Application of DEA Method in Computer Network Security Evaluation

Yan-mei Yang[1, a], Yan-ling Zhang[2,b]

[1]Computer Engineering Department, Tangshan Vocational College of Science and Technology, Tangshan, China

[2]Computer Engineering Department, Tangshan Vocational College of Science and Technology, Tangshan, China

[a]yangyanmei604@163.com, [b]zhangyanling2005@126.com

Keywords: DEA method; Computer network security; Evaluation

Abstract. Since the affectation of vulnerabilities and viruses, there will be a variety of security issues in the application process of computer network. In order to provide effective protection for computer network security, computer network security evaluation system should be established. This article will use DEA method to evaluate the security of the computer network, which will improve the level of computer network security.

1. Introduction

The development of network technology brings convenience to people's lives, but also provide convenience for network virus attacks, Trojans and some other damaging programs, which brings growing danger to computer network security [1]. It has a very important practical significance to evaluate the risk accurately and scientifically, prevent the risk effectively and reduce the loss of computer network security problems [2].

Computer network security is affected by many factors, such as intrusion, vulnerabilities, viruses, etc. These factors are related to each other, and there are complex nonlinear relationships between factors and evaluation results [3]. Traditional evaluation methods such as AHP, gray model, etc. have the characteristics of complicated operation, difficult to accurately describe the non-linear relationship, and low evaluation accuracy [4]. DEA method is the new research of operational research in various fields [5]. DEA method has strong objectivity and flexibility, which has been used successfully in various field. Since parameters don't have to be estimated in DEA method, the mathematical operation portion ease have operation and high accuracy. This article will use DEA method to evaluate the security of the computer network research, which will improve the level of computer network security.

2. Construction of Computer Network Security Evaluation Model

2.1 Data Envelopment Analysis

(1) Brief of Data Envelopment Analysis

Data envelopment analysis (DEA)is a system analysis method developed in "relative efficiency evaluation" by well-know scholar Charnes and Cooper, etc. DEA is a new field cross-over studied by operational research, management science and mathematical economics, which is an important and effective analysis tool in the field of management science and system engineering. In DEA model, there are systems called decision making units (DMU). DEA model can judge rationality and effectiveness of the individual unit inputs and outputs. DEA method is an analysis method, using linear programming to evaluate the relative effectiveness of those comparable similar units based on a number of input and output indicators. For those complex systems with multiple inputs and multiple outputs, DEA method has certain advantages.

(2) DEA mathematical model

Suppose the number of DMU is n, and the numbers of "input" and "output" are respectively m and s. xij represents the i-th input of the j-th DMU; yrj represents the r-th output of the j-th DMU. Xj=（x1j，x2j，…，xmj）T and Yj=（y1j，y2j，…，ysj）T are respectively the inputs and outputs representation of DMU. According to the evaluation thought of DEA model, linear programming model can be configured by introducing the slack variables.

$$\min \theta = V_D$$
$$s.t.\begin{cases} \sum_{j=1}^{n} \lambda_j X_j + S^- = \theta X_{j0} \\ \sum_{j=1}^{n} \lambda_j Y_j - S^+ = Y_{j0} \\ \lambda_j \geq 0,\ \ j = 1,2,\cdots,\ \ n \\ S^- \geq 0,\ \ S^+ \geq 0 \end{cases} \qquad (1)$$

Where, λ_j is a kind of combination weight of DMU; $\sum_{j=1}^{n} \lambda_j Y_j$ and $\sum_{j=1}^{n} \lambda_j Y_j$ are the input and output vectors in this weight combination. S^+ and S^- are slack variables, S^+ equals to $(s^{+1},\ s^{+2},\ \cdots,\ s^{+s})^T$, $S^{—}$ equals to $(s^{-1},\ s^{-2},\ \cdots,\ s^{-m})^T$. This model make the input as small as possible, in the situation that the output does not fall below a certain condition.

The above model is called C^2R model, which constructs function relationship in the angle of the input as small as possible while the output constant. So ,there are some linear programming problems.

1) If the optimal value equals to 1, the j0-th DMU is weak DEA efficient, otherwise weak DEA invalid.

2) If the optimal value equals to 2, and S^{*+}, S^{*-} equals to 0, the j0-th DMU is DEA effective, whereas DEA invalid.

Production set cone assumption is unrealistic or unreasonable sometimes, so it should be get rid. When the production set satisfy convexity, invalidity and minimal resistance, we can obtain BC^2 model, which meet the income scale.

$$\min \theta = V_D$$
$$s.t.\begin{cases} \sum_{j=1}^{n} \lambda_j X_j + S^- = \theta X_{j0} \\ \sum_{j=1}^{n} \lambda_j Y_j - S^+ = Y_{j0} \\ \sum_{j=1}^{n} \lambda_j = 1, \lambda_j \geq 0,\ \ j = 1,2,\cdots,\ \ n \\ S^- \geq 0,\ \ S^+ \geq 0 \end{cases} \qquad (2)$$

2.2 Evaluation Process of DEA Method

The following is the steps of DEA model applied in the evaluation of computer network security, including determining the evaluation purpose, selecting decision unit, selecting the evaluation data, evaluating computer network security and analyzing.

(1) Determine the evaluation purpose.

The evaluation purpose is the basic to ensure the successful use of DEA method, since the input and output indicators are established bade on the evaluation purpose. The determination of evaluation purpose is the key.

(2) Select decision unit.

The number of DMU is general not lower than the number of indicators, which includes input indicators and output indicators.

(3) Select the evaluation data, and calculate.

If the calculation results do not match the model assumption, the input and output indicators should to be adjusted and recalculated, otherwise the computer network security evaluation goes extremes.

(4) Evaluate computer network security.

Evaluate the computer network security based on the DEA method, then determine the scale models combining the model.

(5) Analyze

According to the evaluation findings' alalyzing of computer network security, the improvement suggestions will be improved.

3. The establishment of computer network security's index system.

3.1 Principles of index selection.

The reasonable and scientific of computer network security evaluation's index is related to the evaluation function, namely related to whether can raise the level of network security through the evaluation. In order to establish a set of sound, rational and scientific evaluation index, there are some principles should be followed.

(1) Scientific.

Only by adhering to scientific principles, the obtained information should be reliable and objective, and the evaluation results can be valid. The index system should comply with the relevant information, laws and regulations of information system security.

(2) Comprehensiveness.

Computer network security assessment is a comprehensive evaluation with multiple indicators, which should be representative, and shall be selected from all aspects of network security. Only by this, can the evaluation be reasonable.

(3) Feasibility.

In the evaluation index system, the data collection should be facilitation, and the index system should reflect things comparable. The evaluation work program should be as simple as possible, avoiding exhaustive, cumbersome and complex.

(4) Stability.

When establishing evaluation index system, the selected indicators should change regularly, and those factors who are ups and downs frequently influenced by chance factors should not be selected. The stable index can be meaningful.

3.2 Specific choice of indicator.

Computer network is a complex system, which affected by many factors. This paper will select indicators form the aspects of inputs and outputs. In principle, to the input indicators, the smaller the better, while to the output indicators, the bigger the better. The specific choice of indicators is as follows.

(1) Input indicators.

This paper selects input indicators from the aspects of management security and logical security, including safety management systems, safety training, emergency response mechanisms, data backup, data recovery, system auditing, access control, anti-virus measures, data encryption, intrusion prevention and so on.

(2) Output indicators.

Output indicators include network room security, security of supply, line safety, safety equipment, fault-tolerant redundancy and so on.

4. Empirical Analysis

Since, the computer network security is short of shared data sets, this paper collects 10 different related data sets of computer network security evaluation to conduct empirical research, represented by DMU_1, DMU_2, DMU_3, DMU_4, DMU_5, DMU_6, DMU_7, DMU_8, DMU_9 and DMU_{10} respectively.

4.1 Set the computer security level

This article will divide the computer network security level to four levels, which are Safety (A), Basic Safety (B), Insecurity (C) and Terribly Insecure (D). Set the total points to 1, and the several score of each security level is shown in Table 1.

Table 1 Computer Network Security Level

Level	A	B	C	D
Score	1~0.85	0.85~0.7	0.7~0.6	0.6~0

(1) Safety.

Safety level indicates that the network has a strong security capability, and the network application is safe. Scores of level A ranges from 0.85 to 1.

(2) Basic safety.

Basic safety level means that the network has certain ability of security, and the network application has basic security. Scores of level B ranges from 0.7 to 0.85.

(3) Insecurity.

Insecurity level indicates that the network security ability is limited, and the network application is unsafe. Scores of level C ranges from 0.6 to 0.7.

(4) Terribly Insecure.

Terrible insecure level shows that security ability is poorer, and network application security situation is grim. Scores of level D are below 0.6.

4.2 Evaluation and Analysis

In this part, the computer network security of these ten samples is evaluated by DEA model. The evaluation results are shown in Table 2, which shows the efficiency value of each sample. These ten samples are also ranked by the efficiency value.

Table 2 Evaluation Results

DMU	DMU_1	DMU_2	DMU_3	DMU_4	DMU_5	DMU_6	DMU_7	DMU_8	DMU_9	DMU_{10}
Efficiency Value	0.937	1	1	0.843	1	0.633	0.812	0.918	0.976	1
Rank	6	1	1	8	1	10	9	7	5	1

From the table 2, we can see that the efficiency value of DMU_2, DMU_3, DMU_5 and DMU_{10} are 1, which means their network safety level achieving an effective level, accounting for 40% of the sample. The safe level of DMU_1, DMU_2, DMU_3, DMU_5, DMU_8, DMU_9 and DMU_{10} is A, accounting for 70% of the total sample. The safe level of DMU4 and DMU7 is B, accounting for 20% of the total sample. DMU_6's safe level is C.

We can see that there are 70% samples are at the security level, 20% samples are at basic simple, while 10% samples are not safe. Computer network security level should have to be further improved and perfected.

5. Summary

This article selected DEA method to evaluate the computer network security. Among the samples, there are 70% in security level, 20% in basic security level, while 10% in unsafe level. Computer network security levels need to be further improved and perfected. DEA model can avoid subjective parameter estimation, which is objective, and applied in cases of small sample data. Constructing virtual network system can obtain more rational evaluation results.

References

[1] Yue Tao. Non-uniform evaluation method for network security based on DEA model. *Journal of Jilin University (Information science edition)*, 2008, 26(4).

[2] Limin Huang. Research on safety evaluation method of computer network information systems. *Shandong University*, 2004.

[3] Zhongwu Li, Liqing Chen. Application of neural networks in computer network security assessment. *Modern Electronic Technology*, 2014,10:80 to 82.

[4] Xiewei Wang. Design and application of computer network security evaluation system. *Communication Design & Application*, 2015.

[5] Ning Xia. Research on network security assessment quantitative methods. *Changchun University of Science and Technology*, 2007.