Research on Network Security Situation Assessment Model Based on Double AHP

Wei Wang[1(✉)], Xuqiu Chen[1], Wei Gan[2], Yi Yang[1], Wenxue Zhang[1], Xiantao Zhang[1], and Fan Wu[3]

[1] State Grid Chengdu Electric Power Supply Company, Chengdu 610000, China
112053432@qq.com
[2] State Grid, Sichuan Electric Power Company, Chengdu 610000, China
[3] Computer Science Department, Tuskegee University, Tuskegee, AL 36088, USA

Abstract. Network security situation assessment is an important part of the situational awareness research process and the most important thing. Situation assessment refers to the assessment of the current security status of the system through real-time analysis of network security situation awareness data and the use of appropriate models and methods. The current network boundaries are gradually disintegrating, and the power Internet is moving toward a trend of complex architecture, increased exposure of attack surfaces, and wider business scope. It is necessary to research mobile security monitoring under the zero-trust architecture to improve business security. Business hazard detection and risk prevention capabilities, and network security situation assessment are the focus of mobile security monitoring research. Aiming at the possible risks in network security, this paper proposes an improved AHP (Analytic Hierarchy Process) to comprehensively evaluate situational awareness information. First, build a single-node hierarchical analysis model based on the analytic hierarchy process inside the node, and calculate the evaluation result of the single-node equipment. Subsequently, the single-node equipment is used as a hierarchical analysis factor, and the hierarchical analysis model has been constructed again, and the situation assessment results of the distributed system composed of multiple nodes are comprehensively calculated. This network security situation assessment model based on double AHP provides a concrete and feasible scheme for the distributed system from single-point situation assessment to multi-point integration situation assessment.

Keywords: Double analytic hierarchy process · Situation assessment · Network security · Zero trust

1 Introduction

With the development of the power Internet, the network structure, scale, data, and applications have become more and more complex and diverse. The network boundary is gradually blurred, and the security problem of the power Internet has become increasingly prominent. Applying zero-trust security protection to the power mobile interconnection business can effectively build "endogenous security" capabilities and

X. Sun et al. (Eds.): ICAIS 2022, CCIS 1588, pp. 489–506, 2022.
https://doi.org/10.1007/978-3-031-06764-8_38

provide guarantees for the safe operation of the power mobile business. The implementation of continuous security monitoring for mobile networks is the cornerstone of the concept of a zero-trust security protection framework. Through continuous monitoring of the user terminal equipment environment and the user's access behavior. The monitoring of changes in environmental data can also help realize dynamic authority control. In zero-trust security protection, decision-making and disposal of potential security risks through situation assessment is the key to meeting mobile security monitoring requirements. Therefore, network security situation assessment can provide strong support for mobile network security.

Security situation assessment [1] refers to the collection, filtering, and correlation analysis of security incidents generated by network security equipment, establishing a suitable mathematical model based on constructing security indexes, evaluating the degree of security threats suffered by the network system as a whole. At present, there are many research results on network security situation assessment methods at home and abroad. As shown in Fig. 1, according to the theoretical and technical basis of the assessment basis, it can be divided into three categories, namely based on mathematical models, based on probability and knowledge reasoning, and based on pattern classification.

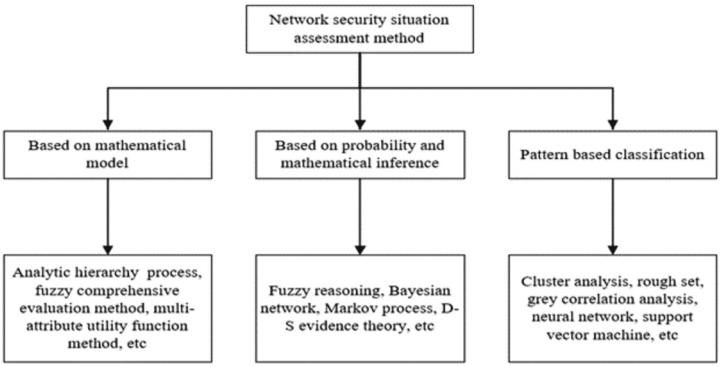

Fig. 1. Network security situation assessment method.

The methods based on the mathematical model are represented by the analytic hierarchy process [2], set pair analysis [3], fuzzy comprehensive evaluation method [4], multi-attribute utility function method [5]. It comprehensively considers the factors that affect network security situation awareness, and then establishes the corresponding relationship between the security index set and the security situation, and then assigns the situation assessment problem to issues such as multi-index comprehensive evaluation or multi-attribute set. Its disadvantage is that the evaluation model constructed by this method and the definition of its variables involve many subjective factors and lack objective unity.

The methods based on probability and knowledge reasoning are represented by fuzzy reasoning [6], Bayesian network [7], Markov process [8], DS evidence theory [9]. It builds models based on expert knowledge and experience databases and uses

logical reasoning to evaluate the security situation. The use of this method to build a model requires first to obtain prior knowledge. From the practical application point of view, the method for acquiring knowledge is still relatively single, mainly relying on machine learning or an expert knowledge base. Machine learning has the problem of operating difficulties, while an expert knowledge base mainly relies on the accumulation of experience.

The methods based on pattern classification are represented by cluster analysis [10], rough set [11], grey correlation analysis [12], neural network [13], and support vector machine [14]. It is established by training, and then the network security situation is evaluated based on the classification of the model. The advantage of this method is that the learning ability is very good, and the model is established more accurately.

The traditional network situation assessment method is usually based on the information collection module to collect the required situation awareness information and store the results in a unified database after data preprocessing. This operation of centrally and uniformly sending the situational information perceived by the security device to the central database may cause data leakage problems during the transmission process. At the same time, the concurrent upload operation of multiple devices will also have the problem of excessive network load. In addition, for the situation assessment in distributed systems, there is a lack of effective feasible schemes for the fusion calculation of single-point situation value to multi-point situation value.

Based on this, this paper proposes a double AHP analysis method based on distributed architecture to evaluate the security situation of the system. The first level of analysis will directly calculate the situation value inside the node, no longer upload the perception result information to the central database, but rely on the principle of consistency of the distributed system to synchronize the situation weight vector of the node to other nodes. Data leakage caused by direct transmission of situational awareness information is avoided. In the second level of analysis, the single-node equipment is used as the analysis factor, and the level analysis model has been constructed again and combined with the situation weight vector, the situation assessment result of the distributed system composed of multiple nodes is comprehensively calculated. This network security situation assessment model based on double AHP provides a concrete and feasible scheme for the distributed system from single-point situation assessment to multi-point integration situation assessment.

The rest of the paper is arranged as follows. In Sect. 2, the construction of the situation indicator system is introduced. Section 3 introduces the double AHP evaluation model and its improvements. Section 4 gives an example analysis of the model. Section 5 summarizes the full text.

2 Construction of the Situation Indicator System

2.1 Build a Hierarchical Network Security Situation Indicator System

A group of scholars represented by Wang Juan and Zhang Fengli [15] of the University of Electronic Science and Technology of China has established a relatively complete set of network security situation indicators with a clear level, comprehensive coverage, and strong reference. This set of indexes can cover different levels of the network, different

data sources, and different users by comparing various situation influencing factors. This article will use this as a blueprint to construct a network security situation indicator system.

Basic operating status indexes: The basic operating state index is a value calculated by collecting system operating data in a certain time window, performing quantitative evaluation on it, and calculating it. This value reflects the current operating status of the network system. Generally speaking, the larger the value, the worse the operating status of the network system. This part can select the basic operating status as the first-level indexes, and specific indexes such as the CPU usage rate, memory usage rate, and hard disk space usage rate of the security equipment as the basic operating status indexes. As shown in Table 1.

Table 1. Description of related fields of basic operating status indexes.

Index name	Description
CPU usage	Host CPU usage per unit time of node device
Memory usage	Host memory usage rate per unit time of node device
Hard disk usage	Host hard disk utilization rate per unit time of node equipment

Equipment vulnerability status indexes: The equipment vulnerability status index is a comprehensive analysis by quantifying the number of vulnerabilities and other information, and then calculating the vulnerability index, which can measure the degree of loss that may be caused to the system when the network faces an attack [16]. Generally speaking, the larger the value, the more vulnerable the network is and the greater the possibility of loss.

Table 2. Description of fields related to device vulnerability status.

Index name	Description
Header tracking vulnerability distribution	Header tracking vulnerabilities in node devices as a percentage of total vulnerabilities
SQL injection vulnerability distribution	SQL injection vulnerabilities in node devices accounted for the percentage of total vulnerabilities
Cross-site scripting vulnerability distribution	The percentage of cross-site scripting vulnerabilities in node devices to the total number of vulnerabilities
Distribution of weak password vulnerabilities	The percentage of cross-site weak password vulnerabilities in the node device to the total number of vulnerabilities

We choose the vulnerability events reported by the vulnerability scanning system as the primary indexes to obtain the hierarchical equipment vulnerability status indicators, as shown in Table 2.

Risk event indexes: Risk event indexes are mainly used to collect various security events caused by cyber-attacks within a certain time and conduct a comprehensive and quantitative assessment of the frequency and degree of harm of these incidents, and then calculate an indication of the harm caused by the network system. A numerical value of the degree. The larger the value, the deeper the degree of this hazard.

Therefore, we combine the types of network security incidents to extract various security incidents such as virus attacks, botnets, Trojan horse attacks, and denial of service as the basic indicators of the risk event indicator system. As shown in Table 3.

Table 3. Description of fields related to risk events.

Index name	Description
Virus attack distribution distribution	The percentage of virus attack incidents suffered by node equipment in unit time in total security incidents
Botnet distribution	Percentage of botnet attack incidents suffered by node devices per unit time in total security incidents
Trojan attack distribution	The percentage of Trojan horse attack incidents per unit time of node equipment in total security incidents
Denial of service distribution	The percentage of denial-of-service attack incidents that the node device suffered per unit time to the total security incidents

Threat event indexes: Threat event indicators are calculated by collecting security events caused by user violations or equipment operation over a while, and quantitatively assessing these events [17].

We can use cyber threat event indicators as the first-level indicators and use various alarm events caused by user operations or abnormal system operation as the second-level indicators to build a threat event indicator system hierarchically, as shown in Table 4.

3 Double AHP Evaluation Model

The AHP [18] was first proposed by Professor T.L.Saaty at the International Conference on Mathematical Modeling. In this method, the decision-making problem is decomposed

Table 4. Description of fields related to threat event indicators.

Index name	Description
Illegal visits	The percentage of virus attack incidents suffered by node equipment in unit time in total security incidents
Offline anomaly	The number of offline abnormalities that the node device suffered per unit time

into different constituent factors, and the factors are sorted according to the relative importance of the factors, to complete the decision-making on the target problem [19].

3.1 The First Level of Analysis

The first analytic hierarchy process obtains the situation assessment result information of the current node through the calculation of the internal perception information of the single node device, and the steps are as follows:

Establish a Hierarchical Structure Model of Equipment Nodes. From top to bottom, the target layer A, the criterion layer B, the index layer C, and the plan layer D are constructed progressively. The target layer is expressed as the purpose of decision-making, that is, the security situation of the current node equipment. The target layer is composed of an element and dominant criterion level factors B_1, B_2, B_3, B_4. The criterion layer considers various factors that can affect the current decision, including four factors: basic operating status B_1, equipment vulnerability status B_2, risk events B_3, and threat events B_4. The index level is a quantitative index that can be calculated by refining the decision-making factors of the criterion level and is limited by the corresponding factors of the criterion level. The various factors at the program level represent the results of the assessment of the node situation, including good D_1, warning D_2, and critical D_3. As Shown in Fig. 2.

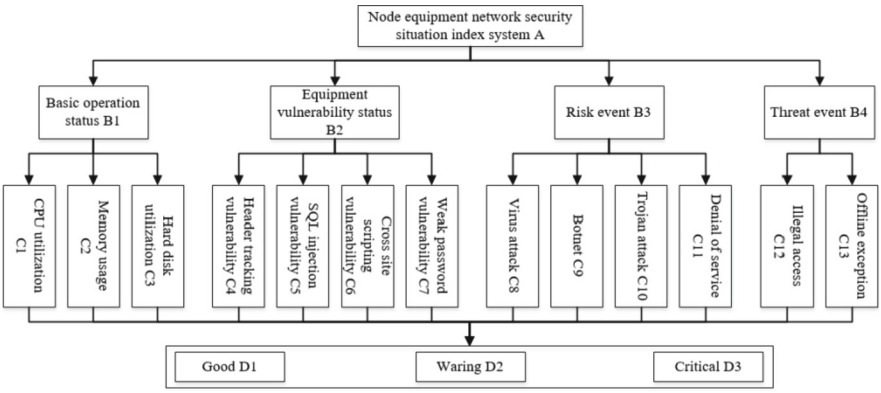

Fig. 2. Node equipment network security situation system.

Construct a Judgment Matrix. Starting from the criterion level of the hierarchical model structure, for the elements of the same level that belong to each factor of the upper level, the judgment matrix is constructed by the pairwise comparison method until the lowest level. Among them, the pairwise comparison method is the relative importance evaluation formed by comparing the factors representing this level with the factors of the upper level that are dominated by each other. Use Santy 1–9 [20] to evaluate the relative importance of each factor. The details are as follows in Table 5.

Table 5. Santy1–9 scaling method.

Value	Meaning
1	Compared with A and B, A and B are equally more important
3	Compared with A and B, A and B are slightly more important
5	Compared with A and B, A and B are obviously important
7	Compared with A and B, A and B are strongly important
9	Compared with A and B, A and B are extremely important
2,4,6,8	The degree of importance between the above two adjacent levels

According to the assignment method shown in Table 1, we can determine the value of each element of the matrix, thereby constructing the judgment matrix $A = (a_{ij})_{n\times n}$, which satisfies the following properties:

$$a_{ij}\begin{cases} = 1 & i = j \\ = \frac{1}{a_{ji}} & i, j > 0 \\ > 0 & i, j > 0 \end{cases} \tag{1}$$

Calculate the Feature Vector. After constructing the judgment matrix according to the pairwise comparison method, the normalized weights of these indicators should be obtained, that is, the feature vector W is obtained from the judgment matrix to express the relative importance of the elements of the same level to the previous element. First, use the following formula to normalize the elements in matrix A by column to obtain a column-normalized column matrix $Q = (p_{ij})_{m\times n}$:

$$p_{ij} = a_{ij} / \sum_{k=1}^{k=1} a_{ij} \tag{2}$$

The Q matrix elements are added by rows to get $\overline{W} = (\alpha_1, \alpha_2, \ldots, \alpha_m,)^T$. Subsequently use

$$w_i = \alpha_i / \sum_{k=1}^{m} \alpha_k \tag{3}$$

to calculate the feature vector $W = (w_1, w_2, \ldots, w_m)^T$.

Consistency Inspection. According to the formula:

$$CI = \frac{\lambda_{max} - m}{m - 1} \tag{4}$$

calculate the consistency index, where m is the order of the judgment matrix. According to the formula:

$$\mathrm{CR} = \frac{CI}{RI} \tag{5}$$

calculate the consistency ratio CR, which RI [21] is shown in Table 6 below.

When $CR < 0.1$, the judgment that the consistency of the matrix can be accepted, the feature vector is also desired, or required to adjust the judgment matrix until $CR < 0.1$.

Table 6. Average random consistency index

Order (m)	Average random consistency index (RI)
1	0
2	0
3	0.52
4	0.89
5	1.12
6	1.26
7	1.36
8	1.41
9	1.46
10	1.49

3.2 The Second Level of Analysis

The situation assessment result information (equipment node situation assessment weight vector) obtained by the first-fold analytic hierarchy process will be sent to other nodes in the network according to the consistency principle of the current distributed system.

Use the received situation assessment result information of other nodes and the security situation assessment result within the node to perform the second-level analysis to calculate the network security situation of the entire distributed system. The steps are as follows:

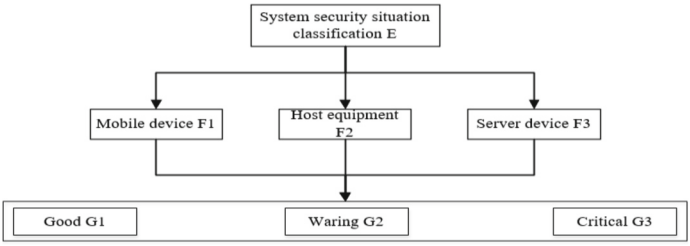

Fig. 3. System security situation classification.

Establish a Hierarchical Model of the Situational Awareness System. From top to bottom, the target layer E, the criterion layer F, and the scheme layer G are constructed progressively. The target layer is expressed as the purpose of decision-making, that is, the current security situation of the system. The target layer is composed of an element and dominant criterion level factors F_1, F_2, F_3. The factors of the criterion layer are the various sensing entities in the current sensing system, including mobile devices, host

devices, server devices, and so on. The program layer represents the evaluation results of the system, including good G_1, warning G_2, and critical G_3. As shown in Fig. 3.

Sorting of Calculation Levels. First layer calculation scheme of all the factors G_1, G_2, G_3 or the rule layer factor F_i level of a single sort $W_{F_iG} = (w_{F_iG_1}, w_{F_iG_2}, w_{F_iG_3})^T$ which

$$W_{F_iG} = W^i = \left(w_1^i, w_2^i, w_3^i\right)^T \tag{6}$$

W^i represents the weight vector of the situation assessment of the i-th device node.

Constructing the Criterion-Level Judgment Matrix. According to the different weight status of equipment assets, continue to use the pairwise comparison method to construct the judgment matrix of criterion layer F, and calculate its eigenvector $W_F = (w_{F_1}, w_{F_2}, \ldots, w_{F_i})^T$.

Total Ranking of Calculation Levels. Calculate the total ranking of the level G of the scheme $W_G = (w_{G_1}, w_{G_2}, w_{G_3})^T$, where

$$w_{G_j} = \sum_{i=1}^{\mathrm{n}} w_{F_i} w_{F_iG_\mathrm{j}} \tag{7}$$

w_{G_j} indicates the weight value of the j-th evaluation result, j = 1, 2, 3.

Consistency Inspection. According to the formula

$$CR = \frac{\sum_{i=1}^{3} w_{F_i} \times CI_i}{\sum_{i=1}^{3} w_{F_i} \times RI_i} \tag{8}$$

calculate the overall ranking consistency ratio of the hierarchy. Among them, CI_i and RI_i with that of the standard-level device i.

When $CR < 0.1$, the matrix that is determined by the consistency check, or need to adjust the ratio of high consistency judgment matrix until $CR < 0.1$;

The factor corresponding to the highest weight item in the total ranking of levels is the result of the security situation assessment of the requested system.

4 Case Analysis

This article takes a small local area network as an analysis example, and the main sensing device nodes include mobile devices, host devices, and server devices. As shown in Fig. 2, this paper mainly uses the basic operating status, equipment vulnerability status, risk events, and threat events perceived in the local area network to evaluate the situation of the internal node equipment of the network. And it establishes the situation indicator system formed by the target layer, the criterion layer, and the indicator layer.

The evaluation model takes the node equipment network security situation indicator system as the target layer C. The criterion layer includes basic operating status B_1,

equipment vulnerability status B_2, risk events B_3 and threat events B_4. The basis of the operating state B_1 can be decomposed into CPU usage C_1, memory usage C_2 and hard drive usage C_3. The vulnerability status of the device B_2 can be decomposed into four indicators: header tracking vulnerability C_4, SQL injection vulnerability C_5, cross-site scripting vulnerability C_6, and weak password vulnerability C_7. Risk events B_3 can be decomposed into virus attacks C_8, botnets C_9, Trojans attacks C_{10} and deny service C_{11}. Threat events B_4 can be divided into two indicators: illegal access C_{12} and offline abnormality C_{13}. The program layer contains three levels of good D_1, warning D_2 and critical D_3.

Because the calculation method is the same, this article only uses mobile devices F_1 as an example to calculate the weight vector of the first-level analysis situation assessment, and the other device assessment weight vectors will be directly given.

Determine the judgment matrix and weight of the situation index system according to the pairwise comparison method, establish the judgment matrix and weight vector of the evaluation factors of the first-level analysis criterion layer (as shown in Table 7) and the judgment matrix of the evaluation factors of the index layer And the weight vector (as shown in Table 8). Establish the judgment matrix and weight vector of the evaluation factors of the first level of analysis program level (as shown in Table 9).

Then calculate the combined weight W_C of each factor of the indicator layer according to the above-mentioned obtained criterion layer weight vector W_B and indicator layer weight vector $W_{B_i\_C}$:

Table 7. The judgment matrix and weight vector of the evaluation factors at the first level of the criterion layer B.

Judgment factors set at the criterion layer B	Judgment matrix	Weight vector $W_B(w_{B_i})$
$B = [B_1, B_2, B_3, B_4]$	$A\_B = \begin{bmatrix} 1.0000 & 0.3333 & 0.1667 & 0.1429 \\ 3.0000 & 1.0000 & 0.2500 & 0.2000 \\ 6.0000 & 4.0000 & 1.0000 & 0.3333 \\ 7.0000 & 5.0000 & 3.0000 & 1.0000 \end{bmatrix}$	$W_B = \begin{bmatrix} 0.0535 \\ 0.1123 \\ 0.2913 \\ 0.5429 \end{bmatrix}$

Table 8. The judgment matrix and weight vector of the evaluation factors at the first level of the index layer C.

Judgment factors set at the indicator layer C	Judgment matrix B_i_C	Weight vector $W_{B_i\_C}(w_{B_iC_j})$
$B_1 = [C_1, C_2, C_3]$	$B_1\_C = \begin{bmatrix} 1.0000 & 4.0000 & 0.5000 \\ 0.2500 & 1.0000 & 0.1667 \\ 2.0000 & 6.0000 & 1.0000 \end{bmatrix}$	$W_{B_1\_C} = \begin{bmatrix} 0.3238 \\ 0.0893 \\ 0.5869 \end{bmatrix}$
$B_2 = [C_4, C_5, C_6, C_7]$	$B_2\_C = \begin{bmatrix} 1.0000 & 0.3333 & 0.5000 & 4.0000 \\ 3.0000 & 1.0000 & 5.0000 & 6.0000 \\ 2.0000 & 0.2000 & 1.0000 & 3.0000 \\ 0.2500 & 0.1667 & 0.3333 & 1.0000 \end{bmatrix}$	$W_{B_2\_C} = \begin{bmatrix} 0.1787 \\ 0.5571 \\ 0.1996 \\ 0.0646 \end{bmatrix}$
$B_3 = [C_8, C_9, C_{10}, C_{11}]$	$B_3\_C = \begin{bmatrix} 1.0000 & 0.1429 & 0.2500 & 0.2000 \\ 7.0000 & 1.0000 & 3.0000 & 4.0000 \\ 4.0000 & 0.3333 & 1.0000 & 0.3333 \\ 5.0000 & 0.2500 & 3.0000 & 1.0000 \end{bmatrix}$	$W_{B_3\_C} = \begin{bmatrix} 0.0531 \\ 0.5319 \\ 0.1566 \\ 0.2584 \end{bmatrix}$
$B_4 = [C_{12}, C_{13}]$	$B_4\_C = \begin{bmatrix} 1.0000 & 3.0000 \\ 0.3333 & 1.0000 \end{bmatrix}$	$W_{B_4\_C} = \begin{bmatrix} 0.7500 \\ 0.2500 \end{bmatrix}$

Table 9. The judgment matrix and weight vector of the evaluation factors at the first level of the plan layer D.

Judgment factors set at the plan layer D	Judgment matrix C_jD	Weight vector $W_{C_jD}(w_{C_jD_k})$
$D = [D_1, D_2, D_3]$	$C_1\_D = \begin{bmatrix} 1.0000 & 5.0000 & 0.5000 \\ 0.2000 & 1.0000 & 0.1429 \\ 2.0000 & 7.0000 & 1.0000 \end{bmatrix}$	$W_{C_1D} = \begin{bmatrix} 0.3338 \\ 0.0755 \\ 0.5907 \end{bmatrix}$
$D = [D_1, D_2, D_3]$	$C_2\_D = \begin{bmatrix} 1.0000 & 5.0000 & 2.0000 \\ 0.2000 & 1.0000 & 0.2000 \\ 0.5000 & 5.0000 & 1.0000 \end{bmatrix}$	$W_{C_2D} = \begin{bmatrix} 0.5559 \\ 0.0904 \\ 0.3537 \end{bmatrix}$
$D = [D_1, D_2, D_3]$	$C_3\_D = \begin{bmatrix} 1.0000 & 0.3333 & 6.0000 \\ 3.0000 & 1.0000 & 9.0000 \\ 0.1667 & 0.1111 & 1.0000 \end{bmatrix}$	$W_{C_3D} = \begin{bmatrix} 0.2819 \\ 0.6583 \\ 0.0598 \end{bmatrix}$
$D = [D_1, D_2, D_3]$	$C_4\_D = \begin{bmatrix} 1.0000 & 3.0000 & 0.1429 \\ 0.3333 & 1.0000 & 0.1111 \\ 7.0000 & 9.0000 & 1.0000 \end{bmatrix}$	$W_{C_4D} = \begin{bmatrix} 0.1549 \\ 0.0685 \\ 0.7766 \end{bmatrix}$

(*continued*)

Table 9. (*continued*)

Judgment factors set at the plan layer D	Judgment matrix C_jD	Weight vector $W_{C_jD}(w_{C_jD_k})$
$D = [D_1, D_2, D_3]$	$C_5\_D = \begin{bmatrix} 1.0000 & 0.2500 & 0.2000 \\ 4.0000 & 1.0000 & 0.5000 \\ 5.0000 & 2.0000 & 1.0000 \end{bmatrix}$	$W_{C_5D} = \begin{bmatrix} 0.0982 \\ 0.3339 \\ 0.5679 \end{bmatrix}$
$D = [D_1, D_2, D_3]$	$C_6\_D = \begin{bmatrix} 1.0000 & 0.5000 & 2.0000 \\ 2.0000 & 1.0000 & 8.0000 \\ 0.5000 & 0.1250 & 1.0000 \end{bmatrix}$	$W_{C_6D} = \begin{bmatrix} 0.2584 \\ 0.6380 \\ 0.1036 \end{bmatrix}$
$D = [D_1, D_2, D_3]$	$C_7\_D = \begin{bmatrix} 1.0000 & 5.0000 & 2.0000 \\ 0.2000 & 1.0000 & 0.1667 \\ 0.5000 & 6.0000 & 1.0000 \end{bmatrix}$	$W_{C_7D} = \begin{bmatrix} 0.5455 \\ 0.0845 \\ 0.3700 \end{bmatrix}$
$D = [D_1, D_2, D_3]$	$C_8\_D = \begin{bmatrix} 1.0000 & 2.0000 & 0.2000 \\ 0.5000 & 1.0000 & 0.2500 \\ 5.0000 & 4.0000 & 1.0000 \end{bmatrix}$	$W_{C_8D} = \begin{bmatrix} 0.1925 \\ 0.1307 \\ 0.6768 \end{bmatrix}$

(*continued*)

Table 9. (*continued*)

Judgment factors set at the plan layer D	Judgment matrix C_jD	Weight vector $W_{C_jD}(w_{C_jD_k})$
$D = [D_1, D_2, D_3]$	$C_9\_D = \begin{bmatrix} 1.0000 & 2.0000 & 0.5000 \\ 0.5000 & 1.0000 & 0.1667 \\ 2.0000 & 6.0000 & 1.0000 \end{bmatrix}$	$W_{C_9D} = \begin{bmatrix} 0.2693 \\ 0.1180 \\ 0.6127 \end{bmatrix}$
$D = [D_1, D_2, D_3]$	$C_{10}\_D = \begin{bmatrix} 1.0000 & 6.0000 & 2.0000 \\ 0.1667 & 1.0000 & 0.2000 \\ 0.5000 & 5.0000 & 1.0000 \end{bmatrix}$	$W_{C_{10}D} = \begin{bmatrix} 0.5750 \\ 0.0819 \\ 0.3431 \end{bmatrix}$
$D = [D_1, D_2, D_3]$	$C_{11}\_D = \begin{bmatrix} 1.0000 & 7.0000 & 4.0000 \\ 0.1429 & 1.0000 & 0.2500 \\ 0.2500 & 4.0000 & 1.0000 \end{bmatrix}$	$W_{C_{11}D} = \begin{bmatrix} 0.6877 \\ 0.0778 \\ 0.2344 \end{bmatrix}$
$D = [D_1, D_2, D_3]$	$C_{12}\_D = \begin{bmatrix} 1.0000 & 4.0000 & 7.0000 \\ 0.2500 & 1.0000 & 1.0000 \\ 0.1429 & 1.0000 & 1.0000 \end{bmatrix}$	$W_{C_{12}D} = \begin{bmatrix} 0.7208 \\ 0.1524 \\ 0.1268 \end{bmatrix}$

(*continued*)

Table 9. (*continued*)

Judgment factors set at the plan layer D	Judgment matrix C_jD	Weight vector $W_{C_jD}(w_{C_jD_k})$
$D = [D_1, D_2, D_3]$	$C_{13}\_D =$ $\begin{bmatrix} 1.0000 & 0.5000 & 6.0000 \\ 2.0000 & 1.0000 & 5.0000 \\ 0.1667 & 0.2000 & 1.0000 \end{bmatrix}$	$W_{C_{13}D} = \begin{bmatrix} 0.3700 \\ 0.5455 \\ 0.0845 \end{bmatrix}$

$$W_C\left(w_{C_j}\right) = \begin{bmatrix} 0.0173 \\ 0.0048 \\ 0.0314 \\ 0.0201 \\ 0.0626 \\ 0.0224 \\ 0.0072 \\ 0.0155 \\ 0.1550 \\ 0.0456 \\ 0.0753 \\ 0.4072 \\ 0.1357 \end{bmatrix}, \text{where}$$

$$w_{C_j} = w_{B_i} \times w_{B_iC_j}, \{\, i | i \in [1, 4], \mathrm{i} \in N^+\}, \{\, j | j \in [1, 13], j \in N^+\} \tag{9}$$

According to the calculated solution layer weight vector W_{C_jD} and the index layer combination weightW_C, the overall ranking of the solution layer W_D is calculated as follow:

$$W_D\left(w_{D_k}\right) = \begin{bmatrix} 0.5027 \\ 0.2717 \\ 0.2256 \end{bmatrix}, \text{where}$$

$$w_{D_k} = \sum_{j=1}^{13} w_{C_j} w_{C_jD_k}, \{\, j, k | j \in [1, 13], k \in [1, 3], \mathrm{j} \in N^+, k \in N^+\} \tag{10}$$

The hierarchical total sorting W_D is the situation evaluation weight vector of the current device node, which is recorded as the weight vector ${W^{F_1}}_D$ of the device F_1, and the first level of analysis is completed.

Similarly available ${W^{F_2}}_D = \begin{bmatrix} 0.4517 \\ 0.2105 \\ 0.3378 \end{bmatrix}$,${W^{F_3}}_D = \begin{bmatrix} 0.6521 \\ 0.3110 \\ 0.0369 \end{bmatrix}$.

The second part of the evaluation model, the second level of analysis, takes the system security situation as the target layer E, and the criterion layer F includes mobile devices B_1, host devices B_2, and server devices B_3. Scheme layer E includes three levels: good G_1, warning G_2, and critical G_3, as shown in Fig. 3.

According to the pairwise comparison method, the judgment matrix and weight of the situation index system are determined, and the judgment matrix and weight vector of the evaluation factors of the second-level analysis criterion layer are established (as shown in Table 10).

Table 10. The judgment matrix and weight vector of the evaluation factors of the second AHP analysis criterion layer.

Judgment factors set at the criterion layer B	Judgment matrix	Weight vector $W_F(w_{F_p})$
$F = [F_1, F_2, F_3]$	$E\_F =$ $\begin{bmatrix} 1.0000 & 5.0000 & 0.5000 \\ 0.2000 & 1.0000 & 0.2000 \\ 2.0000 & 5.0000 & 1.0000 \end{bmatrix}$	$W_F = \begin{bmatrix} 0.3537 \\ 0.0904 \\ 0.5559 \end{bmatrix}$

Since the scheme level G is the same as the scheme level D in the first-level analysis, the weight vector $W_{F_pG}(w_{F_pG_q})$ of the second level analysis scheme level evaluation factors to the criteria level factors to which they belong is equivalent to the first level analysis of the corresponding equipment node. The total order of levels, namely $W_{F_pG} = W^{F_p}{}_D$, $\{p|p \in [1, 3], \mathrm{i} \in N^+\}$.

According to the weight vector of the solution layer W_{F_pG} and the weight of the criterion layer W_F, the total ranking of the solution layer is calculated W_G:

$$W_G\left(w_{G_q}\right) = \begin{bmatrix} 0.5811 \\ 0.2881 \\ 0.1308 \end{bmatrix}, \text{where}$$

$$w_{G_q} = \sum_{p=1}^{3} w_{F_p} w_{F_pG_q}, \{\, p, q|p \in [1, 3], q \in [1, 3], \mathrm{p} \in N^+, q \in N^+\} \tag{11}$$

The hierarchical total sorting W_G is the situation assessment weight vector of the current equipment node, and the second-level analysis is completed.

The analysis results show that the proportion of good evaluation grades is 0.5811, the proportion of warning evaluation grades is 0.2881, and the proportion of critical evaluation grades is 0.1308. According to the criterion of maximum comprehensive evaluation weight, it can be seen that the network security situation assessment is in a good state.

5 Conclusion

This paper uses a hierarchical analysis model to evaluate the security situation of the system. The first level of analysis will directly calculate the weight vector of the situational security level of a single node, and will not upload this assessment information to the central database, but rely on the principle of consistency of the distributed system to ensure the synchronization of the assessment information, Effectively avoiding the leakage of assessment information and the tampering of security data. The second-level analysis carried out re-built the level analysis model around the importance of equipment, realized the situation assessment of the system directly within a single node, and provided the situation assessment for the distributed system from single-point situation assessment to multi-point integration. A concrete and feasible solution.

Acknowledgement. This work is supported by the State Grid Sichuan Company Science and Technology Project: "Research and Application of Key Technologies of Network Security Protection System Based on Zero Trust Model" (No.SGSCCD00XTJS2101279).

References

1. Wei, Y., Lian, Y., Feng, D.: Network security situation assessment model based on information fusion. Comput. Res. Dev. **46**(3), 353–362 (2009)
2. Wang, Z., Jia, Y., Li, A., Zhang, J.: Quantitative assessment method of network situation based on fuzzy analytic hierarchy process. Comput. Secur. **1**, 61–65 (2011)
3. Jiang, Y., Xu, C.: Advances in set pair analysis theory and its applications. Comput. Sci. **33**(001), 205–209 (2006)
4. Chen, L., Lv, C.: Research on power risk assessment method based on fuzzy comprehensive evaluation. Electric Power Sci. Eng. **026**(011), 50–54 (2010)
5. Gao, J., Guo, F.: Interval intuitionistic fuzzy multi-attribute decision-making method based on reference point dependent utility function. Statist. Decis. **17**, 45–50 (2019)
6. Qian, B., Cai, Z., Xiao, Y., Yang, J., Liao, N.D., Su, S.: Network security situation awareness of metering automation system based on fuzzy inference. South. Power Grid Tech. **13**(2), 51–58 (2019)
7. Ding, H.D., Xu, H., Duan, R., Chen, F.: Network security situation awareness model based on Bayesian method. Comput. Eng. **46**(514), 136–141 (2020)
8. Mao, Y.: Research on situation prediction method combined with hidden Markov and genetic algorithm. Ph.D. dissertation, Northwest University (2019)
9. Tang, Y.L., Li, W.J., Yu, J.X., Yan, X.X.: Network security situation assessment method based on improved DS evidence theory. J. Nanjing Univ. Sci. Tech. **39**(04), 405–411 (2015)
10. Skopik, F., Wurzenberger, M., Settanni, G., Roman, F.: Establishing national cyber situational awareness through incident information clustering. In: Procedding of International Conference on Cyber Situational Awareness, pp. 1–8 (2015)
11. Dianwen, L., Xiu, J., Xin, T.: Chaos-GA-BP neural network power load forecasting based on rough set theory. J. Phys. Conf. Ser. **1**, 012132. IOP Publishing (2010)
12. Ly, B., Manickam, S.: Novel: adaptive grey verhulst model for network security situation prediction. Proc. Int. J. Adv. Comput. Sci. Appl. **7**(1), 90–95 (2016)
13. He, F., Zhang, Y., Liu, D., Ying, D., Liu, C.Y., Wu, C.S.: Mixed wavelet-based neural network model for cyber security situation prediction using MODWT and Hurst exponent analysis. In: Proceeding of International Conference on Network and System Security, pp. 99–111 (2017)

14. Liu, H., Zhou, L.Q., Rui, J., Zhao, Z.W.: Evaluation model based on support vector machine and the weight of the adaptive network security situation weights. Comput. Syst. **27**(7), 188–192 (2018)
15. Wang, J., Zhang, F.L., Fu, C., Chen, L.S.: Study on index system in network situation awareness. J. Comput. Appl. **27**(8), 1907–1909 (2007)
16. Gong, J., Zang, X.D., Su, Q., Hu, X.Y., Xu, J.: Overview of cyber security situational awareness. J. Softw. **28**(04), 1010–1026 (2017)
17. Zhang, H.B., Yin, Y., Zhao, D.M., Liu, B.: Network security situation awareness model based on threat intelligence. J. Commun. **42**(6), 182–194 (2021)
18. Mustafa, M.A., Al-Bahar, J.F.: Project risk assessment using the analytic hierarchy process. IEEE Trans. Eng. Manage. **38**(1), 46–52 (1991)
19. Saaty, T.L.: The analytic hierarchy and analytic network measurement processes: applications to decisions under Risk. Euro. J. Pure Appl. Math. **1**(1), 122–196 (2008)
20. Shilun, G.: A 1–9 determines coefficient function evaluation scale method. Value Eng. **1**, 33–34 (1989)
21. Hong, Z.G., Li, Y., Fan, Z.H., Wang, Y.: Calculation of high-order average random consistency index (RI) in analytic hierarchy process. Comput. Eng. Appl. **12**, 45–47 (2002)
22. Berguiga, A., Harchay, A.: An IoT-based intrusion detection system approach for TCP SYN attacks. Comput. Mater. Continua **71**(2), 3839–3851 (2022)
23. Ju, X.: An overview of face manipulation detection. J. Cyber Secur. **2**(4), 197–207 (2020)
24. Samad, M.A., Choi, D.: Analysis and modeling of propagation in tunnel at 3.7 and 28 ghz. Comput. Mater. Continua **71**(2), 3127–3143 (2022)
25. Devi, S.K., Subalalitha, C.N.: Deep learning based audio assistive system for visually impaired people. Comput. Mater. Continua **71**(1), 1205–1219 (2022)
26. Al-Adhaileh, M.H., Alsaade, F.W.: Detecting and analysing fake opinions using artificial intelligence algorithms. Intell. Autom. Soft Comput. **32**(1), 643–655 (2022)