A Dynamic Network Robustness Evaluation Method in Cyberspace Based on Perron-Frobenius Eigenvalue

Yin Wang[1,2]
[1]Tsinghua University
[2]Institute of Software Chinese Academy of Sciences,
Beijing, P.R. China
wangyin00@gmail.com

ZhiYu Huang
[2]Institute of Software Chinese Academy of Sciences,
Beijing, P.R. China

***Abstract*—Cyberspace has become a promising research topic in recent years. One of the key problems to be solved is to evaluate the robustness of the networked nodes, that is, how the network enhance the system performance and how to measure the contribution quantitatively, which plays a crucial role in both network plan and security sectors. In this article, we proposed two methods to measure network robustness called A-PFE and W-PFE based on Perron-Frobenius theorem. Simulations have shown that the proposed W-PFE method can effectively reflect the dynamic network robustness when the network changes. Moreover, it has the further advantage of simple calculation and clear physical concept characteristics, comparing with traditional methods such as exploratory data analysis.**

Keywords; cyberspace; network robustness; effectiveness evaluation; Perron-Frobenius

I. INTRODUCTION

The concept of cyberspace has become the hot topic recently. Although the concept of cyberspace is plastic and contentious, it can be characterized as an agglomeration of individual computing devices that are networked to one another and to the outside world [1]. The cyberspace covers physical domain, information domain as well as perceptual domain, including all information systems, civil infrastructure facilities and human beings. As a result, it has become a promising academic research sector that attracts hundreds of professors, industrial engineers as well as research institute experts. In cyberspace, weapons, devices, facilities, operators and commanders are heterogeneously networked through physical media such as optical fibers, microwave cables, GPS (global positioning system) and wireless (UHF\VHF\HF) communication methods. Network robustness is a very important parameter when establish the topology of networks or evaluate the effectiveness to combat electronic or network attacks as well as complex electromagnetic environment.

The difficulty of network robustness evaluations can be described from three aspects. Firstly, traditionally, network robustness is always analyzed qualitatively, and the quantitative methods haven't been widely used. Secondly, those existing quantitative methods mainly adopt commercial simulation tools such NS2 and OPNET or complicated evaluation methods such as exploratory data analysis. The key principles of those commercial simulation tools are to analyze communication links statistically, in order to reflect the dynamic changes of the network. However, those methods cannot straightforwardly illustrate the performance gain due to networked effectiveness. The reference [2] proposed a network robustness evaluation method based on exploratory data analysis by RAND Corporation (a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world). The method is effective to analyze the network effect, but it is too complicated and takes up a huge number of computing resources, which hinders its practical deployment. Thirdly, researchers in reference [3] describe a network robustness effectiveness evaluation method base on Perron-Frobenius Eigenvalue (PFE), and it can be shown that this method is simple and straightforward. However, when the net has a huge number of nodes, the method is not sensitive for the changes of the network structure. Moreover, it provides insufficient analysis of the dynamic performance analysis.

In this paper, we illustrate the weighted PFE (W-PFE) method to assess network robustness. Through its adjacency matrix, we calculate the dominating eigenvalue to represent the network robustness. When the net is very large and can be divided into several subnets that are not cross-linked, each subnet has a weighted eigenvalue and is summed up together to acquire the weighted-average eigenvalue. Simulations have been performed using the HLA-RTI tool, a distributed simulation tool to analyze the dynamic change of the established net in the complex electromagnetic environment. Simulations validate the correctness of the proposed W-PFE method.

II. SYSTEM ARCHITECTURE

A. *The mathematic expression of a paticular net through adjacency matrix*

Link is the basic unit in a net, which logically represents the relationship between different weapons, equipments, and people. The overall network robustness is achieved through links which connects nodes and elements. As a result, we could use the adjacency matrix to describe the network architecture. Figure 1 illustrates a typical network in cyberspace, and Figure 2 presents its adjacency matrix.

978-0-7695-4235-5/10 $26.00 © 2010 IEEE
DOI 10.1109/CyberC.2010.41

In Figure 1, each link is given a number to represent the importance of the link. For example, if the link is very useful or strong enough to counter jamming, it might be assigned a large number. On the contrary, if the link is very weak or not very important, it might be given a small number. There are five levels to show the importance of the link in this scenario, in which 5 means the most close link connection, 1 means the weakest link connection, while the value 0 represent a disconnected link.

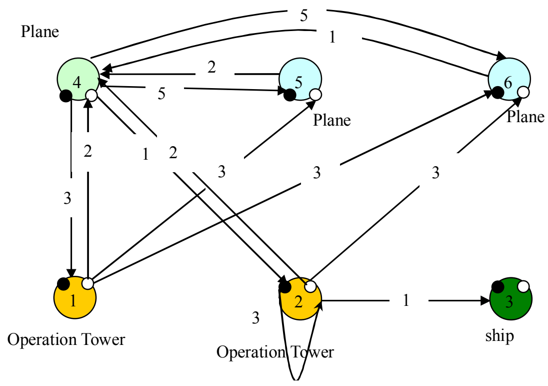


Figure 1. A typical network architecture in cyberspace

$$
\begin{array}{c}
 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6
\end{array}
\begin{array}{c}
\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\
\begin{bmatrix}
0 & 0 & 0 & 2 & 3 & 3 \\
0 & 3 & 1 & 2 & 0 & 3 \\
0 & 0 & 0 & 0 & 0 & 0 \\
3 & 1 & 0 & 0 & 5 & 5 \\
0 & 0 & 0 & 2 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0
\end{bmatrix}
\end{array}
$$

Figure 2. The adjacency matrix description of the typical network in Fig. 1

B. *The description of Perron-Frobenius Eigenvalue method*

In Figure 2, it can be found that the adjacency matrix is a "non-negative matrix", in which all the elements are non-negative real numbers. According to the famous Perron-Frobenius theorem, the matrix has a real eigenvalue whose absolute value is largest among all the eigenvalues (this eigenvalue is called the Perron-Frobenius eigenvalue.)[4]. In the PFE method, the largest eigenvalue is used to measure network robustness. It can be shown that, the larger the eigenvalue is, the higher the performance of the network. The largest eigenvalue has relationship with the size of the adjacency matrix and link levels. Therefore, we can adopt the normalized eigenvalue E_{NE} to represent the network robustness, which is defined as

$$E_{NE} = \frac{\rho_{PFE}}{N\lambda} \times 100\%. \tag{1}$$

In Equation 1, ρ_{PFE} stands for the Perron-Frobenius eigenvalue, N is the size of the $N \times N$ adjacency matrix, while λ represents the link levels. It can be easily shown that, when all the nodes are interconnected, and all the links are given the largest link level, the normalized eigenvalue E_{NE} equals to 1.

For the network shown in Figure 2, the Perron-Frobenius eigenvalue ρ_{PFE} equals to 9.20, and therefore, the normalized eigenvalue is calculated as

$$E_{NE} = \frac{\rho_{PFE}}{N\lambda} = \frac{9.20}{6 \times 5} = 30.7\%, \tag{2}$$

which is used to character the network robustness.

C. *The description of weighted-PFE method used in mutually no cross-linked network*

It has been mentioned that the proposed PFE method in the above section cannot effectively be applied in large size of network. The slight link change of a network might not reflect the E_{NE} value of the whole network. Normally, a large net can be disassembled into several mutually no cross-linked subnets [5]. As a result, each subnet can be given a weight to represent the importance of the subnet. There are two ways for weighting. One is averagely weighted, which means that each subnet share the same weight, while another method assigns each subnet the weight according to the nodes within the subnet. The former is called the A-PFE (Average PFE) method, while the latter is named as the W-PFE (Weighted PFE) method. For A-PFE, its entire network robustness, that is to say, the normalized eigenvalue is defined as

$$E_{NE} = \sum_{i=1}^{M} \frac{E_{NEi}}{M}. \tag{3}$$

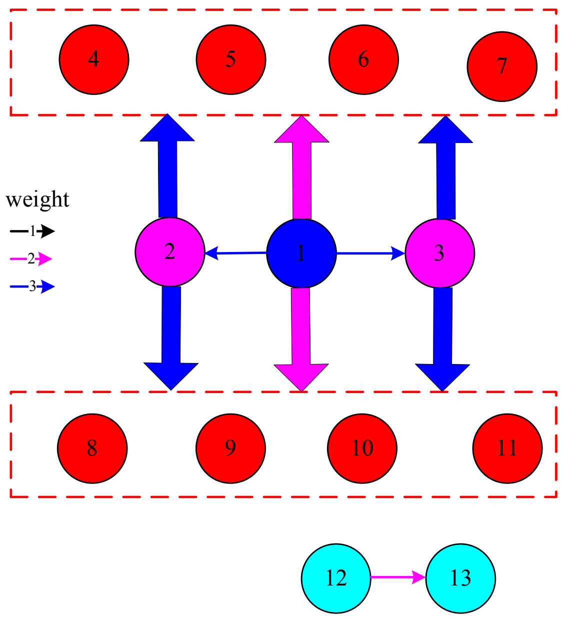
For W-PFE, E_{NE} is calculated as

$$E_{NE} = \sum_{i=1}^{M} \lambda_i E_{NEi} \quad , \tag{4}$$

in which λ_i satisfies $\sum_{i=1}^{M} \lambda_i = 1$.

III. SIMULATION VALIDATION

The concept of network is firstly proposed by the U.S. DOD (Department of defense) in order to increase the survivability of military facilities when damaged by nuclear attacks. The core idea lays in the fact that when several nodes of a network are destroyed, information can also be transported through other ways. Adaptability is the basic ability of the future network in cyberspace. It means that when confront disruptive power or in the complicated electromagnetic environment, the network can automatically adjust the network structure, communication routes, etc. to adapt this change. As a result, to evaluate the dynamic network robustness is in an emerging need. In this article, we illustrated a particular net, which is attacked on time 30 second, 90 second, 180 second and 400 second. On time 90 second and 210 second, the net adaptively adjusts its network architecture. There are 15 nodes in the network, which can be divided into A, B, C, D four no cross-linked subnets, as illustrated by Figure 3. The adjacency matrixes on time 0, 30, 90, 180, 210, 400 are shown on Figure 4. The maximum weight value of the network is 3. Simulation is based on the HLA/RTI platform to meet the characteristics of the dynamic network changes.



Net A: 1，2，3　　Net B: 1，4，5，6，7，8，9，10，11

Net C: 2，3，4，5，6，7，8，9，10，11　　Net D: 12，13

Figure 3. The topology illustration of the simulated net

Net A　Net B　Net C　Net D

$$\begin{bmatrix}
0 & 3 & 3 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

(a) 0 second

Net A　Net B　Net C　Net D

$$\begin{bmatrix}
0 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

(b) 30 second

Net A　Net B　Net C　Net D

$$\begin{bmatrix}
0 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

(c) 90 second

Net A　Net B　Net C　Net D

$$\begin{bmatrix}
0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

(d) 180 second

Net A Net B Net C Net D

$$\begin{bmatrix} 0&3&2&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&1&1&1&1&1&1&2&2&0&0&0&0\\ 0&0&0&1&1&1&1&1&1&1&1&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{bmatrix}$$

(e) 210 second

Net A Net B Net C Net D

$$\begin{bmatrix} 0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&1&1&1&1&1&1&2&2&0&0&0&0\\ 0&0&0&1&1&1&1&1&1&1&1&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{bmatrix}$$

(f) 400 second

Figure 4. Adjacency matrix illustrations of the simulated network

Simulation results have been shown in Figure 5. It can be clearly shown that, the PFE method cannot reflect the changes of the network after 30 second. Although the adjacency matrix has changed, the largest eigenvalue doesn't change significantly. The A-PFE and W-PFE method can show those changes significantly, and W-PFE method results in a more effective network robustness due to the weights are defined according to network nodes numbers. For W-PFE method, finally, the network robustness dropped from 33.2% to 8.4% due to electronic attacks.

IV. Conclusion

Cyberspace has become a promising research topic in recent years. In cyberspace, weapons, devices, facilities, operators and commanders are networked through heterogeneous physical media. As a result, to evaluate the network robustness is in emerging need for network planners as well as network security experts. In this article, we proposed two methods to measure network robustness called A-PFE and W-PFE based on Perron-Frobenius theorem. Simulations have shown that the proposed W-PFE method can effectively reflect the dynamic network robustness when it changes. Due to its simple calculation and clear physical concept characteristics, it is believed to be widely used in the near future.

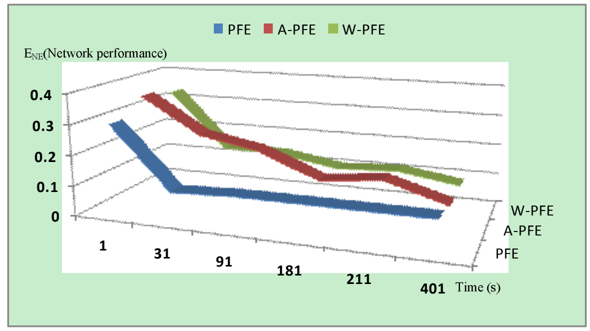


Figure 5. Dynamic network robustness evaluations using PFE, A-PFE, and W-PFE

References

[1] Martin C. Libicki. "Cyberdeterrence and Cyberwar". Http://www.rand.org.

[2] David A. Shlapak, etc. "A Question of Balance, Political Context and Military Aspects of the China-Taiwan Dispute". Http://www.rand.org.

[3] Li Qing, Wang Yu, Song Mingming. "Research and Application on the Effectiveness Evaluation of Loop model of Air Defense System under Complex Environment" (in chinese), command, control and simulation, vol. 4, pp. 59-63, August 2009.

[4] ZHANG Xian-da. Matrix Analysis and Applications. Beijing: Tsinghua University Press, 2004.

[5] Y. Wang, K. Gong, and Z. W. Chen, "Theoretical analysis of performance degradation due to phase noise and I/Q imbalance in MQAMOFDM systems," in *Proc. IEEE International Conference on Communications (ICC'08)*, Beijing, China, May 2008.