TELKOMNIKA, Vol. 13, No. 4, December 2015, pp. 1242~1250
ISSN: 1693-6930, accredited A by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v13i4.3104

Influence of Sensor Nodes on the Invulnerability of Tree Network

Lifeng Jiang[1,2,a*], Fengming Zhang[1,b], Rennong Yang[3,c], Kun Xu[2,d]
[1]Institute of Equipment management and safety Engineering, Air Force Engineering University, Xi'an 710051, China
[2]Air Force Aviation University, Changchun, 130022, China
[3]Aeronautics and Astronautics Engineering College, Air Force Engineering University, Xi'an 710038, China
e-mail: redish3737@163.com[a], zfm@163.com[b], yrn@163.com[c], xk@163.com[d]

Abstract

In the transformation process from the complex system of great industrial era to the information era, the component having sensing function plays an important role in the evolution of complex system. To abstract the complex system of "tree" structure as "tree" network, To abstract the components include the component having sensing function as nodes, and how the sensor nodes in the network affect network invulnerability is studied quantitatively in this paper. Firstly, the experimental program for network invulnerability is designed; secondly, the indicators for measuring the network invulnerability and the importance of node are proposed; then, the invulnerability experiments are carried out in two conditions-with or without sensor nodes in "tree" network; finally the experimental data are statistically analyzed. Results show that after the addition of sensor nodes, the invulnerability of "tree" network is promoted when subject to random attack and particular attack. The research results are of reference significance for improving self-invulnerability in the transformation process from complex system to information. The experimental program and the relevant conclusions obtained by experiment in this paper have certain innovation.

Keywords: *invulnerability, complex system, sensor*

Copyright © 2015 Universitas Ahmad Dahlan. All rights reserved.

1. Introduction

When the complex system in large industrial era makes the transformation to meet the needs of the information era, to enhance the ability of the system to obtain information is one of the important purposes of the transformation. If the sensor with the ability to obtain information can be used as component to be integrated into the complex system, it will have a positive impact on information transformation. However, such component cannot only enhance the ability to obtain information of the system, but also have impact on the invulnerability of system by changing the way of information interaction between the components in the system. Because the invulnerability of system directly determines the viability of the system in a specific external environment, it has great significance to study it. Currently, some achievements have been made in the research of system invulnerability. And in particular, the research method by the abstraction from complex system to complex network and the study in invulnerability has been proved effective. However, the researches on the relationship between the component and the invulnerability of system are not much. Based on the existing researches, experimental program in the invulnerability of complex system is designed from the perspective of network, the indicators for measuring the network invulnerability and the importance of node are proposed, the invulnerability experiments are carried out in two conditions-with or without sensor nodes in "tree" network, and based on the experimental data, the invulnerability relationship between sensor and the complex system is analyzed. The results of Experiment show that the components of the system can affect the invulnerability of the system, the research from this point is a important supplement to existing research methods.

Received September 16, 2015; Revised November 4, 2015; Accepted November 17, 2015

2. State of the Art

At this stage, the research on invulnerability of the system is mainly reflected in the following three aspects:

(1) Research on how to build network model of complex system [1]-[4], the network model has a characteristic of small-world network model [5] or scale-free network model [6].

(2) According to the research requirements to design experimental program of invulnerability and getting various types of data required for the research of invulnerability from the experiment [7]-[9].

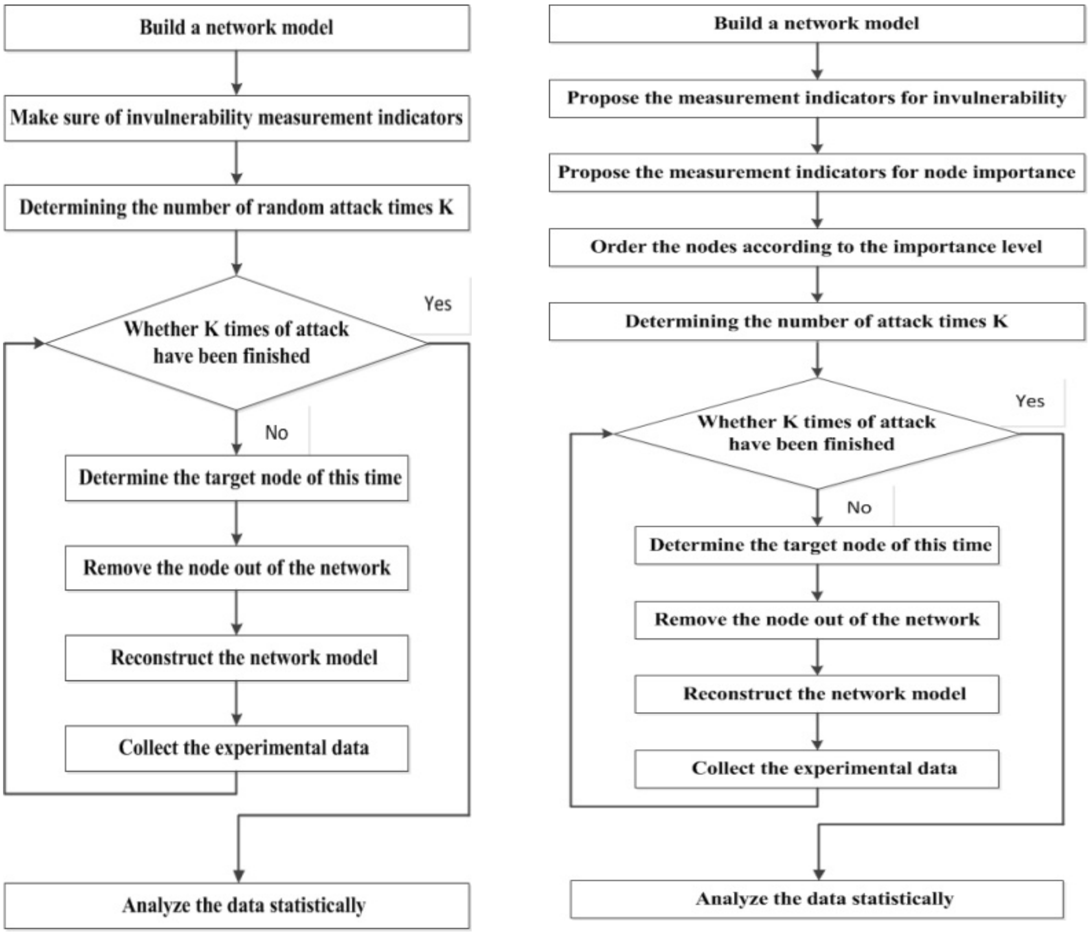
(3) Research on the measure of invulnerability [10]-[12], especially the research for large scale complex system has made important achievements [13]-[15].

The existing results are mainly studied the topology structure on the impact of the invulnerability, however the research on the relationship between component and invulnerability is not much, but this is the key point of the paper.

3. Method

3.1. Experimental Program for Invulnerability Based on Random Attack Strategy

Random attack strategy means to randomly select several nodes that compose network with equal probability as attack targets when attacking the network. A network with N nodes is subject to random attack by ten times in the experiment. Figure 1(a) shows a flowchart of the experimental program.


Build a network model
Make sure of invulnerability measurement indicators
Determining the number of random attack times K
Whether K times of attack have been finished
Yes
No
Determine the target node of this time
Remove the node out of the network
Reconstruct the network model
Collect the experimental data
Analyze the data statistically
Build a network model
Propose the measurement indicators for invulnerability
Propose the measurement indicators for node importance
Order the nodes according to the importance level
Determining the number of attack times K
Whether K times of attack have been finished
Yes
No
Determine the target node of this time
Remove the node out of the network
Reconstruct the network model
Collect the experimental data
Analyze the data statistically

(a) Random attack experiment

(b) Particular attack experiment

Figure 1. Flowchart of experiment

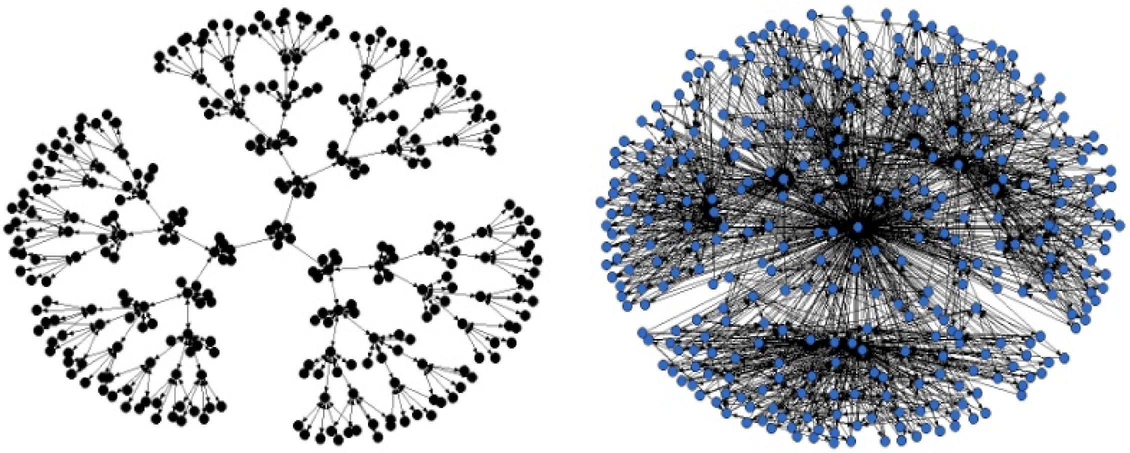
3.2. Experimental Program for Network Invulnerability Based on Particular Attack Strategy

Particular attack strategy means to select more important network nodes as prior targets when attacking the network. The key of this strategy lies in how to order the nodes in terms of their importance to determine the order of particular attack according to a standard. Figure 1(b) shows the flowchart of the experimental protocol.

3.3. Preparation of the Experiment

3.3.1. Build Network Model

It is supposed that there are 300 nodes after the complex system of “tree” structure is abstracted as a network model, and these nodes are divided into two categories: one is command-issue node, of which the function is to issue behavior instructions to their corresponding action nodes, 50 totally (denoted by C); the other is action node, 250 totally (denoted by A), of which the function is to execute the instructions from command-issue node. The command-issue nodes of each level can exchange information between upper and lower levels. And all the action nodes of each level can only exchange information with corresponding command-issue nodes, and ultimately can establish a network model of “tree” structure. Figure 2(a) shows two-dimensional view of the network model of “tree” complex system.



(a) “Tree” network

(b) “Tree” network with addition of sensor nodes

Figure 2. Two-dimensional view of network model

The network model containing sensor nodes can be established based on “tree” network model. Through study in the positions and functions of real complex system sensors, the introduction of sensor nodes can derive the following assumptions: sensor nodes belong to command-issue nodes within the sub-network; sensor nodes can monitor all the nodes within the sub-network except for command-issue nodes; the sensor nodes of the upper command level can monitor all the nodes of lower levels that are subject to the control of command-issue nodes within the same sub-network; sensor nodes only transmit the collected information to the command-issue nodes from the same sub-network.

Finally “tree” network model with sensor nodes can be built, of which the 2D view is shown in Figure 2(b).

3.3.2 Indicators for Measuring Network Invulnerability and Nodes Importance Level

The indicators for measuring network invulnerability used in the paper are the relative size and network relevance.

Network relevance: a measure of the relevance of each node in the network. The formula is as follows:

$$C = 1 - \left[\frac{V}{N(N-1)/2} \right] \quad (1)$$

V is the number of the nodes that are not reachable in network;

N is the scale of the network.

Relative size: the ratio of the number of network nodes in the maximum sub-network after the attack to the number of network nodes that are not subject to attack.

3.3.3. Determination of the Attack Times and the Order of the Network Nodes

(1) Determination of the attack times

Random attack needs to be conducted by 10 times in the invulnerability experiment of two network models based on random attack strategy, and the probabilities of being attacked for the node are 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90% and 100% respectively.

In the invulnerability experiment based on particular attack strategy, the "tree" network without addition of sensor nodes attacks 5 nodes of the network one time, with 10 times of particular attack in the experiment; the "tree" network with addition of sensor nodes attacks 10 nodes one time, with 10 times of particular attack in the experiment.

(2) Order of the network nodes in terms of importance

The nodes of two network models are ordered according to the degree centrality levels. For the "tree" network without addition of sensor nodes, only the first 50 nodes in the importance are listed, because the experiment is carried out 10 times and only 5 nodes are attacked one time. Table 1 shows the order of the "tree" network nodes according to the sum values of the in-degree and out-degree of degree centrality. For the "tree" network with addition of sensor nodes, only the first 100 nodes in the importance are listed, because the experiment is carried out 10 times and only 10 nodes are attacked one time. Table 2 shows the order of the "tree" network nodes with addition of sensor nodes according to the sum values of the in-degree and out-degree of degree centrality.

Table 1. Order of "tree" network nodes in terms of degree centrality

Node	Out-degree	In-degree
C19, C20, C21 and C22	9.000	9.000
C1, C2, C3, C4, C5, C6, C7, C8, C9, C10, C11, C12, C13, C14, C15, C16, C17 and C18	8.000	8.000
C23, C24, C25, C26, C27, C28, C29, C30, C31, C32, C33, C34, C35, C36, C37, C38, C39, C40, C41, C42, C43, C44, C45, C46, C47, C48, C49 and C50	6.000	6.000

Table 2. Order of degree centrality of the "tree" network with addition of sensor nodes

Network node	In-degree	Out-degree
S1	349	1
S4	132	2
S3 and S2	104	2
S10	62	5
S9	62	3
S5, S6, S7 and S8	48	3
S21 and S22	34	4
S19 and S20	27	4
S11, S12, S13, S14, S15, S16, S17 and S18	20	4
C19, C20, C21 and C22	13	9
C11, C12, C13, C14, C15, C16, C17 and C18	12	8
C5, C6, C7, C8, C9 and C10	11	8
C2, C3 and C4	10	8
C1	9	8
C23, C24, C25, C26, C27, C28, C29, C30, C31, C32, C33, C34, C35, C36, C37, C38, C39, C40, C41, C42, C43, C44, C45, C46, C47, C48, C49 and C50	11	6
S23, S24, S25, S26, S27, S28, S29, S30, S31, S32, S33, S34, S35, S36, S37, S38, S39, S40, S41, S42, S43, S44, S45, S46, S47, S48, S49 and S50	5	6

3.4. Experiment

3.4.1. Random Attack Experiment

Random attack experiment can be divided into the random attack experiment of “tree” network and random attack experiment of “tree” network with the addition of sensor nodes. The procedures of two experimental parts are similar and consistent with the process shown in Figure 1(a). The experimental data of “tree” network after ten times of random attack are shown in Table 3. The experimental data of “tree” network with the addition of sensor nodes after ten times of random attack are shown in Table 4.

Table 3. Statistics of invulnerability indicators for “tree” network in random attack experiment

Attack times	Relative size	Network relevance
1	0.413	0.2342
2	0.4567	0.3681
3	0.1067	0.0378
4	0.1933	0.1166
5	0.0333	0.0197
6	0.0567	0.0275
7	0.04	0.0227
8	0.0233	0.0172
9	0.01	0.0076
10	0	0

Table 4. Statistics of invulnerability indicators for “tree” network with addition of sensor nodes in random attack experiment

Attack times	Relative size	Network relevance
1	0.8857	1
2	0.7886	1
3	0.6971	1
4	0.3086	0.3984
5	0.1971	0.2832
6	0.1314	0.1543
7	0.3143	1
8	0.0457	0.1337
9	0.0229	0.069
10	0	0

3.4.2. Particular Attack Experiment

Particular attack experiment can be divided into the particular attack experiment of “tree” network and particular attack experiment of “tree” network with the addition of sensor nodes. The procedures of two experimental parts are consistent with the process shown in Figure 1(b). The experimental data of “tree” network after ten times of particular attack are shown in Table 5.

Table 5. Statistics of invulnerability indicators for “tree” network in particular attack experiment

Attack times	Relative size	Network relevance
1	0.3	0.1924
2	0.14	0.0607
3	0.06	0.0317
4	0.06	0.0171
5	0.02	0.0100
6	0.02	0.0083
7	0.02	0.0064
8	0.02	0.0045
9	0.02	0.0023
10	0	0

The experimental data “tree” network with the addition of sensor nodes after ten times of particular attack are shown in Table 6.

Table 6. Statistics of invulnerability indicators for “tree” network with addition of sensor nodes in particular attack experiment

Attack times	Relative size	Network relevance
1	0,9714	1
2	0.9429	1
3	0.4	1
4	0.0686	0.0180
5	0.02	0.0123
6	0.02	0.0117
7	0.02	0.0111
8	0.0171	0.0083
9	0.0171	0.0045
10	0	0

4. Results and Analysis

4.1. Statistical Analysis of Random Attack Experiment

According to the definition relative size, it can be known that the value can be used to measure the damage degree of the main network after being attacked randomly; the value closer to 1 indicates that the main network is subject to low-level damage, and the network invulnerability is better.

Figure 3 shows that in the face of equal probability of a random attack, the damage extent of the “tree” network after the addition of sensor nodes is lower than before, when subject to a random attack, which suggests the introduction of sensor nodes can alleviate the damage of the network thus improving the network invulnerability.

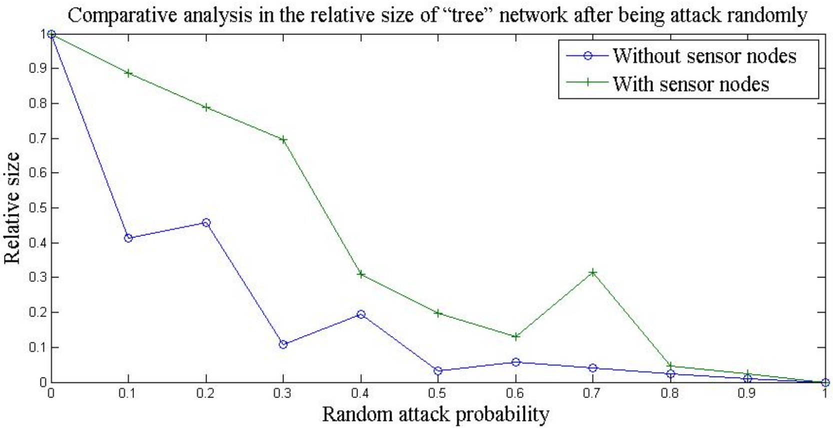


Figure 3. Comparative analysis in the relative size of “tree” network after being attack randomly before and after the addition of sensor nodes

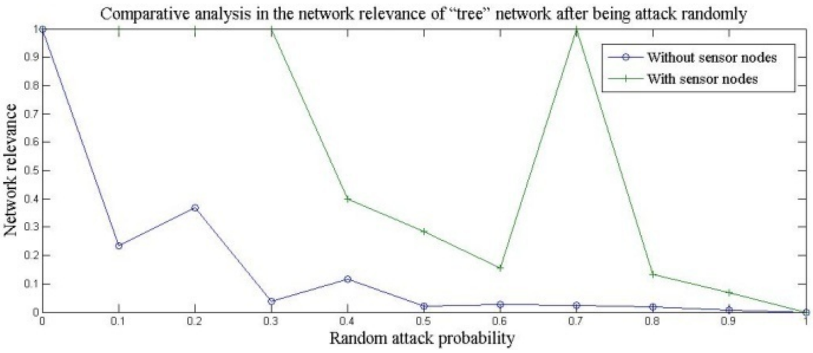


Figure 4. Comparative analysis in the network relevance of “tree” network after being attack randomly before and after the addition of sensor nodes

After the network is randomly attacked, some nodes are directly eliminated, and the other nodes become isolated ones. These nodes and the network have lost contact in information, so the nodes have been isolated outside the main network. Network relevance is used in the paper to measure the number of isolated nodes in the network, the large number of isolated nodes means higher degree of the network damage.

When the network is subject to the random attacks of different probabilities, the network relevance value of “tree” network with addition of sensor nodes is higher than before as shown in Figure 4. This indicates that the addition of sensor nodes enhances the survivability of the network.

4.2. Statistical Analysis of Particular Attack Experiment

Figure 5 shows that when subject to a particular attack, the damage extent of the “tree” network after the addition of sensor nodes is far lower than before in the first three attacks, which exhibits good invulnerability according to the definition of relative size. From the fourth attack, the damage degrees of two main networks are similar, indicating that the two have similar invulnerability.

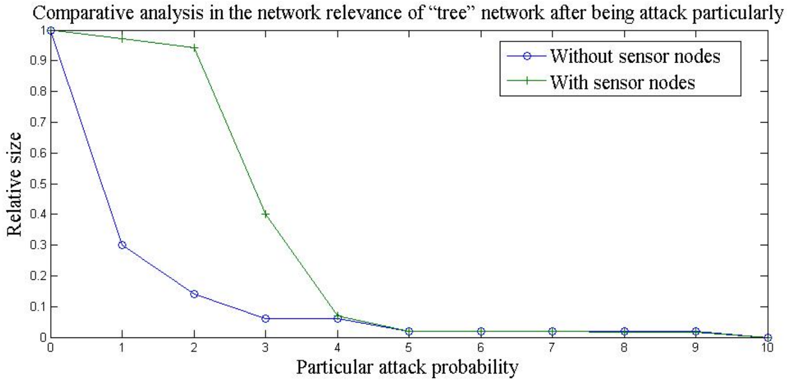


Figure 5. Comparative analysis in the relative size of “tree” network after being attack particularly before and after the addition of sensor nodes

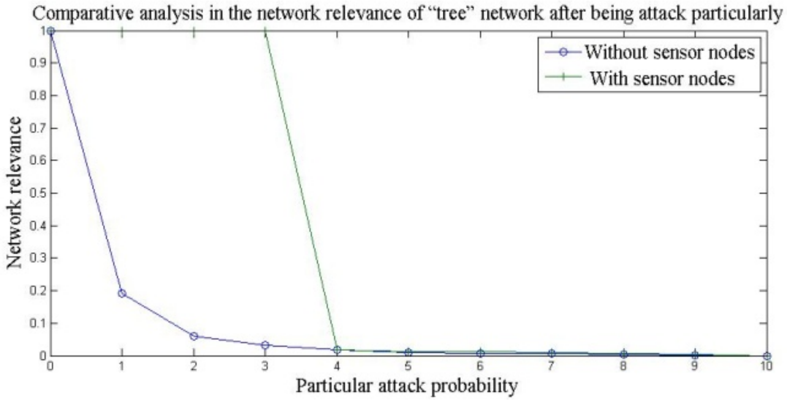


Figure 6. Comparative analysis in the network relevance of “tree” network after being attack particularly before and after the addition of sensor nodes

Figure 6 shows that when subject to a particular attack, the network with the addition of sensor nodes is less prone to generate isolated nodes compared with that without sensor nodes in the first three particular attacks, thus showing good invulnerability. From the fourth attack, the probabilities to generate isolated nodes of two main networks are similar, indicating that the two have similar invulnerability.

5. Discussion

The following conclusions can be drawn from the experiments above based on the analysis of the experimental data:

(1) After the addition of sensor nodes, the invulnerability of “tree” network is promoted when subject to random attack, mainly embodied in the decreased damage level of the main network and the decreased probability of network node to generate isolated nodes.

(2) In the “tree” network with hierarchical characteristics, the higher level of the sensor nodes means more nodes establish the information exchange relationship with them; the higher in-degree and out-degree of values of the degree centrality indicate better invulnerability promotion when subject to random attack, and vice versa.

(3) After the addition of sensor nodes, the invulnerability of “tree” network in particular attack is improved to some extent, but from the fourth attack, the addition of sensor node to the network has little effect on invulnerability. This is mainly because the important 22 sensor nodes (S1-S22) that cause the change in the information exchange relationship of network node has been destroyed after the first three attacks, and the remaining 28 sensor nodes have low out-degree and in-degree values due to the bottom location in the network, with little influence on the network invulnerability.

(4) After the addition of sensor nodes to “tree” network, the improving function in invulnerability in particular attack is not so good as that in random attack. Although the addition of sensor nodes to the network can change the exchange relationship between the information between nodes, the sensor node may become particular target of attack, as the out-degree and in-degree values of centrality are high. Once these sensor nodes are attacked, the new information exchange relationship ceases to exist, and then the promotion of invulnerability will be not effective.

(5) The addition of sensor nodes to the network can change the information exchange relationship between network nodes and has impact on the network invulnerability. This indicates that in the informatization of the complex system, the network invulnerability can be improved by optimizing the sensor node information exchange relationship with the other nodes in the network.

6. Conclusions

The relationship between sensor and the invulnerability of complex system is studied in this paper, the results show that adding new types of components to the system will have an impact on its invulnerability. The results of the research will help to further research on how to improve the invulnerability of complex system.

Acknowledgement

During the writing papers, the study was of great help Dr. Ying Zhang, to express my gratitude.

References

[1] Nasiruzzaman ABM, Pota HR. Complex Network Framework Based Comparative Study of Power Grid Centrality Measures. *International Journal of Electrical and Computer Engineering*. 2013; 3(4): 543-552

[2] Zhong PY, Shuai B, Chen GT. Model and simulation on cascading failure survivability of hazardous materials transportation network under terrorist attack. *Application Research of Computers*. 2013; 30(1): 107-110

[3] Lv JG, Guo JF, Liu YY, Zhang W, Allen J. Approaches of influence maximization in social networks with positive and negative opinitions. *Dyna*. 2015; 90(4): 407-415

[4] Lazár Ivan, Husár Jozef. Verification of sequential patterns in production using information entropy. *Tehnicki Vjesnik*. 2013; 20(4): 669-676

[5] Watts DJ, Strogatz SH. Collective Dynamics of Small-world Networks. *Nature*. 1998; 393(6684): 440-442

[6] Barabasi AL, Albert R. Emergency of Scaling in Random Networks. *Science*. 1999; 286(5439): 509-511

[7] Babaei M, Ghassemieh H, Jalili M. Cascading failure tolerance of modular small-world networks. *IEEE Transaction on Circuits and Systems-II: Express Briefs*. 2011; 58(8): 527-531

[8] Cetinkaya EK, Broyles D, Dandekar A. Modelling communication network challenges for future internet resilience, survivability, and disruption tolerance: A simulation-based approach. *Telecommunication Systems*.2011; 52(2): 751-766

[9] Albert R, Jeong H, Barabasi AL. Error and attack tolerance of complex networks. *Nature*.2000; 406:378-382

[10] Tian CG, Lu XY, Chu LS, Dong T, Li DX. Multi-Objective Transmission Network Planning with Consideration of Power Grid Vulnerability and Wind Power Accommodation. *Journal of Engineering Science and Technology Review*. 2013; 6(3):30-34

[11] Wu J, Barahona M, Tan YJ. Spectral measure of structural robustness in complex networks. *IEEE Transactions on Systems Man and Cybernetics Part A.* 2011; 41(6): 1244-1252

[12] Liu YN, Tang H, Zhao GF, Xiao YP, Xu C. Network Invulnerability Assessment Technology based on the ENI. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2013; 11(9): 4896-4903

[13] Estrada E, Hatano N, Benzi M. The physics of communicability in complex networks. *Phys Rep*.2012; 514(3): 89-119

[14] Shang YL. Local natural connectivity in complex networks. *Chin Phys Lett. 2011;* 28(6): 068903

[15] Wu J, Tan SY, Tan YJ, Deng HZ. Analysis of Invulnerability in complex networks based on natural connectivity. *Complex Systems and Complexity Science*. 2014: 11(1): 77-86