ISSN 1749-3889 (print), 1749-3897 (online)
International Journal of Nonlinear Science
Vol.16(2013) No.1,pp.31-36

Based on Research in the Area of Wireless Sensor Network Monitoring Systems

Hongxing Yao, Zebiao Feng *
Faculty of Science, Jiangsu University, Zhenjiang, Jiangsu ,212013, P.R.China
(Received 5 March 2012, accepted 28 April 2013)

Abstract: In order to improve the regional monitoring system intelligent and anti-attack performance, the article from the network self evolution characteristics of new point of view, using the application of wireless sensor network in monitoring system and defining the monitoring network model with the characteristics of wireless sensor networks. Using the enemy attack as the main purpose of evolution model, the experiments show that the use of preferential attachment between new and old nodes selection, making the network show the evolution ability is more stable and reliable, effectively maintain the network degree distribution form. Using mean field theory as the theoretical basis, analysis the characteristics of network. Simulation results show that, the network system can defend the attack of the enemy, to maintain the efficiency of the transmission network.

Keywords:wireless sensor networks; detection networks; defense of networks; mean field theory

1 Introduction

With the rapid development of resource exploration technology in recent years, many remote uninhabited areas become the main provider of energy. Uninhabited area causes a lot of territorial disputes because of its rich mineral resources. How to control these areas effectively, monitor these areas real-time becomes a problem [1]. Currently, many countries are monitoring unmanned area by radar, usually in a remote area construction of the radar station to the surrounding environment monitoring. However, the construction of the radar station conditions is relatively high, the cost is very expensive. Therefore, more subtle and low-cost wireless sensor networks are development to control a direction of the unmanned area[2].

Generation of wireless sensor networks for unmanned area monitoring provides a different perspective. In wireless sensor networks, the nodes are mostly random distribution in complex geomorphology areas, or running humans can not get close to the bad and dangerous environment even, in order to the sensor nodes save energy generally closer node more prone to data transmission, which makes the wireless sensor network has the characteristics of a certain local world[3]. The characteristics of the local world of wireless sensor networks are more and more used in all aspects. Zhu Zhengwei[4], the design of a transmission based on wireless sensor network platforms, solution to the high cost of existing wind farm monitoring and control methods and maintenance difficult issues effectively. Liu Lei[5] improved leeway drift model used in marine search and rescue, the state of motion of the sensor nodes are randomly deployed in the ocean surface modeling, simulation and analysis by the sensor network area coverage and network connectivity under different sea conditions, its state of motion. Dang Yuefang[6] analysis the potential advantages of wireless sensor networks in the battlefield environment, and the application of the status quo in the military field. Bian Qiuxiang and Xing Yao[7] studied two complex networks (LGS), and to promote its application in the enterprise economy. Breakthrough in theory. Li[8] from the point view of the evolution of wireless sensor networks, put forward a local area network clustering evolution model, and verify the effectiveness of the network for data transmission, it is more true to a certain extent embodies the characteristics of wireless sensor networks, but there are still some limitations and did not consider its energy problems the heterogeneity of the energy of sensor network nodes. Li Xiang and Chen Guanrong [9], raise a local world evolving model, this portrait of the self-organization of the network evolution more realistic. Luo Xiaojuan [10]from the dynamic evolution of the wireless sensor network, and demonstrate the degree distribution of the network transmission efficiency and network characteristics.

* **Corresponding author**. *E-mail address*: fzbdgfyx@126.com

IJNS.2013.08.15/739

In this paper, based on the reference literature we designed a model of a wireless sensor network to monitor the area affected by external attacks. In order to destroy the entire network rapidly, the enemy will first attack the important node which hsa large node node in the network. Node supplement is need to maintain normal transfer of the entire network information to defend against attacks on the network, the new node and the original node preferential attachment mechanism to establish a communication link. After a longer time attacked, analysis the data of the entire network. The theory based on the impact of the changed nodes in a wireless sensor network self-organization evolution, the degree distribution of the network and the network transmission efficiency. The analysis tool is the mean-field theory, we analyzed some of the characteristics of the network evolution process finally, and simulation experiments to verify the text of the relevant conclusions.

2 The idea of a base model

Basic evolution of wireless sensor network construction algorithm is as follows [10]:

Initial conditions: the network has n0 nodes and e0 edges then adding a new node with the m connections, then at each time step, the new nodes are selected in accordance with a probability distribution network already has m nodes, and connection its established.

The new node is connected with M nodes throughout the network randomly get local world.

According to the preferential attachment of the probability distribution:

$$\prod(k_i) = \prod_{i \in local}(k_i) \Big/ \sum_{j \in local} k_j = \frac{M}{m_0 + t} \frac{k_i}{\sum\limits_{j \in loca} k_j} M \geq m.$$

The above is a reference model of the design ideas of the present model.

3 Regional monitoring model design

In this paper, a square area simulation tested uninhabited area is used. Uniformly in a square two-dimensional plane of the wireless sensor placed evenly wherein these wireless sensors is detected by the radio wave signal to the reception of different frequencies in the region. Enemy invasion will be associated with each other by radio, our sensors can capture these signals and passed on to one's own staff ultimately. These sensors transmit information between, on the formation of a large wireless sensor networks. Imaginary enemy to invade the region, in order to hide the combat strength, they will choose to destroy the monitoring network, they will choose the first attack node, so that soon the whole network will be paralyzed. We want to in enemy attack node while adding nodes, these nodes and the original nodes how to establish a connection is a major problem. This paper made some analysis on this issue.

3.1 Defense model design

Initial conditions: initial network N_0nodes and the node are evenly distributed in the plane of the region, when the area attacked defense process of the wireless sensor network as follows:

Add nodes: from the monitoring to the node being attacked at every predetermined time step to add a new sensor node and the connection the M sensors connected to an existing composition of the m nodes in the local world when the merit principle in accordance with the given connection. Attack wireless sensor networks, connectivity impaired, the new node must be connected to higher degree nodes, in order to avoid the connection to the isolated point of death has been destroyed. That the new node with the existing probability of nodes connected to obey:

$$\prod(k_i) = \prod_{i \in local}(k_i) \Big/ \sum_{j \in local} k_j = \frac{M}{m_0 + t} \frac{k_i}{\sum\limits_{j \in loca} k_j} \tag{1}$$

N (t) is the total number of nodes of the network. New node is the probability of m times local world, on the completion of the the added network within a time step.

Attack node: We assume that the network in each time step length node attacked probability is p, the enemy target is a relatively large degree of the node, so the entire sensor network degrees larger nodes easier enemy preferably target of attack, the probability were destroyed is bigger. Therefore, the probability of node i destroyed obey distribution:

$$\prod^{*}(k_i) = \frac{k_i}{\sum\limits_{a\in N(t)} k_a} \tag{2}$$

3.2 The theoretical basis for the derivation

According to the mean field theory, we can derive the rate of change of the moment:

$$\frac{\partial k_i}{\partial t} = m\prod(k_i) - pk_i\prod^{*}(k_i) = m\frac{M}{m_0+tp}\frac{k_i}{\sum\limits_{j\in loca} k_j} - \frac{pk_i^2}{\sum\limits_{a\in N(t)} k_a} \tag{3}$$

$0 \le p \le 1m \le M \le m_0 + t$. Here we discuss some of the characteristics of wireless sensor networks with probability p attack the above mechanisms compensation after network:

1. When $M = m$, In this case, all of the nodes in the network to add the sensing node and the local world M are connected, i.e. the new node with equal probability is connected to all the sensor nodes in the local world M. The rate $k_i(t)$of change at this time is as follows:

$$\frac{\partial k_i}{\partial t} = m\frac{M}{N(t)}\frac{1}{M} - \frac{pk_i^2}{\sum\limits_{a\in N(t)} k_a} = m\frac{M}{m_0+t(1-p)}\frac{1}{M} - \frac{pk_i^2}{N(t)<k(t)>} \tag{4}$$

$N(t)$ is the total number of the sensor of the time t network and$N(t) = m_0 + t(1-p)$,$< k(t) >$is the average number of of all sensor transmission line network of wireless sensor network node average degree. We assume that the total degree of the entire network at time t is $S(t)$.

$e(t)$is the total number of the transmission link of the network.

$$S(t) = N(t)\times < k(t) > \tag{5}$$

In addition, based on the knowledge of the wireless sensor networks available:

$$\begin{cases} \frac{de(t)}{dt} = m - p < k(t) > \\ e(t) = S(t)/2 \end{cases} \tag{6}$$

Solving:

$$S(t) = \frac{2m(1-p)}{1+p}t \tag{7}$$

Put the equation (7) into the equation (4) can be obtained:

$$\begin{aligned} &\frac{\partial k_i}{\partial t} = m\frac{M}{m_0+t(1-p)}\frac{1}{M} - pk_i\frac{k_i}{\sum\limits_{a\in N(t)} k_a} \\ &= m\frac{M}{m_0+t(1-p)}\frac{1}{M} - \frac{pk_i^2}{N(t)<k(t)>} \\ &= \frac{m}{t(1-p)} - \frac{pk_i^2(1+p)}{2mt(1-p)} \end{aligned} \tag{8}$$

The using of the initial value $k_i(t_i) = m$solution the above equation the approximate degree of monitoring network distribution

$$P(k) \to e^{-\frac{(1+p)k}{2m(1-p)}}$$

The results showed that the enemy attack network node when the preferred connection does not work, After a long evolution ($t \to \infty$) monitoring network degree distribution is an exponential distribution of the form, the entire distribution curve downward trend and increasing attack probability p, the faster the greater probability of decline.

2. When $m < M \le m_0 + t$, In this case sensors with existing sensors the newly added local node connection of the sensor in the world, in accordance with the selection of the best connection. the total number of the sensor in the network at the time t, $N(t) = m_0 + t(1-p)$, Using the above equation :

$$\begin{aligned}\frac{\partial k_i}{\partial t} &= m\frac{M}{N(t)}\frac{k_i}{\sum\limits_{j\in loca} k_j} - pk_i\frac{k_i}{\sum\limits_{a\in N(t)} k_a} \\ &= m\frac{M}{m_0+t(1-p)}\frac{k_i}{M<k(t)>} - pk_i\frac{k_i}{N(t)<k(t)>} \\ &= \frac{mk_i}{S(t)} - \frac{pk_i^2(1+p)}{2mt(1-p)})\end{aligned} \tag{9}$$

Put the equation (7) into the equation (9) can be obtained:

$$\frac{\partial k_i}{\partial t} = \frac{(mk_i - pk_i^2)(1+p)}{2mt(1-p)} \tag{10}$$

The using of the initial value $k_i(t_i) = m$solution the above Bernoulli equation to approximate the degree distribution:

$$P(k) \to e^{-\frac{k}{2m^2(1-p)}}$$

Through the analysis formulas the preferential attachment degree distribution curve slow decline with increasing p. It is worth noting that, when the time step size tends to infinity, the network is not distributed to the power rate evolution, which is due to enemy attack node is a large degree of the node, which makes the results the evolution of the network to a certain change occurred.

4 Simulation analysis

Use the software simulation analysis of the theoretical results. First, the simulation in the case of both $M = m$ and $m < M \leq m_0 + t$, Different attack probability after the destruction in the network's degree distribution curve of the important nodes. Finally, simulate both cases the diameter of the network and network efficiency. And analysis the results of the data.

4.1 Simulation analysis of the effects

Fig 1,2 shows the network is attacked in different probability. Where in the distribution of degrees distribution function to immediately select a sensor node, and its degree is exactly the probability of k. there is k nodes to establish a communication path around , through a comparative analysis add a network node with existing local world preferential attachment, can avoid attack and the loss of communication capabilities effectively. As Figure 1 shows, with a higher degree nodes of the entire network,the increase in the probability of being attacked gradually reduced, but we can see the degree distribution of the entire network does not change essentially, the other in the degree more hours no node distribution. This shows that no preferred connection when the old and new nodes connected to a broadcasting form, some unimportant edge node degree also increased, thus inevitably resulting in energy loss.

Figure 2 shows that, when connected preferential attachment work, the entire monitoring network attacks, and the large degree of node is still faster rate decrease, but through comparative analysis, we found that even in the case of deleting zero probability that the network node distribution effects but also superior to Figure 1, because the enemies are more likely to attack large node, the new node also tend to node connectivity which leads to some edge node has been increasingly marginalized. Causing low node distribution more so in fact conducive to the transmission of network information, so that each sensor to better perform their duties. Figure 1, Figure 2 shows that the model of this paper defense enemy attack, the network remained the degree distribution of the form before the attack, and this we can infer the connectivity of the network is not completely damaged. In summary, when network attacks and preferential attachment network degrees lower nodes showing significant small-world properties. Both cases the size distribution was still exponential distribution , and the distribution curve of degree with increasing attack probability p acceleration attenuation.

4.2 Monitoring network diameter and transmission efficiency of simulation analysis

First, the definition of the concept: the network diameter is the maximum distance between any two sensor network. Network transmission efficiency E is defined as the level value of the reciprocal of the distance between any two nodes i and j, i.e.

$$E = \frac{1}{N(N-1)}\sum_{i\geq j}\frac{1}{D_{ij}}$$

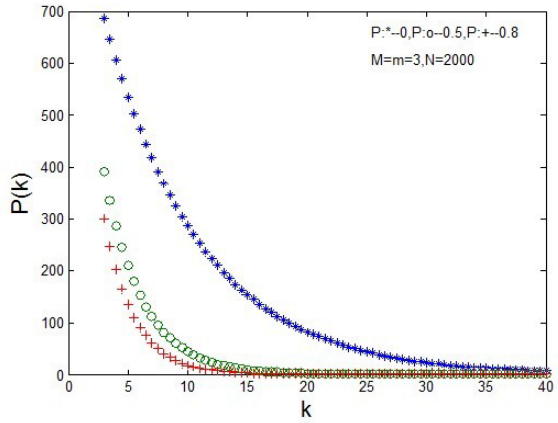

Figure 1: When M=m, the distribution curve

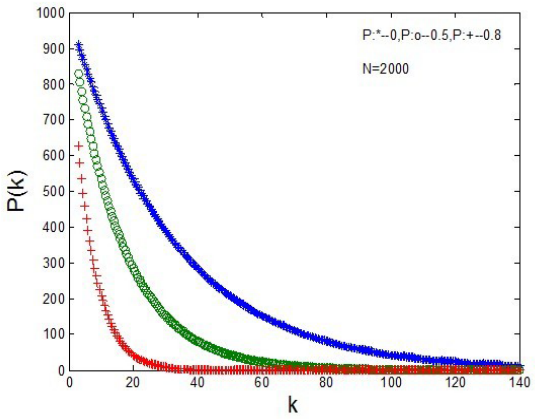

Figure 2: When $m < M < N(t)$,the distribution curve

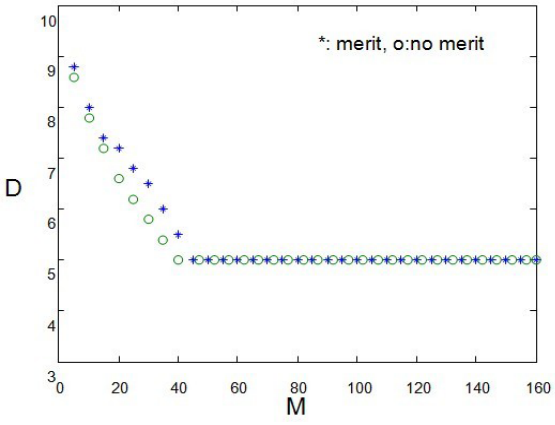

Figure 3: Local world-scale network diameter

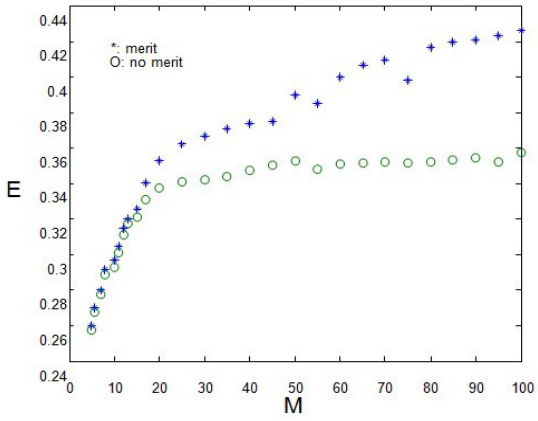

Figure 4: In both cases the local world-scale network efficiency

Network energy efficiency is used to indicate that the monitoring network receives data information, is transferred between the node data transmission efficiency.

Seen from Figure 3, when the network is under attack, preferential attachment mechanism Network moderate large sensor more likely attracted new entrants sensor, to establish communication links between them more easily, thus increasing the monitoring network clustering coefficient and reduce the diameter of the network the preferred link does not work, the clustering coefficient is relatively small. In addition, when the local world-scale increases from 5 to about 50, the diameter of the network is a sharp decline after the diameter of the network is stable at 5, which indicates that the new node when monitoring network attacks by the enemy to establish a link with the existing node reducing the diameter of the network can be to some extent compensate for the loss of important nodes being attacked. And our local world should be selected as large as possible, but when the local world, the small size to a certain extent, the diameter of the network is stuck in a certain value. This shows that the tightness between each sensor node reaches a certain level will no longer increase.

Seen from Figure 4, now, when the network after being attacked preferentially connected to the local world is larger, is conducive to the restoration of the network transmission efficiency. In particular, when the local world scale between 5-50.the monitoring of the network transmission efficiency increases rapidly. However, the size of local world increases, the efficiency of networks transmission has stabilized. The decrease in diameter of this network is reciprocal. In addition, preferential attachment mechanism works, the network transmission efficiency is greater than the network of no merit-based mechanism, and with the local world-scale increases more and more obvious.

5 Conclusion

Wireless sensor network characteristics applied to the monitoring network, and improve network performance. It is the degree distribution of the network form And transmission efficiency study. The introduction is the key parameters of the attack probability, mean field theory analysis the attack probability distribution, network diameter, network transmission efficiency. Simulation results show that the network continues to attack the preferred connection mechanism, with the increase in the probability of the attacker, the degree distribution of the network in the form remains unchanged. And the network can still maintain the basic transmission efficiency, to guard against enemy attacks on the network. Article the curve simulation software simulation, simulation of wireless sensor network evolution if we can use the simulation software platform. it will give a broader prospect of wireless sensor network, which is an important direction for future research.

References

[1] Zhu Zhengwei, Chen Zongwen. Research on Application of Wireless Sensor Network in Wind Power Generation. *Process Automation Instrumentation*, 33(05)(2012):60-63.

[2] Liu Lei, Wang Xiaoqing. Quantitative analysis on sensor number of ocean surveillance wireless sensor networks. *Electronic Measurement Technology*, 35(5)(2012):107-113.

[3] Dang Yuefang. Wireless Sensor Networks in Military Application. *Information & Communications*,35(5)(2012):153-157.

[4] Bian Qiu- xiang ,Yao Hongxing. Linear generalized synchronization of complex networks. *Systems Engineering-Theory & Practice*, 31(7)(2011):1334 - 1339.

[5] Li Shudong,Li Xiang,Yang Yixian.A local - world heterogeneous model of wireless sensor networks with node and link diversity .*Physica A , Statistical Mechanics and Its Applications*, 390(6)(2011):1182-1191.

[6] Li Xiang,Jin Yuying,Chen Guanrong. Complexity and synchronization of the world tradeWeb.*A Statistical Mechanics and Its Applications*, 328(1-2)(2003):287-296.

[7] Luo Xiaojuan,Yu Huiqun. Local-World Dynamic Evolving Network Model for Wireless Sensor Network. *Journal of East China University of Science and Technology(Natural Science Edition)*, 38(02)(2012):216-220.