. 4. Network efficiency η versus α for two different values of m.

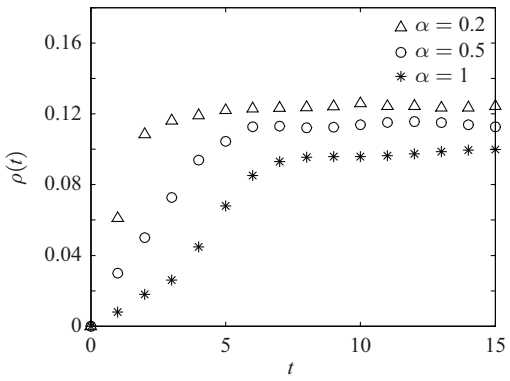


Fig. 5. Density of infected nodes $\rho(t)$ versus t for three different values of α.

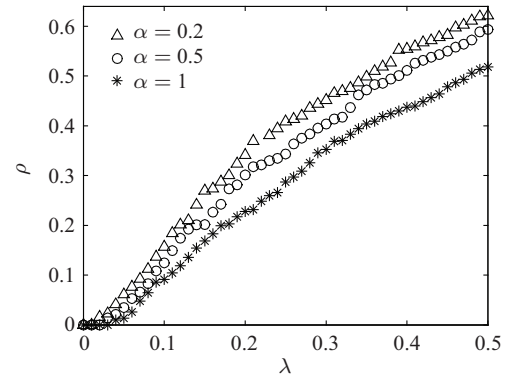


Fig. 6. Prevalence ρ versus the effective spreading rate λ for three different values of α.

4.2. Virus spreading in the WSN evolution model

Figure 5 shows the evolutions of the density of infected nodes $\rho(t)$ with t for three different values of α, where $\lambda = 0.1$ and $m = 2$. From Fig. 5, we observe that the viruses can spread in the network and eventually reach a steady state for a given effective spreading rate λ, and the virus propagation velocity is reduced with the increase of α. According to this, we can conclude that the higher the number of C-type nodes in the network, the more slowly the viruses spread. Thus, increasing the C-type node density can effectively inhibit the spreading of viruses in the network.

Figure 6 depicts the evolution relationships between the prevalence ρ and the effective transmission rate λ for three different values of α, where $m = 2$. From Fig. 6, we find that as α decreases, the virus threshold obviously decreases, while the virus prevalence continuously increases, which indicates that the increase of the C-type nodes can weaken the probability of virus outbreak in the network. Figure 6 also shows that no matter how the value of α changes, the virus thresholds are all relatively small, which implies that the viruses are able to spread easily in the network and eventually reach a steady state. Therefore, when viruses appear in the network, the key nodes should be especially protected.

Figure 7 exhibits the change of the prevalence ρ with the effective spreading rate λ for three different values of m, where $\alpha = 0.5$. As shown in Fig. 7, for a given λ, the prevalence ρ increases as m increases, which mainly because the large m raises the efficiency of data transmission, and more importantly, also accelerates the spread of virus in the network. As a result, more network nodes are infected. From this, we can conclude that in order to reduce the spreading velocity of viruses in the network, a smaller m should be chosen when we utilize the evolution model to generate a network, i.e., lowering the heterogeneity of the network, which approximately agrees with the conclusions obtained by previous studies on the propagation behavior of viruses in scale-free networks.

Figure 8 illustrates the dependence of relative prevalence ρ_k on node degree k for two different values of α, where $\lambda = 0.5$ and $m = 2$. As shown in Fig. 8, when the value of λ is given, the nodes with large degrees are infected more easily. From this, we can see that in the process of virus spreading, after the hubs have been quickly infected, viruses will pervade in the nodes with smaller values of node degree. Figure 8 also shows that the transmitting tendency of viruses in the network will be weakened with the increase of density of C-type nodes.

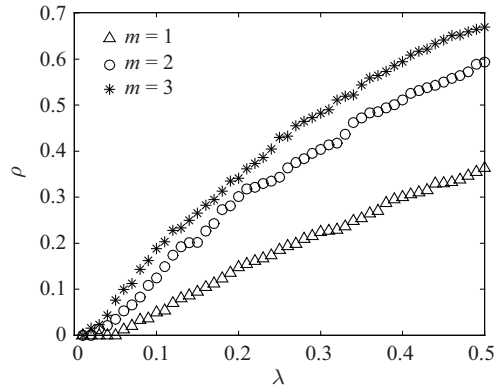


Fig. 7. Prevalence ρ versus λ for three different values of m.

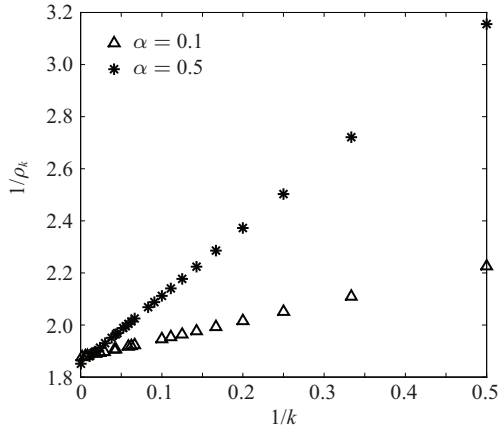


Fig. 8. Relative prevalence ρ_k versus k for two different values of α.

From Figs. 3–8, we can draw a conclusion that in the WSN evolution model, increasing the value of m can obviously improve the efficiency of data transmission, but the energy consumption of network nodes also increases. Meanwhile, when viruses spread in the networks, the large m greatly increases the transmission velocity of viruses. Therefore, in the process of constructing a WSN by using the proposed evolution model, we should consider all the above cases to determine a reasonable value of m. In addition, when the number of C-type nodes is larger, the network efficiency will be apparently reduced. In fact, the number of C-type nodes may not be too large, and thus a smaller α should be selected. However, when viruses spread in the network, we can appropriately increase m to effectively mitigate the virus spreading in the network.

5. Conclusion

Application research of the complex network theory in a WSN has attracted wide attention. In this paper, we present a new evolution model to study the decrease in the fault tolerance of WSN, and discuss the spreading dynamical behaviors of viruses in the model. In order to dynamically balance the energy consumption of the entire network and prolong the network life cycle in the evolution model, the product of node residual energy and cluster node degree is taken as the judgment basis for establishing priority connection. Firstly, it is found that the degree distribution of the evolution model has a scale-free property, so a better fault tolerance can be obtained. Secondly, increasing the number of cluster nodes reduces the network efficiency and the virus prevalence in the network. Thirdly, the heterogeneity of the network improves the network efficiency, but also accelerates the spreading of network viruses. Finally, when viruses propagate in the network, the nodes with large degrees are infected first, then the nodes with smaller degrees are infected. In order to further expand the application fields of the WSN, using the complex network theory to explore the network fault tolerance and the transmission dynamic behavior of viruses in the network deserve to be studied further. This paper deals only the case that residual energies of nodes obey a uniform distribution, but in the real networks, it may satisfy a variety of distributions. Thus, the influence of node residual energy distribution on the spreading behavior of viruses is worth further investigation. Additionally, combining the specific network transport protocols to discuss the virus spreading in the evolution model is another problem that should be studied in the future.

References

[1] Boccaletti S, Latora V, Moreno Y, Chavez M and Hwang D U 2006 *Phys. Rep.* **424** 175
[2] Newman M E J 2003 *SIAM Rev.* **45** 167
[3] Watts D J and Strogatz S H 1998 *Nature* **393** 440
[4] Barabási A L and Albert R 1999 *Science* **286** 509
[5] Costa L F, Oliveira O N, Travieso G and Rodrigues F A 2011 *Adv. Phys.* **60** 329
[6] Herdelberger R 2007 *Nature* **450** 623
[7] Akyildiz I F, Su W and Sanakarasubramaniam Y 2002 *Comput. Netw.* **38** 393
[8] Puccinelli D and Haenggi M 2005 *IEEE Circ. Syst. Mag.* **5** 19
[9] Tan H Ö and Köpeoglu I 2003 *ACM Sigmod Record* **32** 66
[10] Kalpakis K, Dasgupta K and Namjoshi P 2003 *Comput. Netw.* **42** 697
[11] Liang W F and Liu Y Z 2007 *IEEE Trans. Mobile Comput.* **6** 2
[12] Lu K, Liu G, Mao R and Feng Y 2011 *IET Wirel. Sens. Syst.* **1** 1
[13] Ding L and Guan Z H 2008 *Physica A* **387** 3008
[14] Hawick K A and James H A 2010 *Int. J. Wirel. Mobile Comput.* **4** 155
[15] Zhu H L, Luo H, Peng H P, Li L X and Luo Q 2009 *Chaos Soliton. Fract.* **41** 1828
[16] Li S D, Li L X and Yang Y X 2011 *Physica A* **390** 1182
[17] Chen L J, Liu M, Chen D X and Xie L 2009 *Chin. J. Comput.* **32** 69 (in Chinese)
[18] Wang Y Q and Yang X Y 2012 *Acta Phys. Sin.* **61** 090202 (in Chinese)
[19] Chelminiak P 2011 *Phys. Lett. A* **375** 3114
[20] Albert R, Jeong H and Barabfisi A L 2000 *Nature* **406** 378
[21] Xu J and Wang X F 2005 *Physica A* **349** 685
[22] Goh K I, Kahng B and Kim D 2001 *Phys. Rev. Lett.* **87** 278701
[23] Motter A E, Zhou C and Kurths J 2005 *Phys. Rev. E* **71** 016116
[24] Pastor-Satorras R and Vespignani A 2001 *Phys. Rev. Lett.* **86** 3200
[25] Shi H J, Duan Z S, Chen G R and Li R 2009 *Chin. Phys. B* **18** 3309
[26] Gong Y W, Song Y R, and Jiang G P 2012 *Chin. Phys. B* **21** 010205
[27] Cheng X, Wang H L and Qi O Y 2002 *Phys. Rev. E* **65** 066115
[28] Anastasi G, Conti M, Francesco M D and Passarella A 2009 *Ad Hoc Netw.* **7** 537
[29] Park H, Haule K and Kotliar G 2008 *Phys. Rev. Lett.* **101** 186403
[30] Qin S and Dai G Z 2009 *Chin. Phys. B* **18** 383
[31] Xu X J and Chen G R 2009 *Int. J. Bifurcation Chaos* **19** 623
[32] Latora V and Marchiori M 2001 *Phys. Rev. Lett.* **87** 198701
[33] Latora V and Marchiori M 2003 *Eur. Phys. J. B* **32** 249