Research on Multidimensional System Security Assessment Based on AHP and Gray Correlation

Xiaolin Zhao(✉), Hao Xu, Ting Wang, Xiaoyi Jiang, and Jingjing Zhao

Beijing Institute of Technology, Beijing 100081, China
zhaoxl@bit.edu.cn

Abstract. Aiming at the problems of the network security evaluation indexes, which are one-sided and difficult to be strictly quantified, this paper proposes the multidimensional system security evaluation method based on AHP and grey relational analysis. Under the guidance of the construction principle of system security evaluation model, this paper puts the source of factors affecting network security as the criterion of dimension Division, and constructs a multidimensional system security evaluation model for environmental security, network security and vulnerability security. On this basis, this paper combines AHP and grey relational analysis theory, and evaluate system security comprehensively and quantitatively. The multidimensional system security evaluation method based on AHP and grey relational analysis can consider the relationship between qualitative and quantitative factors in system security, and it is highly logical and flexible. This method also can effectively solve the problem that system security is difficult to evaluate objectively and quantitatively, and the system security evaluation can be pushed from a simple rough comparison to a comprehensive quantitative calculation stage.

Keywords: Network security · Security assessment · Analytic Hierarchy Process · Gray correlational analysis

1 Introduction

The number of internet users in China reached 829 million, increasing 3.8 percentage points comparing with 2017 years. It is shown by "43th Statistical Report on Internet Development in China" that the internet penetration rate reached 59.6% at the end of December 2018 [1].

With the implementation of the "internet plus" plan, cyber-system security attacks will intensify and cyberspace security threats have become one of the most serious challenges that affect national security and economic development. For example, Ransomware Wannacry attacked many hospitals, companies, universities and government organization across at least 150 countries, having more than 200 thousand victims in May, 2017. In order to deal with the increasingly serious system security problems, experts believe that we need to fully consider its security during the system design phase and evaluate network system security for controlling the system security

W. Han et al. (Eds.): CTCIS 2019, CCIS 1149, pp. 177–192, 2020.
https://doi.org/10.1007/978-981-15-3418-8_13

assessment. At present, the indexes used in quantitative evaluation of network security are relatively unimportant in our country. The lack of consideration of the entire system coupled with the fact that system security is hard to be strictly quantified, which can't meet the current system security needs.

This paper intends to build a multi-dimensional system security assessment model for environment security, network security and vulnerability security based on network theory, Analytic Hierarchy Process (AHP), gray relational analysis theory (GT). AHP is used to determine the weight of each index under the guidance of this model. The gray relational analysis is used to quantitatively evaluate the network security and improve the system security analysis and calculation method. Finally, according to the needs of the experimental task, the simulation system is tested, which shows the effectiveness and feasibility of the method.

2 Related Work

From the published literature, there are some representative methods of network security assessment at home and abroad can be divided into the following three categories [2]:

The security evaluation method based on mathematic model draws on the traditional multi-objective decision theory, and aggregates multiple influencing factors to construct the evaluation function. The advantage of this method is that it can directly reflect the security, such as the traditional weight analysis method, set analysis of the law [3, 4]. But this method also has many deficiencies. For example, the core evaluation function of the structure and the choice of parameters need a unified evaluation criteria and measurement, which often reply on the help of expert knowledge and experience, inevitably with subjective factors.

On the one hand, the system security assessment method based on knowledge reasoning processes uncertainty information by means of fuzzy sets, probability theory and D-S evidence theory [5], on the other hand, by reasoning and aggregating multi-source multi-attribute information [6]. The research focus of system security assessment in knowledge reasoning are: the method based on the fault graph model, the attack tree based method [7], the privilege graph based method, the attack graph model [8], the Bayesian network based method [9], the hierarchical method [5] and so on. Compared with the traditional mathematical model, the method of system security assessment based on knowledge reasoning can simulate the human way of thinking. The evaluation process has a certain degree of intelligence to avoid the influence of human subjective factors on the objectivity of system security assessment. However, the method also have some challenges, such as the inaccessibility of reasoning rules and the combination of explosions, which make them restricted in practical application.

The system security assessment method based on data mining and pattern recognition has strong learning ability by evaluating the security of the system by mining system security modules from training samples or historical data [10]. The process of security assessment based on pattern recognition is mainly divided into two stages: building model and pattern matching. Representative studies include: support vector machine (SVM) method [11], neural network based method [12], gray relational

method [13, 14] and Hidden Markov Model based methods [15]. Although the method of system security assessment based on pattern recognition has the advantage of objectivity, it needs a large amount of training data to learn the parameters in the model. It is difficult for the general network system to obtain a large amount of data. At the same time, it is also difficult to use the evaluation method based on pattern recognition to realize the prediction of the network attack event.

The factors which affect security are gray and hierarchical for cyberspace. Analytic Hierarchy Process (AHP) [16] can reflect the evaluation results of the whole system, build multi-level and multi-dimensional evaluation which reflects the hierarchy of the system, and calculate the importance of each factor. However, AHP has defects that its subjectivity is too strong. It is based on the experience of experts, so there are some problems that are difficult to quantify. There is comparison for several traditional methods in Table 1. In order to solve the problem in these methods, this paper establishes a multi-dimensional network assessment model based on AHP and gray correlation. We add a gray-scale quantitative assessment model, which can quantify the collected data more objectively.

Table 1. Comparison for several traditional methods

Method	Data acquisition	Objectivity	Model building	Accuracy of results
Data mining	Difficult	Strong	Easy	Strong
Knowledge reasoning	Easy	Strong	Difficult	Strong
AHP	Easy	Weak	Easy	Weak
What we want?	Easy	Strong	Easy	Strong

Our Contributions

Based on AHP and gray correlation (GC) [17], this paper mainly has the following contributions:

- We established the index system of system security assessment by analyzing the internal relations among the influencing factors;
- The paper uses metasploitable2 as the experimental environment. We established a relatively standard test reference environment. The tools we used are easy to obtain;
- We calculated the overall system security assessment value by combining AHP and GC. It shows the correctness of the algorithm by comparing with other algorithms. It was tested the sensitivity of the factors affecting the algorithm.

The first part of this article is about the introduction of background and the necessity of AHP-GC. The second and third part introduces the theory and calculation method of the algorithm in detail. The fourth part is the experimental design and experimental results of the test part. The last is a conclusion.

3 Multidimensional Network Security Assessment Method Based on AHP-GC

This paper uses AHP-GC multi-dimension security assessment methods. The main process is shown as Fig. 1:

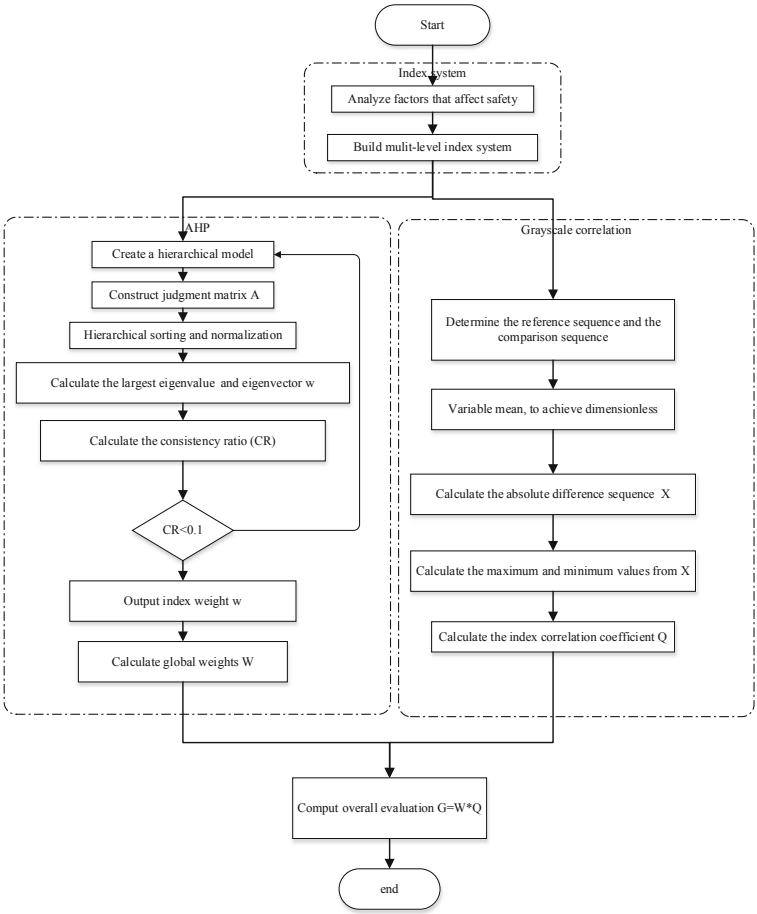

Fig. 1. Overall sequence diagram

Firstly, we need to analyze the factors that affect security, and then establish the comparison matrix between the factors according to the relationship so that AHP can be used to obtain the weight of each index following [16]. Gray correlation analysis is based on the comparison with the reference sequence to get the correlation with the ideal sequence. The correlation can be considered as the score corresponding to each index. In order to solve the security value of the whole system, it is used that the weighted average sum of the scores.

The following describes the establishment of the index model and GC method to obtain indexes of the score.

3.1 Establishment of Multidimensional System Security Assessment Index Model

Based on the classification theory of system security influence factors, this paper divides the system security into three dimensions according to the actual situation, including the host environment security, network security and vulnerability security. The multi-dimensional system security assessment model established in this paper is shown in Fig. 2. The system security includes three sub-metrics, host security, network security and vulnerability security.

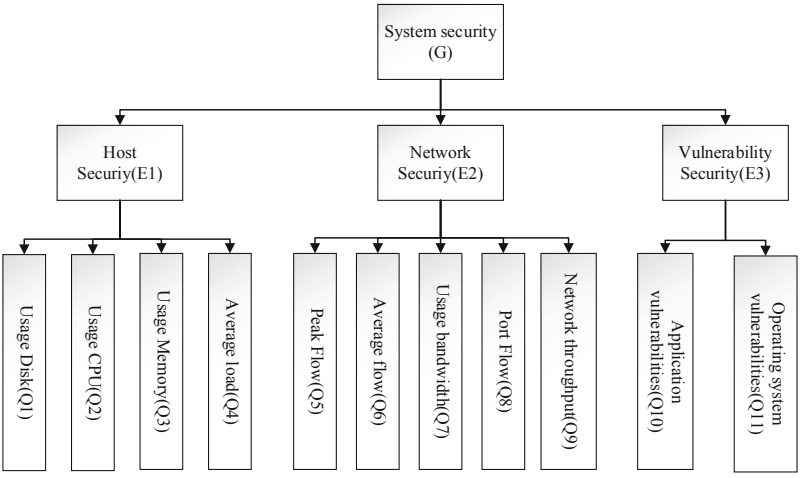

Fig. 2. Muliti-dimensional system security index system

An important factor that really threatens system security is vulnerability. So from a vulnerability perspective, we can divide system security metrics into two parts, known security and unknown security. Known security refers to security issues that have been compromised. The number of vulnerabilities can be found on CNNVD [18] and the extent of the vulnerability can be determined. Another type of security is unknown, vulnerability exists but have not been compromised. When the system is attacked by unknown security, we can only rely on the system anomaly to detect the problem, so we chose the host and network indexes to detect unknown vulnerabilities. Use vulnerability security to evaluate known vulnerabilities.

After the index system is established, the score of each index is collected and the weight of each index is calculated. Finally, the security index of the entire system is obtained through the weighted average calculation method, and the global index is between 0 and 1. The closer the result value is to 1, the safer it is. In order to have a better judgement on the security of the system, we can set the level of security for the system (Table 2).

Criteria for evaluation mainly from the service and vulnerability point of view. If there is a high-risk vulnerability, the system is in an insecure state. If the system is completely out of control, such as crashing, being shut down, etc., it may be receiving a DDOS attack or a great potential for unknown vulnerability. Therefore, it should also be considered as insecure.

The following describes in detail the use of the GC evaluation method of calculating the value.

3.2 Network Security Quantitative Evaluation Method Based on Gray Correlation Analysis

The network security quantitative assessment process based on gray relational analysis can be roughly divided into four steps: determining the analysis sequence, Nondimensionalizing variables, calculating the correlation coefficient and calculating the gray relational degree.

(1) Determine the analysis sequence
The basic idea of gray relational analysis is to determine whether the relationship is close according to the similarity of the geometric shapes of the sequence curves. Therefore, when using gray relational analysis to quantify a qualitative problem, problem is analyzed as a sequence on the basis of qualitative analysis at first. And then we need to determine multiple variables to construct a reference sequence and some comparison sequences as formula 1,

$$\mathbf{X}_i = \{x_i(1), x_i(2), \ldots, x_i(m)\} \, (i = 0, 1, 2, \ldots, n) \tag{1}$$

among then, $x_i(k)$ represents the value of the k-th index in the sequence $\mathbf{X}_i$, among which $\mathbf{X}_0$ is defined as the reference sequence and other vectors $\mathbf{X}_i(i = 1, 2, \ldots, n)$ are defined as the comparison sequences. $\mathbf{X}_0$ is a template for comparison and also an ideal standard of comparison. $\mathbf{X}_0$ can be constructed using the best values of multiple indexes. A comparison sequence is the data sequence consisting of factors that affect the behavior of the system.

(2) Nondimensionalize variables
In the constructed sequence of analyzes, the units of measurement and the orders of magnitude of the various evaluation indexes are not the same in general, but the different dimensions and orders of magnitude are inconvenient for comparison or it is difficult to draw the correct conclusions when comparing. Therefore, there are incompatibilities in the original data. It can't be directly evaluated. In order to reflect the real situation as much as possible and ensure the reliability of the analysis results, the original data of each evaluation index needs to be treated without dimension before the comprehensive evaluation, which is said as dimensionless variables. In this paper, the method of averaging is used to nondimensionalize the analysis sequence. As is shown in formula 2, the basic idea is to use the average of all the data in the analysis sequence as the denominator of the sequence to re-determine the analysis sequence.

$$x_i^{'}(k) = \frac{x_i(k)}{\bar{x}_i} \tag{2}$$

where, $\bar{x}_i$ is the average of the factors of $\mathbf{X}_i$.

(3) Calculate the correlation coefficient

The correlation coefficient is the degree of association between the node pairs in the geometric curves of the reference sequence and the comparison sequence, and the formula is as shown in Formula 3. The correlation coefficient of the *k*th indexes is,

$$\delta_i(k) = \frac{\Delta \min + \rho \Delta \max}{\Delta x_i(k) + \rho \Delta \max} \tag{3}$$

where, $\Delta x_i(k) = |x(k) - x_i(k)|$ is the value of the *k*-th data of the absolute difference sequence. Absolute difference sequence is an analytical sequence composed of the absolute value of the difference between the reference sequence and the comparison sequence. As is shown in formula 4, *n* sets of evaluations constitute *n* absolute difference sequences, and each set of evaluations is composed of *m* indexes.

$$\Delta \mathbf{X}_i = \{|x(1) - x_i(1)|, \ldots, |x(m) - x_i(m)|\}(i = 1, 2, \ldots n) \tag{4}$$

Δmax, Δmin respectively represent the maximum and minimum values in the *n* absolute difference sequences, and their calculation methods are shown in Eqs. 12 and 13.

$$\Delta \max = \max_i(\max(\Delta \mathbf{X}_i)) \tag{5}$$

$$\Delta \min = \min_i(\min(\Delta \mathbf{X}_i)) \tag{6}$$

ρ called the resolution coefficient, the value ρ is generally in the interval (0, 1), the smaller the value, the correlation coefficient between The greater the difference, the stronger the resolution. When the value ρ is less than 0.5463, the resolution is the strongest. Therefore, the usual value ρ is 0.5.

(4) Calculate the gray relational degree

Since the correlation coefficient is the degree of association between the reference sequence and the comparison sequence in each node of the geometric curve, when the correlation degree between the reference sequence and the comparison sequence is compared, the correlation coefficient obtained is more than one. The excessively scattered information makes the overall comparison unusually difficult. Therefore, we need to integrate the reference sequence and the comparative sequence in the geometric curve of each node in the degree of association value. That is the integration of correlation coefficient set as a value. As the reference sequence and comparison of the number of correlation between the sequence of numbers, this value is called gray Correlation.

When calculating the gray relational degree, the index weight can be introduced to combine the correlation coefficient with the hierarchy weight, and the formula for calculating the gray relational degree r is shown in Formula 7. Among them, $\omega(k)$ represents the weight value of the kth evaluation index in the analysis sequence, and the weight of each index satisfies Formulas 8 and 9.

$$r = \sum_{k=1}^{m} \omega(k)\delta(k) \tag{7}$$

$$\omega(k) \in [0, 1] \tag{8}$$

$$\sum_{k=1}^{m} \omega(k) = 1 \tag{9}$$

The gray relational value reflects the size of the correlation between the reference sequence and the comparison sequence. The closer the value is to 1, the greater the correlation between the comparison sequence and the reference sequence is. In this paper, we choose the optimal value of each index in the historical data of the network to build a reference sequence. The closer the value of gray relation is to 1, the better the security of the network to be evaluated.

4 Experimental Design and Analysis

4.1 Experimental Environment Configuration and Index System Interpretation

In order to verify the effectiveness and feasibility of AHP and GC multi-dimensional system security assessment, we set up the experimental environment.

First of all, we need to find a recognized experimental environment, and then conduct comparative experiments.

Experimental Environment to Build. This article chooses metasploitable2 virtual machine. Metasploitable2 virtual machine is a specially Ubuntu operating system. It is designed as a security tool to test and demonstrate common vulnerability attacks. This virtual machine is compatible with VMware, VirtualBox and other virtual platforms. So this is a system which has its own vulnerability. The system can be downloaded from source forge.net [19] After the test environment is set up, we need to scan for system vulnerabilities. We use Nessus [20] for scanning. Nessus is the most widely used system vulnerability scanning and analysis software tool in the world. It can be downloaded from [20]. In addition, the status of the system is monitored to determine potential system intrusion. We use Ganglia [21] to monitor the system. Ganglia is an open source cluster monitoring project sponsored by UC Berkeley and designed to measure thousands of nodes. It can test system performance. There are websites [21] to download.

Experimental Comparison Design. The experimental environment has a lot of exploits that can be exploited, so the final score should tend to be high-risk. At the same time, we set of five experiments by repairing the system vulnerabilities and attacks system. Results of group experiments in five different groups are shown in Table 2.

We can see from the table, S3 level is the dividing line. S1 and S2 can be considered as temporary security. S4 and S5 can be considered dangerous and require warning. S1 is a relatively safe environment, and S5 shows that the worst case, the value of each index close to the maximum value. It may be lost control of computer, unable to measure system attributes such as CPU occupancy, memory usage, etc. The index is observed before The data can be collected. Through the above method to set the experimental environment and experimental control group. By comparing the results of different evaluation methods with the known experimental results to determine the accuracy of the algorithm, and comparing the results of different experimental groups of the same algorithm, the consistency test result of the algorithm is obtained.

Table 2. Experimental comparison design

Number	Level	Assessed value (x)	Assessment method
1	S1	$0.9 \leq x \leq 1$	Patch all vulnerabilities, and no attack
2	S2	$0.8 \leq x < 0.9$	Repair high-risk vulnerabilities, and there are flaws which can't be used, the system is operating normally
3	S3	$0.7 \leq x < 0.8$	Based on the experimental environment, some vulnerabilities are repaired and there are still some exploitable vulnerabilities and low-level DDOS attacks
4	S4	$0.6 \leq x < 0.7$	The default level of the experimental environment, there are high-risk vulnerability. The services are normal
5	S5	$0 < x < 0.6$	In the experimental environment, add DDOS attack to lead to service stopped

Index Interpretation and Collection. This article has 11 indexes, (Q1–Q11). It includes the statistics of the system host status information, network information and vulnerability information. For host status information, it includes hard drive usage (Q1), CPU usage (Q2), memory usage (Q3), and average system load (Q4). Q1 and Q2 have access to get the current resource usage, smaller value is better. Q2 represents the percentage of CPU that is occupied in real time during program execution, the average system load indicates the average load on the CPU. And the information contained is statistical information about the number of the processes that CPU is processing and the processes that wait for CPU for a period of time. The ideal single core load should be around 0.7.

According to the network information, the statistical indexes are Peak Flow (Q5), Average Flow (Q6), Usage bandwidth (Q7), port flow (Q8), and network throughput

(Q9). These indexes monitor traffic from different perspectives variety. Q9 monitors the status of a single port, Q10 monitors the total network operation.

According to vulnerability information, there are two indexes, application level (Q10) and system level indexes (Q11). This index is actually a vulnerability weighted score. The level and rating of the vulnerability comes from CVE.

Experimental data collected are shown in Table 3 based on the host security dimension, network security dimension and vulnerability security dimension respectively. The reference data value is the historical data information of the system to be evaluated for statistics and analysis. The optimal value of each index is extracted; and the comparative data value is the index value collected by the network in real time.

Table 3. Environmental security indexes data information table

Index	Reference	Exp1	Exp2	Exp3	Exp4	Exp5
Q1	6%	0%	8%	63%	23%	99%
Q2	3%	4%	26%	53%	0.4%	99%
Q3	36%	20%	97%	47%	36%	99%
Q4	70%	70%	50%	40%	50%	99%
Q5	2385 KB/sec	1200 KB/sec	128 KB/sec	40 MB/sec	5013 KB/sec	40 MB/sec
Q6	67 KB/sec	67 KB/sec	72 KB/sec	36 MB/sec	129 KB/sec	36 MB/sec
Q7	2%	0%	34%	99%	25%	99%
Q8	396 KB/sec	300 KB/sec	100 KB/sec	36 MB/sec	875 KB/sec	36 MB/sec
Q9	1200 KB/sec	120 KB/sec	150 KB/sec	36 MB/sec	1075 KB/sec	36 MB/sec
Q10	0	0	0	0	1	1
Q11	0	0	0	1	2	2

4.2 Data Preprocessing

In order to avoid the problem of being unable to calculate due to the different units and scales of the collected index data, the collected index data needs to be preprocessed first. Generally, data are normalized to the interval (0, 1) through dimensionless processing, and the index attributes can be monotonously reflected. We hope that the network system is the most secure state when the index value is 1, and the security state decreases with the decrease of the index value until the network system reaches the least secure state when the index value is 0. Considering the characteristics of different indexes, we will adopt different normalization methods.

For indexes Q1, Q2, Q3, Q4 and Q7, their index values vary in the interval (0, 1), and the best reference value is given. Therefore, we calculate the absolute difference between the index value and the reference value to preprocess the index, as shown in Formula 10.

$$x_i^{'} = 1 - |x_i - x_0|,\ i = 0, 1, 2, \ldots, n \tag{10}$$

Where, x_0 represents the best reference value, and x_i represents the comparison index value. And any of the treated index values is certainly in the interval (0, 1), and the closer it is to 1, the higher the security is. Obviously, $x_0 = 0$.

For indexes Q10 and Q11, we need to normalize the index value to the interval (0, 1) as shown in Formula 11 after calculating the absolute difference according to Formula 10.

$$x_i'' = \frac{x_i' - \min(x_i')}{\max(x_i') - \min(x_i')}, \; i = 0, 1, 2, \ldots, n \tag{11}$$

Where, $\min(x_i')$ is the minimum, and $\max(x_i')$ is the maximum of x_i'. And any of the treated index values is certainly in the interval (0, 1), and the closer it is to 1, the higher the security is.

For indexes Q5, Q6, Q8 and Q9, considering the large data scale span, if calculated according to formulas 7 and 8, the processed index values may be distributed at both ends of 0 and 1, unable to reflect the real security situation, and will affect the subsequent calculation. Therefore, as shown in Formula 19, the index scale is firstly reduced through logarithmic calculation to make its distribution relatively uniform, and the final normalized index value is obtained through the calculation of Formulas 10 and 11.

$$y_i = \ln(x_i), \; i = 0, 1, 2, \ldots, n \tag{12}$$

After the calculation of Formulas 19, 17 and 18, the index value y_i'' can be relatively evenly distributed in the interval (0, 1), and the closer it is to 1, the higher the security is.

4.3 Multidimensional Network Security Evaluation Index Weight Calculation

We use AHP to calculate the weight of each index. First, we give the comparison matrix of the three indexes in the criterion layer, as shown in Table 4.

Table 4. The first level index weight matrix

	E1	E2	E3
E1	1	0.5	1/3
E2	2	1	1/2
E3	3	2	1

Tables 5, 6 and 7 respectively show the pairwise comparison matrix of host security, network security and vulnerability security.

Table 5. Host security (E1) index weight table

	Q1	Q2	Q3	Q4
Q1	1	1/5	1/3	0.25
Q2	5	1	3	1
Q3	3	1/3	1	0.2
Q4	4	1	5	1

Table 6. Network security (E2) index weight table

	Q5	Q6	Q7	Q8	Q9
Q5	1	5	0.5	7	4
Q6	0.2	1	1/7	2	1
Q7	2	7	1	9	7
Q8	1/7	0.5	1/9	1	0.25
Q9	0.25	1	1/7	4	1

Table 7. Vulnerability indexes weight table

	Q10	Q11
Q10	1	1/3
Q11	3	1

After calculation and consistency test, the final weight and consistency test results of each indicator are shown in Table 8.

Table 8. Index weight and consistency validation

Criterions	Weight	Indexes	Weight	Overall weight
E1	0.1638	Q1	0.0734	0.0120
		Q2	0.3772	0.0618
		Q3	0.1378	0.0226
		Q4	0.4116	0.0674
		CR	0.0572	
E2	0.2973	Q5	0.2986	0.0888
		Q6	0.0725	0.0215
		Q7	0.4973	0.1478
		Q8	0.0390	0.0116
		Q9	0.0926	0.0275
		CR	0.0289	
E3	0.5390	Q10	0.25	0.1347
		Q11	0.75	0.4042
		CR	0	
CR	0.0032			

4.4 Result

By using AHP, we obtain the weight vector of every index $\mathbf{W} = (W_1, W_2, \ldots, W_{11})^T$. And the correlation coefficient matrix of indexes $\mathbf{\Delta} = (\boldsymbol{\delta}_1, \boldsymbol{\delta}_2, \boldsymbol{\delta}_3, \boldsymbol{\delta}_4, \boldsymbol{\delta}_5)^T$ could be calculated by using the grey correlation method, where, $\boldsymbol{\delta}_i = (\delta_i(1), \delta_i(2), \ldots, \delta_i(11))^T$ represents the correlation coefficient vector of the j-th experiment. Therefore, Formula 13 can be used to obtain the comprehensive evaluation score of the sequence.

$$\mathbf{G} = \mathbf{W} * \mathbf{\Delta}^T \tag{13}$$

Shown in Fig. 3, we draw 6 correlation curves of the analysis sequence, respectively representing one reference sequence and 5 comparative experiments mentioned in Table 4, where horizontal coordinates represent 11 indicators of multi-dimensional system security index system, and vertical coordinates represent values of preprocessed indicators. On the whole, all curves look close to the reference sequence curve, but the safer the comparison sequence, the closer the curve is to the reference sequence. After calculating, we get the correlation coefficients of every index in 5 experiments, and show them in Table 9.

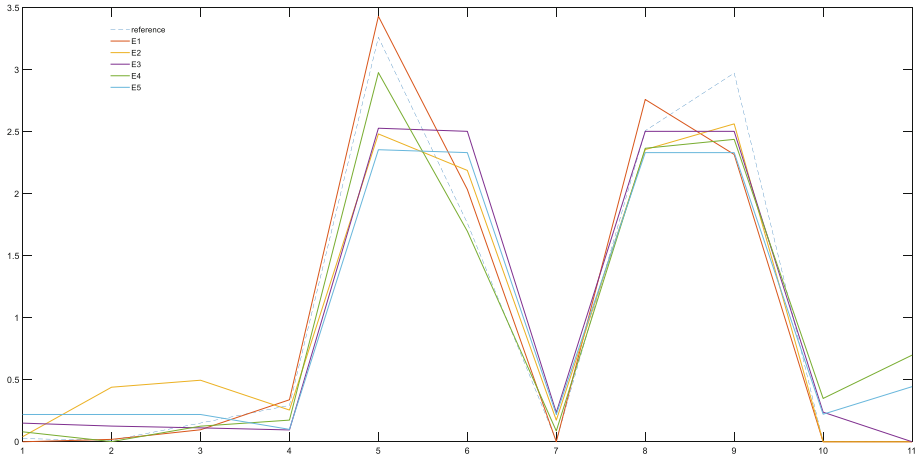

Fig. 3. Correlation curve

Table 9. Comparison of evaluation results

Number	δ_1	δ_2	δ_3	δ_4	δ_5
Q1	0.9474	0.9664	0.7836	0.8914	0.6993
Q2	0.9853	0.5146	0.7992	0.9759	0.6860
Q3	0.8932	0.5675	0.9211	0.9473	0.8678
Q4	0.9093	0.9231	0.6958	0.7922	0.7007
Q5	0.7278	0.3678	0.3820	0.6140	0.3333
Q6	0.6255	0.5162	0.3798	0.8737	0.4436
Q7	0.9818	0.7324	0.6654	0.8516	0.6816
Q8	0.6429	0.7485	0.9886	0.7617	0.7194
Q9	0.4083	0.5251	0.4908	0.4587	0.4139
Q10	1.0000	1.0000	0.6551	0.5647	0.6709
Q11	1.0000	1.0000	1.0000	0.3934	0.5048

We calculate the score of the network system states based on AHP-GC, and compare the method with AHP and AHP-Entropy [22], which are popular method to evaluate network security. The scores and security levels by different methods for different experimental states are shown in Table 10.

It is shown that various methods are basically correct for system assessment and reflect the trend of system security. At the same time, we can see that AHP-GC are better than AHP and AHP-Entropy. It shows that the AHP of gray correlation is correct.

Table 10. The scores and security levels by different methods

Number	Expected outcome	AHP-GC		AHP		AHP-Entropy	
	SL	Score	SL	Score	SL	Score	SL
1	S1	0.950	S1	0.989	S1	0.990	S1
2	S2	0.873	S2	0.861	S2	0.879	S2
3	S3	0.704	S3	0.508	S5	0.461	S5
4	S4	0.653	S4	0.398	S5	0.357	S5
5	S5	0.581	S5	0.064	S5	0.059	S5

Sensitivity Analysis

By looking at the weights of the different indexes in Table 9, you can see that all the indexes have a weight value greater than 0. 01. The smallest is 0. 0116, standing for hard drive usage and port flow. Weight values can't be too small, otherwise the role of the system's indexes will be ignored. The weight requested is within the acceptable range. The maximum weight value is 0.486, which is the system vulnerability index. This fulfil the requirements. Because vulnerabilities are the direct cause of system security. The environmental and cyber security metrics are just the performance of a vulnerability threat.

In addition, the value in host environment is changed and other is the same in Experiment 1 and Experiment 2, and the number of vulnerability is 0, which shows that the algorithm is sensitive to changes of the host environment. The host environment and network environment of Experiment 2 and Experiment 4 are basically similar. It is different from the number of vulnerabilities. It can be seen that the vulnerability assessment is sensitive and the weights are relatively large.

According to the system security assessment results in Table 10, the results of system security evaluation method written in paper are basically similar with the traditional method. The evaluation result is more accurate based on numerical correction.

Based on the analysis of the experimental results, it is verified that the proposed system security assessment method can comprehensively quantify the indexes of system security in the three dimensions of host environment security, network security and vulnerability security. It accurately and objectively evaluates the comprehensive security of the system. Therefore, the validity and feasibility of the multi-dimensional system security assessment method are verified experimentally based on AHP and gray correlation.

5 Conclusion

At present, the existing indexes of system security assessment are difficult to quantify strictly. This paper presents a multi-dimensional system security assessment method based on AHP and gray relation. The source of network security factors is taken as the criterion of dimension division under the guidance of system security assessment model construction principles. The multi-dimensional system security assessment model which includes host environment security, network security and vulnerability security is constructed to evaluate the system security synthetically.

At the same time, the method overcome the shortcomings of the traditional qualitative assessment methods and quantitative assessment methods combining the AHP and gray relational analysis to quantify the system security. It is logical and flexible to solve the problems existing in comprehensive quantitative assessment of system security Multi-level, multi-factor and non-quantitative issues. The security assessment method proposed in this paper can accurately and effectively quantify the comprehensive security of the network and avoid the subjectivity and one-sidedness of the traditional security assessment methods through experimental verification.

Acknowledgement. This work was supported by National Key R&D Program of China (Grant No. 2016YFB0800700).

References

1. China Internet Network Information Center. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201902/P020190318523029756345.pdf. Accessed 22 Sep 2019
2. Zhao, M.: Survey on technology of network security assessment. Comput. Sci. Appl. **05**(1), 18–24 (2015)

3. Chen, J.: A network security risk assessment model based on unascertained mathematics. J. Air Force Eng. Univ. **15**(2), 91–94 (2014)
4. Huang, X.: Research on network security evaluation system based on fuzzy comprehensive evaluation method. In: International Conference on Economics (2017)
5. Zhang, Y.: DS theory and hierarchical weight based network security risk assessment. Comput. Appl. Soft. **28**(11), 294–297 (2011)
6. Liu, H.: Network security evaluation model based on uncertainty reasoning. J. Acad. Armored Force Eng. **6** (2006)
7. Yao, L., Dong, P., Zheng, T., et al.: Network security analyzing and modeling based on Petri net and Attack tree for SDN. In: International Conference on Computing. IEEE (2016)
8. Yin, X., Fang, Y., Liu, Y.: Real-time risk assessment of network security based on attack graphs, vol. 92, pp. 75–80 (2013)
9. Qi, Z., Zhou, C., Tian, Y.C., et al.: A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems. IEEE Trans. Ind. Inform. **99**, 1 (2018)
10. Swarup, K.S.: Artificial neural network using pattern recognition for security assessment and analysis. Neurocomputing **71**(4–6), 983–998 (2008)
11. Wang, C., Jing, Z., Li, X.: Research on DDoS attacks detection based on RDF-SVM. In: International Conference on Intelligent Computation Technology and Automation (2017)
12. Zhang, Y.B., Yan, Z.Q.: Researches on the network security evaluation method based on BP neural network. Appl. Mech. Mater. **686**, 470–473 (2014)
13. Wang, C.Y.: Assessment of network security situation based on grey relational analysis and support vector machine. Appl. Res. Comput. **30**(6), 1859–1862 (2013)
14. Yang, J., Chen, Q.B.: Network security evaluation based on grey relation projection multi-criteria decision. Comput. Knowl. Technol. **2011**(29), 76 (2011)
15. Xiang, S., Lv, Y., Xia, C., Li, Y., Wang, Z.: A method of network security situation assessment based on hidden Markov model. In: Li, K., Li, J., Liu, Y., Castiglione, A. (eds.) ISICA 2015. CCIS, vol. 575, pp. 631–639. Springer, Singapore (2016). https://doi.org/10.1007/978-981-10-0356-1_65
16. Li, X., Xu, J., Li, D.: Index system of reliability evaluation for distribution network based on analytic hierarchy process. Proc. Chin. Soc. Univ. Electr. Power Syst. Autom. **21**(3), 69–74 (2009)
17. Tian, G., Zhang, H., Zhou, M.C., et al.: AHP, gray correlation, and TOPSIS combined approach to green performance evaluation of design alternatives. IEEE Trans. Syst. Man Cybern. Syst. **99**, 1–13 (2017)
18. CNNVD: Vulnerability information. http://www.cnnvd.org.cn/web/vulnerability/querylist.tag. Accessed 22 Sep 2019
19. rapid7user. https://sourceforge.net/projects/metasploitable/files/Metasploitable2/. Accessed 22 Sep 2019
20. Tenable. https://www.tenable.com/products/nessus-vulnerability-scanner. Accessed 22 Sep 2019
21. Ganglia: Ganglia Monitoring System. http://ganglia.info/?page_id=66. Accessed 22 Sep 2019
22. Ma, R., Ge, H., Gu, S.G., et al.: A method for determining the reference framework of network security metric index system. J. Cyber Secur. **4**(1), 67–78 (2019)