Open Access

Evolutionary Model of Equipment Maintenance Support Force Networks with Partial Information

Lu Yu[1], Han Zhen[2,*], Gu Ping[2] and Chen Liyun[1]

[1]*Department of Information Engineering, Mechanical Engineering College, Shijiazhuang, Hebei, 050003, P.R. China;* [2]*Department of Equipment Command and Management, Mechanical Engineering College, Shijiazhuang, Hebei, 050003, P.R. China*

Abstract: The paper highlights the theory of complex networks, and proposes an evolutionary model to solve the evolutionary problem of equipment maintenance support force systems, which has provided partial information. Firstly, the paper applied equipment maintenance support force systems into complex networks, and defined six network parameters. Secondly, the network evolutionary steps are described. Finally, a dynamic evolutionary model whose parameters can be flexibly set, was used as the test object. The paper discusses various network parameters under three kinds of selection probability. The parameter values demonstrated feasibility of the evolutionary model, and illustrated that the model can provide auxiliary decision for commanders to develop support programs in the pre-war.

Keywords: Complex networks, Equipment maintenance support force, Evolutionary model and partial information.

1. INTRODUCTION

In the information battlefield, tasks involved in equipment maintenance and support conditions are uncertain and changeable [1], which bring high improbability in support activities. At the same time, with the emergence of perception and response support theory, the timeliness, adaptability, distribution and synergy of equipment maintenance support are facing new challenges [2]. These objectively require transition from the equipment maintenance support force systems to the complex networks.

At present, the complex networks' theory has widely been used in the industrial production systems, national power systems, urban transport systems and community management systems, *etc.* [3-7]. With the development of science and technology, its advantages will become increasingly apparent.

In wartime, the partial information of our equipment maintenance support force systems is often accessed by the enemy [8]. At the same time, their evolutionary problems have not been studied yet from the perspective of complex networks. Therefore, the paper introduced the theory of complex networks and built the evolutionary model of equipment maintenance support force networks with partial information.

2. SIMILARITY ANALYSIS

Equipment maintenance support force systems are composed of maintenance units, maintenance command structures, maintenance materials, and so on. They are constructed in accordance with the principles of comprehensive and integrated structure, interrelated function and complementary performance. It can be considered as an organic whole, which is composed of the maintenance entities, such as maintenance units, establishing the relationships between the maintenance entities. Therefore, there are many similarities between the equipment maintenance support force systems and complex networks, such as multiple entities, complex relationships and evolutionary function, etc. The complex networks' theory is introduced to equipment maintenance support force systems in the paper, revealing their evolutionary characteristics in wartime and providing auxiliary decision for commanders to develop support programs in the pre-war.

According to the description of complex networks, the maintenance entities are considered as nodes and the relationships between these entities as edges, which constitute equipment maintenance and support force networks. At the same time, because of the warfare demands of interconnection, interoperability (non-directional edges) and quick action (time restriction of the edges), the paper focused on the non-directional and weighted complex networks.

3. THE DEFINITION OF NETWORK PARAMETER

① Degree distribution

The node degree $k(i)$ is the number of nodes that are directly connected to node i. The degree of distribution reflects the probability distribution of all the nodes' degrees in the network.

② Center degree and node capability

*Address correspondence to this author at the Department of Equipment command and Management, Mechanical Engineering College, Shijiazhuang, Hebei, 050003, P.R. China; Tel: 18253453912; E-mail: hanzhenzhen1986@163.com

The center degree characterizes the degree of each node from the network center. The center degree *h*(*i*) is [9]:

$$\mathrm{h}(i) = \frac{k(i)}{N-1} \tag{1}$$

The *k*(*i*) represents the degree of node *i*, and *N*-1 represents the maximum possible number of neighbouring nodes of node *i*.

The center degree can not characterize the capability of node *i* [2]. Therefore, the capability weight $\mu(i)$ is introduced to characterize the node capability.

③ Average time of network path

The time weight w_{ij} characterizes the shortest distance between the node *i* and *j*. The average time of network path is the average value of the shortest distance between any two nodes. The average time d_{ij}^{w} is:

$$d_{ij}^{w} = \frac{2}{N(N-1)} \sum_{i,j \in N, i \neq j} w_{ij} \tag{2}$$

④ Network clustering coefficient

The node *i* has *k*(*i*) edges that connect other nodes. Actually the number of interconnected edges between the *k*(*i*) nodes is E_i. The clustering coefficient of node *i* can define c_i as :[10]

$$c_i = \frac{2E_i}{k(i)[\mathrm{k}(i)-1]} \tag{3}$$

The clustering coefficient of the entire network is:

$$C = \frac{1}{N} \sum_{i} c_i \tag{4}$$

The clustering coefficient reflects the link degree between the neighbouring nodes.

⑤ The ratio of the number of nodes in the network giant component

The network giant component is a local area that contains most of the nodes. The ratio of the number of the nodes in a network giant component is the ratio of the number of nodes between a period of time after and before in the giant component, which reflects the continued capability to maintain network connectivity. The ratio R_1 is:

$$R_1 = \left. \sum_{i=1}^{m} n_i^{'} \middle/ \sum_{i=1}^{m} n_i \right. \tag{5}$$

The denominator is the number of the nodes of *m* giant components before a period of time, and the molecule is the number of the nodes of *m* giant components after a period of time.

The ratio reflects network performance from the perspective of the number of nodes in the local area.

⑥ Network quality performance

According to the theory of entropy and the particular operation of equipment maintenance support force networks, network quality performance R_2 can be defined as follows:

$$\begin{cases} \mathrm{d}_2 = \sum_{i=1}^{N} h(i) \mathrm{n} d_3 = \sum_{i=1}^{N} \mu(i) \\ r_1 = 1 - \dfrac{-\sum_{i=1}^{N} \dfrac{h(i)}{d_2} \log_2 \dfrac{h(i)}{d_2}}{\log_2 d_2} \\ r_2 = 1 - \dfrac{-\sum_{i=1}^{N} \dfrac{\mu(i)}{d_3} \log_2 \dfrac{\mu(i)}{d_3}}{\log_2 d_3} \\ R_2 = r_1 r_2 \end{cases} \tag{6}$$

The quality performance indicates the degree of flow accuracy of the material, information and energy among the nodes. At the same time, it reflects network performance from the perspective of the accuracy of network operation.

4. NETWORK EVOLUTIONARY MODEL UNDER PARTIAL INFORMATION

Network evolutionary model has four main forms, such as increase or decrease of nodes, and increase or decrease of edges. At present, many researchers have conducted a lot of studies on the evolution of complex networks [11-13], which mainly include network evolutionary model under deliberate and random attacks. Deliberate attack is an attacking mode in which the enemy grasps all the information of the opponent troops. Random attack is an attacking mode in which enemy does not grasp the information of the opponent troop. Deliberate and random attacks are two attacking modes in extreme situation. In real battlefield, the attacking mode which is mostly adopted is the one where partial information of the opponent troop is grasped by the enemy [14, 15].

It is assumed in this study that the equipment maintenance support force networks have N nodes with the probability of information to be grasped by the enemy is *a* ($0 \leqslant a \leqslant 1$). When *a*=0, it implies that the enemy cannot obtain information, after which enemy adopts the random attack. When *a*=1, it implies that the enemy obtains all the information. The enemy adopts deliberate attack in this case. Usually, the condition is $a \in (0,1)$. At this point, the networks are divided into a known area (0, *a*] that the enemy selectively attacks based on the importance of nodes, and an unknown area (*a*, 1) that the enemy randomly attacks. These are the attacking modes under partial information.

In information warfare, in addition to the two sides of the competitors against each other in combat units, the opponents are more prone to destroy each other's logistical support networks. Equipment maintenance support force networks are a part of the logistical support networks. Therefore, there are the objects which enemy focuses on in the fight. In wartime, they are attacked that leads to the reduction of nodes and edges. At the same time, they obtain external support which lead to increase the nodes and edges.

The enemy obtains partial information and performs the following evolutionary steps:

Step 1: The initial networks are the non-directional and weighted networks, which have m_0 nodes and e_0 edges.

Step 2: The enemy attacks firstly on the networks' known area. At each equal time step, the networks follow one of the four different conditions in accordance with a certain probability.

Case 1: According to the information obtained, the enemy selectively attacks the networks, and disconnects m_a edges. This disconnection probability $q1$ is shown as:

$$q1=\frac{k(i)\big/w_{ij}}{\sum_{i=1}^{N}\sum_{j=1}^{N}\mathrm{k}(i)\big/w_{ij}} \tag{7}$$

The $k(i)$ is the degree of node i, and w_{ij} is the path time between the node i and j.

Case 2: It includes the functions of n_b nodes which are disabled with probability $q2$. The networks disconnect m_c edges that connect n_b nodes. The probability $q2$ is:

$$q2=\frac{h(i)\times\mu(\mathrm{i})}{\sum_{i=1}^{N}h(i)\times\mu(\mathrm{i})} \tag{8}$$

The $h(i)$ is the center degree of node i, and $\mu(i)$ is the capability weight of node i.

Case 3: Support institutions increase n_d nodes $v_j(j=1,2,\cdots,d)$ for the established networks with probability $q3$. The newly added nodes are arranged in the specified area, and given appropriate maintenance capability weight $\mu(j)(j=1,2,\cdots,d)$. The m_e edges are established between each new node v_j and the existing node v_i. The probability $q3$ is:

$$q3=\frac{h(\mathrm{i})\times\mu(i)/w_{ij}}{\sum_{i=1}^{N}\{h(i)\times\mu(i)/w_{ij}\}} \tag{9}$$

Case 4: The established networks increase m_f new edges. One end of the new edge is randomly connected to one node, and the other end is connected to another node with probability q4. The probability $q4$ is:

$$q4=\frac{k(i)}{\sum_{i=1}^{N}k(i)} \tag{10}$$

Step 3: Secondly, the enemy attacks the unknown area. At each equal time step, the networks follow the following one of the four different conditions in accordance with a certain probability.

Case 1: The m_k edges are deleted with probability $p1$. The probability $p1$ is:

$$p1=\frac{1}{\sum_{i=1}^{N}e_t(i)} \tag{11}$$

The denominator is the number of network edges at time t.

Case 2: The n_g nodes are deleted with probability $p2$. The networks disconnect m_h edges that are connected to the n_g nodes. The probability $p2$ is:

$$p2=\frac{1}{\sum_{i=1}^{N}k_t(i)} \tag{12}$$

The denominator is the total number of network nodes at time t.

Case 3: The n_r nodes $v_j(j=1,2,\cdots,r)$ are increased with probability $p3$. The newly added nodes are arranged in the specified area, and given appropriate node capability weight $\mu(j)(j=1,2,\cdots,r)$. The m_s edges are established between each new node v_j and the existing node v_i. The probability $p3$ is as follows:

$$p3=\frac{\mu(i)}{\sum_{i=1}^{N}k_t(i)\mu(i)} \tag{13}$$

Case 4: The established networks increase m_u new edge with probability $p4$. The probability $p4$ is:

$$p4=\frac{h_t(i)}{\sum_{i=1}^{N}e_t(i)h_t(\mathrm{i})} \tag{14}$$

5. SIMULATION EXAMPLE

In this study, firstly the traditional equipment maintenance support force network is taken as an example, followed by the calculation of evolutionary parameters. Secondly, the paper designs a dynamic network that is used as the network with partial information. Finally, its evolutionary parameters are simulated.

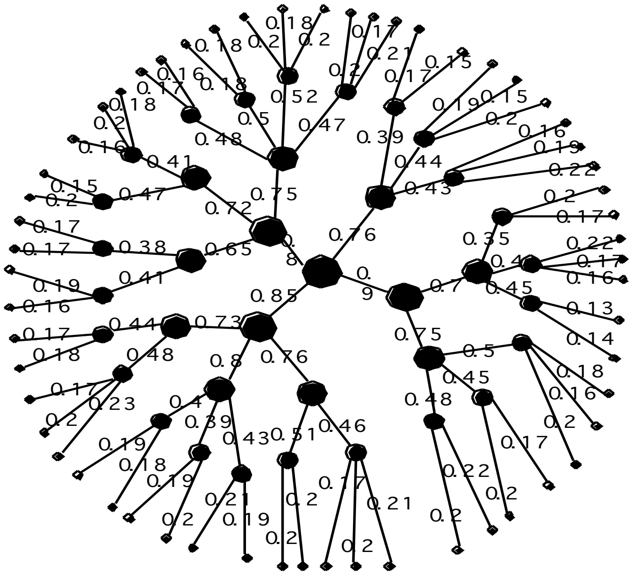

Fig. (1). The network topology.

Table 1. Evolutionary parameters of the traditional network.

Number of Nodes	Number of Edges	Average Time of Network Path	Network Clustering Coefficient	Network Quality Performance
94	93	0.5474	0	0.108

Table 2. Values of selection probability and evolutionary values of edges and nodes.

	Evolution	Selection Probability	Evolutionary Values
Unknown area under random attack	reducing edges	$q1 = 0.6 \sim 0.8$	$m_a = 5$
	reducing nodes	$q2 = 0.4 \sim 0.5$	$n_b = 2 \;\; m_c = 5$
	increasing nodes	$q_3 = 0.1 \sim 0.4$	$n_d = 1 \;\; m_e = 4$
	increasing edges	$q4 = 0.4 \sim 0.6$	$m_f = 3$
Known area under deliberate attack	reducing edges	$p1 = 0.2 \sim 0.3$	$m_k = 3$
	reducing nodes	$p2 = 0.1 \sim 0.15$	$n_g = 1 \;\; m_h = 4$
	increasing nodes	$p3 = 0.1 \sim 0.2$	$n_r = 2 \;\; m_s = 7$
	increasing edges	$p4 = 0.2 \sim 0.3$	$m_u = 9$

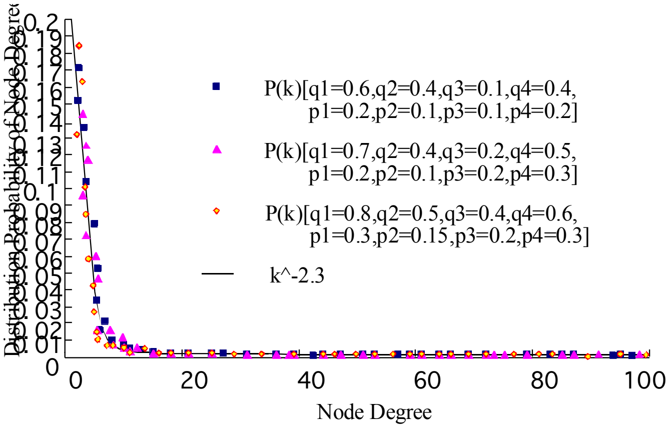

Fig. (2). Degree distribution statistics of the network.

As shown in Fig. (**1**), the maintenance entities are considered as nodes and the relationships among maintenance entities are taken as edges, with the sizes of nodes reflecting the capability of the entities, and the value on an edge reflecting the path time between the two nodes, which constitute an equipment maintenance support force network. According to the above definition of network parameters, the paper uses Lingo software to calculate the parameters. The results are shown in Table **1**.

The enemy adopts deliberate attacks as the attacking mode against the known area. The network has a certain capability to defend and camouflage, therefore, the probability of being attacked is 100%. The enemy adopts random attacks as the attacking mode against the unknown area. Because of the commander's capability and high-performance weapon, the probability of being attacked is not too low. Considering the above situations, the paper sets the values of selection probability and evolutionary values of edges and nodes, which are shown in Table **2**.

Assuming that the simulation time is 100 steps, in order to eliminate the influence of random factors in the simulation, the paper carried out 10 separate simulations for each simulation, and then these results were averaged.

6. THE ANALYSIS OF SIMULATION RESULTS

Degree distribution is carried out statistically at the end of the simulation whose results are shown in Fig. (**2**). These results are close to the curve $P(k)=k^{-a}$(a=2.3) under three kinds of selection probabilities. Therefore, degree distribution of the network follows a $a\approx 2.3$ power-law distribution, and the network has scale-free characteristics.

As shown in Fig. (**3**), the average time of the network path experiences the reduction after the first increase under three kinds of selection probabilities. It illustrates that the network, from deliberate attacks to random attacks, experiences reduction in the number of edges and nodes from greater to less than the increase in the number of edges and nodes. The increase in the rate of decreasing edges and nodes

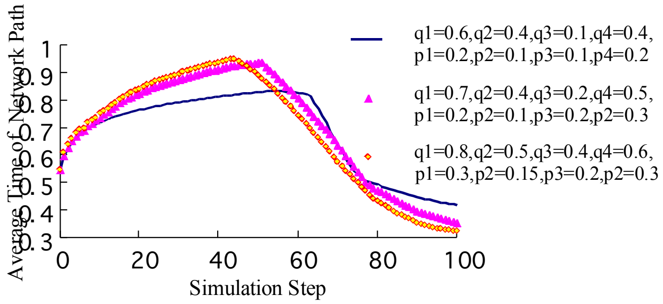

Fig. (3). Average time of network path.

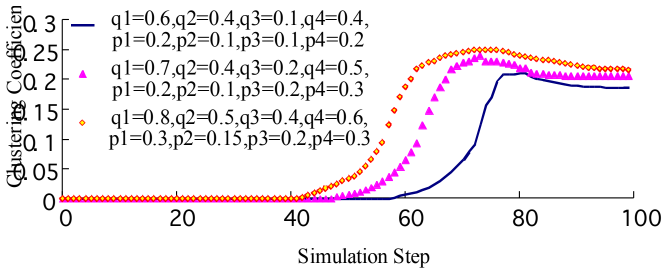

Fig. (4). Network clustering coefficient.

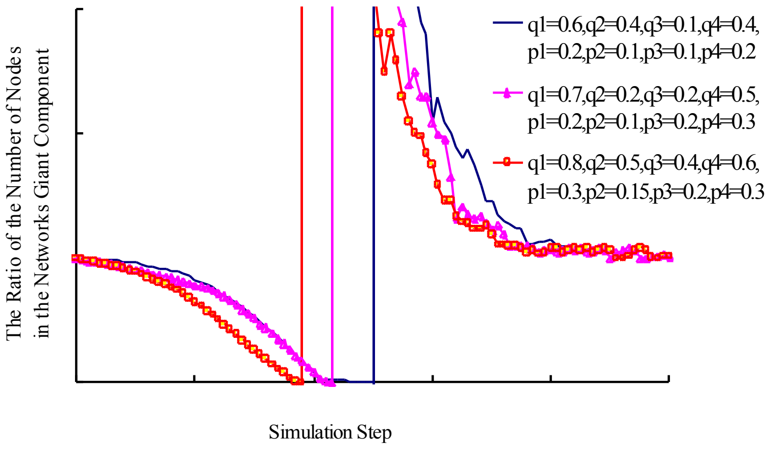

Fig. (5). The ratio of the number of nodes in the network giant component.

is due to the increased rate of average time of the network path and its maximum value. At the same time, with the increased rate of increasing edges and nodes, the reduction rate of the average time of the network path gradually increased. The average time of the network path is less than its initial value at the end of the simulation. Therefore, the dynamic network is more rapid compared to the traditional network in terms of the support speed.

As shown in Fig. (**4**), the initial value of clustering coefficient is zero in the traditional network. With the simulation progress, network clustering coefficient remains near zero. The reason is that the number of network nodes and edges is in the reduced state. Later, network clustering coefficient increases rapidly due to constant addition of the nodes and edges. Finally, the network clustering coefficient stabilizes, and then the network maintains the balance on the number of nodes and edges entering and exiting.

The network has a short average time of network path shown in Fig. (**3**), and has a large clustering coefficient shown in Fig. (**4**). Therefore, the network has the characteristics of 'small-world" networks.

As shown in Fig. (**5**), the ratio of the number of nodes in the network giant component is steadily reduced in the beginning for a period of time under three kinds of selection probabilities. The reason is that a large number of nodes and edges are constantly eliminated from the network. When the simulation step is 38, the ratio of the number of nodes in the giant component experiences transition in q1=0.8. The number of nodes and edges entering the network is greater than the number of nodes exiting the network. Secondly, the ratios begin to gradually reduce, but their value is above 1. Finally, these ratios fluctuate in the vicinity of 1, till the moment the network maintains the balance in terms of the number of nodes and edges entering and exiting the network, and the connectivity of the network becomes steady.

Because of deliberate attacks from the enemy, a large number of nodes and edges exit the network. With random attacks, the number of nodes and edges entering the network

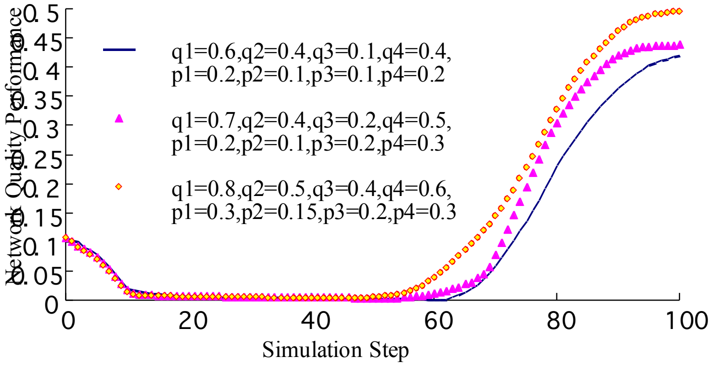

Fig. (6). Network quality performance.

is greater than the number of nodes exiting the network. As can be seen from Fig. (**6**), the network quality performance is reduced in the beginning for a period of time. When reduced to a certain extent, it becomes steady. After a certain time it gradually increases.

As can be seen from Figs. (**5** and **6**), network performance experiences a gradual reduction in the beginning. To a certain extent, it fluctuates in the vicinity of its minimum value. It gradually increases after a certain simulation step, then the fluctuation in the vicinity becomes stable with fixed performance value.

From the above analysis, a more realistic evolutionary model can be obtained by setting flexible parameters. It can be concluded that the proposed evolutionary method is feasible.

CONCLUSION

In reality, the proposed method is only known for designing equipment maintenance support force networks based on partial information, to analyze their evolution. The paper puts forward an evolutionary model with partial information. It shows the evolutionary law of the networks under different conditions by adjusting parameters, and reveals the evolutionary characteristics in wartime. The above simulation results prove the feasibility of the evolutionary model, and illustrate that the model can provide auxiliary decision for commanders to develop support programs in the pre-war. For the next stage, the researchers aim to further improve the current evolutionary model.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work was financially supported by the National Natural Science Foundation of China under Grant No.61271152.

REFERENCES

[1] H. Xu, W. P. Wang and C. L. Chen, “State space modelling of materiel maintenance support systems in wartime,” *Journal of System Simulation*, vol. 20, pp. 1139-1142, 2008.

[2] Y. G. Xu, J Qiu and G. J. Liu, “Dynamic evolution model of equipment maintenance organizational structure based on multielement-weighted network,” *Acta Armamentaria*, vol. 33, pp. 488-496, 2012.

[3] H. Okhravi and D. M. Nicol, “Application of trusted network technology to industrial control networks,” *International Journal of Critical Infrastructure Protection*, vol. 2, pp. 84-94, 2009.

[4] M. Jalili, “Social power and opinion formation in complex networks,” *Physica A*, vol. 392, pp. 959-966, 2013.

[5] O. Mulken and A. Blumenan, “Continuous-time quantum walks: Models for coherent transport on complex networks,” *Physics Reports*, vol. 502, pp. 37-87, 2011.

[6] S. Gourley and N. F. Johnson, “Effects of decision-making on the transport costs across complex networks,” *Physica A*, vol. 363, pp. 82-88, 2006.

[7] X. F. Wang, X. Li and G. R. Chen, “Complex network theory and its application,” In: *Proceedings of Qing Hua University*, pp. 1-8, 2006.

[8] B. Lopez, A. Pla and D. Daroca, “Medical equipment maintenance support with service-oriented multi-agent services,” *Lecture Notes in Computer Science*, vol. 7057, pp. 487-498, 2012.

[9] R. Albert and A. L. Barabasi, “Statistical mechanics of complex networks,” *Reviews Modern Physics*, vol. 74, pp. 47-97, 2002.

[10] M. Annunziato, I. Bertini and S. Pizzuti, “Evolving complex neural networks,” *Lecture Notes in Computer Science*, vol.4733, pp. 194-205, 2007.

[11] R. Albert, H. Jeong and A. L. Barabasi, “Error and attack tolerance of complex networks,” *Nature*, vol. 406, pp. 378-382, 2000.

[12] R. Cohen, K. Erez and D. Ben-avraham, “Breakdown of the internet under intentional attack,” *Physical Review Letters*, vol. 86, pp. 3682-3685, 2001.

[13] M. Jalili, “Error and attack tolerance of small-worldness in complex networks,” *Journal of Informetrics*, vol. 5, pp. 422-430, 2011.

[14] P. Chen, X. F. Wu and Y. Li, “Attack strategy for uncertain topology of complex networks,” *Application Research of Computers*, vol. 27, pp. 4622-4623, 4629, 2010.

[15] J. Wu, Y. J. Tan and H. Z. Deng, “Model for invulnerability of complex networks with incomplete information based on unequal probability sampling,” *Systems Engineering-Theory & Practice*, vol. 30, pp. 1207-1217, 2010.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014