Advances in Computer Science Research, volume 89
2019 International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME 2019)

Construction of Hierarchical Network Security Situation Early Warning Model Based on Fuzzy Reasoning

Guowei Suo[1], Ronghua Guo[1,*], Jiawei Du[1], Yinglong Liu[1], Jinsuo Wang[1] and Zibiao Niu[2]
[1]LEETC, Zhoushan Road 17#, Luoyang City, Henan Province, China
[2]Army Academy of Border and Coastal Defense, Xi'an City, Shaanxi Province, China
[*]Corresponding author

***Abstract*—The network security situation early warning has been deeply studied in the paper, and a hierarchical network security situation early warning model has been established based on fuzzy reasoning. First of all, the correlation theory of fuzzy reasoning in artificial intelligence has been introduced, we master the framework of fuzzy reasoning algorithm and the related knowledge of hierarchical design model. then, the network security situation early warning process and fuzzy reasoning process have been designed, At last, the network security situation early warning hierarchical frame and the structure model based on fuzzy reasoning has been realized.**

Keywords—network security; early warning; fuzzy reasoning

I. INTRODUCTION

The network security situation assessment[1] can acquire relevant elements on space and time, use specific mathematical prediction models and prior knowledge to predict the development trend, tell the decision makers the current network status, quantify or correlate the original network event data information, synthesize a variety of security factors, give the network current status data value, and put it into practice. As input, it is sent to the network security situation early warning module, and the network security situation early warning uses the established situation awareness early warning model to process the assessment value of these situations to provide early warning services.

The real-time generation of situation awareness assessment results and analysis of situation data information is the basis of network security situation awareness early warning[2]. Network security situation assessment is the precondition of network security situation early warning. Through processing and calculating various original network time situation index data by some network security situation assessment algorithm, the network security situation assessment value is obtained. These data are not isolated, and there is a correlation between the data in the time dimension. Therefore, searching index data and network security situational awareness value from historical data can provide help for situational early warning[3]. In network security situation awareness early warning, due to the limited early warning function of some products, network security situation early warning is difficult to judge, control and reasoning early warning from the overall security, Therefore, according to the current network totality conditions, we must use new technologies to carry out early warning more effectively.

For the research of early warning model, we need to focus on accuracy, real-time and flexibility. Currently, the research of early warning in China has just started. There are no established standards on technologies and theories, and it has very theoretically and practically significance to carry out the related research. Therefore, this paper constructs a network security situation early warning model based on fuzzy reasoning.

II. THE RELATED THEORY OF NETWORK SECURITY SITUATION EARLY WARNING

A. Network Security Situation Early Warning

Simply speaking, the network security situation early warning using the sequences data generated by network security situation calculation part, use a certain early warning speculation and mining algorithm to obtain the implicit rules in a certain time series, and finally deduce and warn the possible network security situation in the future, and display it in a visual way such as network security situation prediction curve[4]. The contents includes the following sections.

1) The network security situation computing process

a) Acquisition of source data

Network security device sensor collects network traffic and application data, merges and fuses them, preprocesses them to remove redundant information, and prepares for subsequent association analysis.

b) The related security event

In the data acquisition based on the original data pretreatment and related security incidents, and security event data server is used to search and match the security events correlation feature information.

c) The network security assessment state

The use of appropriate evaluation technologies and methods, the prior various security incidents knowledge has been synthesized to evaluate the results of current network security status.

2) Early warning of network security situation

The early warning of network security situation is aimed at captured messages. The process includes three steps: network traffic analysis, network security situation assessment and network security situation prediction[5].Finally, it reports the results of network security situation early warning according to the early warning model, and visualizes the network security situation with various display modes and angles. There are many existing ways of network security situation early warning.

a) Early warning based on the result of network security situation assessment

The data source of network security situation early warning is the time series evaluation value produced by network security situation assessment. Taking these data as input, the early warning reasoning algorithm is used to find out the rules contained in a certain time series, deduce the security situation data that may occur in the future, and report the network security situation early warning information in visual way.

b) Early warningofnetworksecurity situation based on the time series

Early warning of network security situation based on the time series mainly takes time series data mining as the main step to explore temporal patterns or models in time series data. Early warning tasks usually include time series similarity search, time series clustering, time series classification and related rules extraction, time series early warning process and so on.

c) Early warningofnetworksecurity situation based on the linear/nonlinear regression

A linear regression function is designed for early warning based on linear regression. The least square method is used to solve the problem. The best fitting line is estimated to be a line that minimizes the error between the actual result data and the straightness estimation. Early warning of network security situation based on the nonlinear regression uses the historical security situation values of multiple time windows in the polynomial regression equation to predict the next security situation value, and then warning report according to the pre-established network security situation early warning model.

B. The Basic Theory of Fuzzy Reasoning

1) Overview

Fuzzy reasoning is an approximate reasoning method which simulates the reasoning behavior of human brain[6]. The decision conditions used in reasoning are different from logical reasoning. The propositions made up of reasoning rules and facts have certain fuzziness and belong to approximate reasoning in essence. There are two common forms of reasoning: hypothetical reasoning with affirmative preconditions and refutation reasoning with negative post conditions.

A simple expression of fuzzy hypothetical reasoning is: $A \to B$, $A^{\bullet} \perp B^{\bullet}$,this expression is different from the hypothetical reasoning of affirmative preconditions: A,B, $A^{\bullet}$, $B^{\bullet}$ can be a fuzzy proposition, and the preconditions in $A \to B$ and $A^{\bullet}$ are not same necessarily.

There are many different forms of fuzzy reasoning, but fuzzy reasoning also belongs to reasoning. The most fundamental problem to be solved is how to deduce conclusions from given premises. At present, experts and scholars have given many different solutions to this problem.

According to the structural characteristics of the proposition's input and output, the fuzzy reasoning can be divided into: *a)* the fuzzy reasoning in which the input and output are all fuzzy sets, which is the fuzzy reasoning in pure fuzzy systems; *b)* the fuzzy reasoning in which the input and output contents are discrete precise data values, which is the reasoning method similar to the artificial intelligence fuzzy neural network; *c)* Fuzzy reasoning in which the input is a fuzzy set and the output is a discrete precise value.

According to the structure and quantity of fuzzy rules, fuzzy reasoning can be divided into: *a)* simple fuzzy reasoning; *b)* multi-dimensional conditional fuzzy reasoning; *c)* chrysanthemum chain fuzzy reasoning.

Fuzzy reasoning is a kind of intellectualized comprehensive reasoning method[7]. The multi-dimensional reasoning method of fuzzy reasoning is introduced, and a hierarchical network security situation early warning model is established to solve the concrete and complex network security situation early warning problems.

2) The algorithm derivation framework for fuzzy reasoning

In the arithmetic of fuzzy reasoning, the rule of fuzzy reasoning directly affects the result of reasoning. The arithmetic deduction framework of fuzzy reasoning includes two parts: structure identification and parameter estimation[8]. Structural identification is to determine the partition of the input space and the rules of fuzzy reasoning. The input space is the membership function corresponding to the input variables to complete the partition. The main task of structural identification is to determine the shape, number and fuzzy rules of the membership function. Then, all the parameters in the framework model are set through the process of parameter estimation, i.e. reasoning rules. The overall framework is shown in Figure 1.

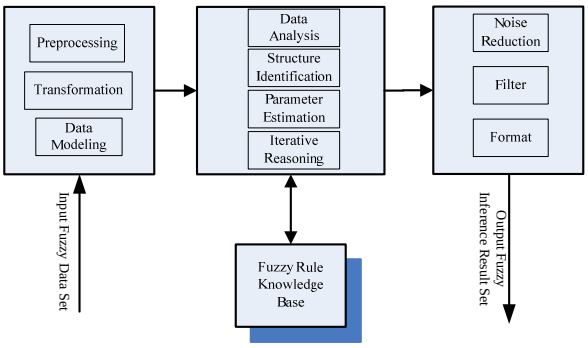

FIGURE I. THE FRAMEWORK STRUCTURE OF THE ALGORITHM FOR FUZZY REASONING

The framework preprocesses the original fuzzy data set, transforms the fuzzy data format and establishes the data set matching the fuzzy data model, then processes it with the fuzzy

reasoning logic, realizes the fuzzy reasoning function with the help of the knowledge base of the fuzzy rules through the structure identification, parameter estimation and the operation of the fuzzy reasoning machine. The framework's fuzzy reasoning process is accomplished by iteration cycle. In addition, it is a pipelined standard process whether it is the pretreatment, transformation, data modeling of the original data set, or the denoising, filtering and formatting of the results. This algorithm derives the framework algorithm, which can inspire better application class design algorithm.

3) Construction of T-S fuzzy reasoning system

The general steps for the fuzzy reasoning system are: *a)* the management of the original data set of the fuzzy reasoning; *b)* the determination of the input and output language variables and language values; *c)* the determination of the membership function parameters of the language variables; *d)* the construction of the fuzzy rule base; *e)* the construction of the core algorithm of the fuzzy reasoning. In order to solve the problem that reasoning rules are too large in multi-dimensional fuzzy process, Takagi-Sugeno proposed T-S fuzzy model, which couples multiple sub-linear models to form a non-linear fuzzy system.

A multi-input and single-output (MISO) T-S fuzzy reasoning system consists of fuzzy language rules, which are expressed as follows.

Rule**$_k$*: ***if x_1 is $\underline{A}_{k1}$ and x_2 is $\underline{A}_{k2}$ and … and $x_n$is $\underline{A}_{kn}$

Then $g_k(Y) = a_{k1}x_1 + a_{k2}x_2 + a_{k3}x_3 + \cdots + a_{kn}x_n$

Note: ***Rule**$_k$* is the *k*rule in the framework of fuzzy algorithm, $k \in \{1, 2, 3, \cdots, N\}$, Yis the discrete value of the input data set for the system, $Y = (x_1, x_2, \cdots, x_n)$. $\underline{A}_{ki}$ ($1 \le i \le n$)is a fuzzy subset on the variable definition field x_j .Its logical premise is the part of fuzzy calculation. The conclusion of logical reasoning is a linear regression function of discrete input data. If the excitation intensity of ***Rule**$_k$* excitation using a product by way of reasoning can be obtained it.

$$\omega_k(X) = \prod_{i=1}^{n} \mu_{A_{ki}}(X) \tag{1}$$

The output expression of T-S fuzzy system is as follows.

$$\sigma_k(X) = \omega_k(X) / \sum_{k=1}^{M} \omega_k(X) \tag{2}$$

$$y = \sum_{k=1}^{M} g_k(X)\sigma_k(X) \tag{3}$$

$$\mu_{A_{ki}}(X) = \exp\{-[(x_k - \alpha_{jk})^2 / \beta_{jk}{}^2]\} \tag{4}$$

Among them, M is the number of fuzzy rules, $\sigma_k(X)$ is the normalized excitation intensity of each rule, α_{jk} and β_{jk} represent the expectation and variance of the membership function, respectively. The rule establishment is the main process of T-S system modeling. The important content is the rule structure determination and the rule parameter identification.

a) SOM clustering algorithms

SOM clustering algorithm using hierarchical design method, including input layer and competition layer. The input layer consists of several neurons, and the competition layer consists of several neurons, each of which represents a category. The neurons between the input layer and the competition layer maintain a fully connected relationship. The specific algorithm steps are as follows:

1. A large initial neighborhood is set up among neurons, and the weights of random initial values are allocated.

2. Design input mode for SOM network, expressed as $X = (X_{1k}, X_{2k}, X_{3k}, \cdots, X_{nk})$.

3. Traverse and calculate the distance d between the model and the competing layer neurons in turn, and find out the neuron c with the smallest distance from the model.

4. Update the weights between cand its neighboring neurons. The formulas are as follows.

$$\omega_{jk}(t+1) = \varphi(t)(x_i - \omega_{jk}(t)) + \omega_{jk}(t) \tag{5}$$

In equation(5), the gain function $\varphi(t) \in (0,1)$.

5. Jump to step ‘2’and repeat.

b) SOM&K-Means clustering algorithms

The SOM&K-Means clustering algorithm takes into account the advantages of SOM algorithm and K-Means algorithm, focusing on the selection of initial clustering centers and the performance of clustering results. Its algorithm steps are as follows:

1. Set the number of executions of clustering algorithm, execute SOM clustering algorithm, input the initial fuzzy data set into SOM model, and obtain the output value of SOM network.

2. The result of SOM fuzzy network transformation is used as the initial clustering input of K-Means algorithm, and the object and cluster are re-mapped according to the clustering center value.

3. Recalculate the expected values of neurons in clusters and find new clustering centers.

4. Repeat step ‘2’and ‘3’until the cluster center does not change.

The SOM&K-Means clustering algorithm not only maintains the self-organizing characteristics of SOM network,

but also has the characteristics of K-Means high efficiency. The most important point is to solve the defect of poor clustering effect caused by poor selection of initial clustering centers.

III. Construction of Early Warning Model for Network Security Situation Based on Fuzzy Reasoning

A. The Network Security Situation Early Warning Process

To carry out network security situation early warning, this section proposes a network security situation early warning model based on the theory of fuzzy reasoning. Based on the quantitative evaluation results of situation elements, the network security situation early warning model is used to effectively predict and warn the network security status. Similarly, network administrators can obtain accurate and effective network security early warning information and grasp the security situation of the network environment by virtue of this early warning process. The network security situation early warning process consists of three stages. The specific network security situation early warning process is shown in Figure II.

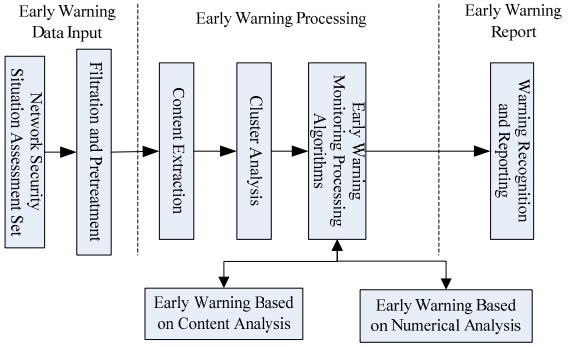

FIGURE II. NETWORK SECURITY SITUATION EARLY WARNING PROCESS

B. The Derivation Process of Early Warning Based on Fuzzy Reasoning

The derivation process of early warning based on fuzzy reasoning, a more accurate early warning model is made by using the methods of fuzzy mathematics and statistical analysis in the field of artificial intelligence, taking into account all the factors related to the network security situation.

1) Analytical recognition and early warning process based on fuzzy reasoning

The early warning process of analysis and recognition based on fuzzy reasoning is to integrate the technology and method of fuzzy reasoning into the content recognition module. Firstly, the network security situation assessment result set obtained is preliminarily operated on data preprocessing, format conversion, key information extraction, and then cluster analysis operation is performed to generate the classification set C.

$$C = \{C_1, C_2, C_3 \cdots, C_n, \cdots\} \tag{6}$$

Next, the most important thing to be accomplished is the establishment of class eigenvectors. Each class is represented by a vector space model, and its equation can be expressed as follows.

$$C_m = (T_{m1}, W_{m1}; T_{m2}, W_{m2}; T_{m3}, W_{m3}; \cdots; T_{mn}, W_{mn}; \cdots) \tag{7}$$

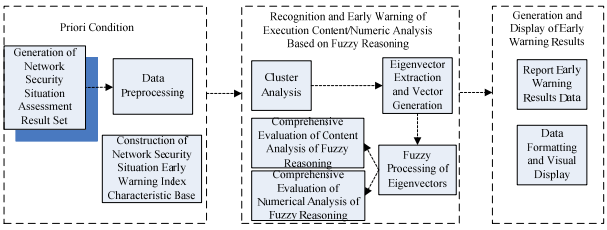

FIGURE III. THE ANALYSIS AND RECOGNITION PROCESS OF EARLY WARNING BASED ON FUZZY REASONING

The process of establishing and implementing the analysis, recognition and early warning based on fuzzy reasoning is shown in Figure III.

In the process of analysis and early warning, it is necessary to set up the factor set of evaluation feature vector and the standard influencing factor set of feature vector beforehand, that is, the characteristic database of network security situation early warning index, so that the index set ($U = \{u_1, u_2, \cdots, u_i, \cdots\}$) of evaluation feature vector can be obtained from the fuzzy reasoning early warning and used to participate in the actual determination of evaluation influencing factors; besides, there should be some correlation with influencing factors. There should also be a set ($V = \{v_1, v_2, \cdots, v_m, \cdots\}$) of security early warning levels related to influencing factors.

2) Comprehensive evaluation process of fuzzy reasoning

The comprehensive evaluation process of fuzzy reasoning includes two sub-processes, one is single factor evaluation and the other is comprehensive evaluation.

a) Single factor evaluation

Determining the single factor evaluation matrix R is the key to complete the single factor evaluation. The single factor evaluation matrix evaluates each eigenvector element in turn.

The degree of membership v_m to r_m was determined. The membership function of element u_i which belongs to the category *m* security early warning level can be expressed as follows.

$$r_{im} = \begin{cases} \dfrac{c_i - s_{i,m-1}}{s_{i,m+1} - s_{i,m}} & s_{i,m-1} < c_i < s_{i,m} \\ \dfrac{s_{i,m+1} - c_i}{s_{i,m+1} - s_{i,m}} & s_{i,m} < c_i < s_{i,m+1} \\ 0 & c_i \le s_{i,m-1} \text{ or } c_i \ge s_{i,m+1} \\ 1 & c_i \equiv s_{i,m} \end{cases} \tag{8}$$

Among them, the factor c_i is the actual measurement data of factor u_i, the factor $s_{i,m}$ is the reference value of type m security early warning level, and factor r_{im} is the membership data of factor u_i to the type m security early warning level. Therefore, the evaluation result set of factor i can be expressed as follows:

$$R_i = (r_{i1}, r_{i2}, r_{i3}, \cdots, r_{im}) \tag{9}$$

Assuming that there are n items in the influencing factors, the order $n \times m$ fuzzy matrix R can be written as follows:

$$R_{n\times m} = \begin{bmatrix} r_{11}, r_{12}, r_{13}, \cdots, r_{1m} \\ r_{21}, r_{22}, r_{23}, \cdots, r_{2m} \\ \cdots\cdots\cdots\cdots \\ r_{n1}, r_{n2}, r_{n3}, \cdots, r_{nm} \end{bmatrix} \tag{10}$$

b) Comprehensive evaluation

The one-factor fuzzy evaluation can reflect the evaluation of one factor on eigenvector elements, and cannot achieve the comprehensive impact of all factors in multi-dimension, so the evaluation results may also have errors. The method of comprehensive evaluation changes the single factor into the combination of the fuzzy vector and the fuzzy matrix R produced by the single factor evaluation, and finally obtains the multi-dimensional fuzzy comprehensive evaluation vector of the characteristic vector, which reflects the comprehensive influence of each factor more reasonably. The calculation formula is as follows.

$$Z = S \times R = (s_1, s_2, s_3, \cdots, s_n) \begin{bmatrix} r_{11}, r_{12}, r_{13}, \cdots, r_{1m} \\ r_{21}, r_{22}, r_{23}, \cdots, r_{2m} \\ \cdots\cdots\cdots\cdots \\ r_{n1}, r_{n2}, r_{n3}, \cdots, r_{nm} \end{bmatrix} = (z_1, z_2, z_3, \cdots, z_n) \tag{11}$$

C. Early Warning Model for Network Security Situation Based on Fuzzy Reasoning

1) Hierarchical structure of early warning model fornetwork security situation

The early warning model based on fuzzy reasoning comprehensively analyses and processes the related multiple result vector sets in the security situation assessment results. By using the alarm index data in the pre-built network security situation early warning index database, the key information in the characteristic vector is extracted and transformed, which is used as the input information of the situation early warning processing. From the network host node situation and network synthesis, the key information in the network security situation early warning index database is extracted and transformed. This paper describes the situation, theoretical security threats and the importance of network node weights. At the same time, it uses the fuzzy reasoning model to warn, and finally visualizes the results of network security situation early warning. The hierarchical structure of early warning model forthe network secsssurity situation is shown in Figure IV.

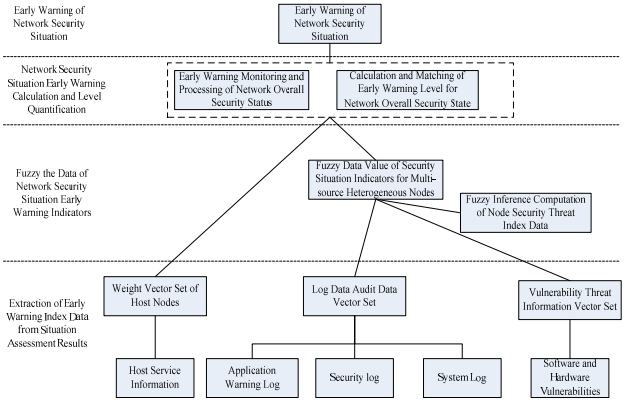

FIGURE IV. THE HIERARCHICAL STRUCTURE OF EARLY WARNING MODEL FOR NETWORK SECURITY SITUATION

The primary target of early warning for network security situation is to introduce the viewpoint of fuzzy data processing, improve the warning time of malicious attacks more accurately, and improve the emergency response ability of network system. To provide managers with the overall security warning level information of the network, decision makers can make corresponding decisions or optimize adjustments based on the situation warning results. The network situation warning model described in Figure IV represents the common network types in the current computer network. The data vector set of the situation assessment results of various security devices, servers or hosts in the network is used as the data source model, and then the early warning indicators are extracted from these inputs for the situation early warning.

2) The early warning for network security situation

The early warning model for network security situation based on fuzzy reasoning is constructed by modularization, which includes three sub-models: the data construction of network security situation early warning index, the sub-model of viewpoint evolution fuzzy reasoning and the sub-model of network situation crisis early warning.A unified viewpoint mining model is constructed, and viewpoint tree is generated to obtain viewpoint elements of various levels and granularities.The viewpoint evolution fuzzy inference sub-model is used to evolve trend prediction results of viewpoints by means of fuzzy inference.The network security situation crisis early warning sub-model is used to calculate trend prediction results, viewpoint evolution fuzzy inference will complete corresponding early warning report according to the level and weight of searly warning. The framework structure is shown in Figure V.

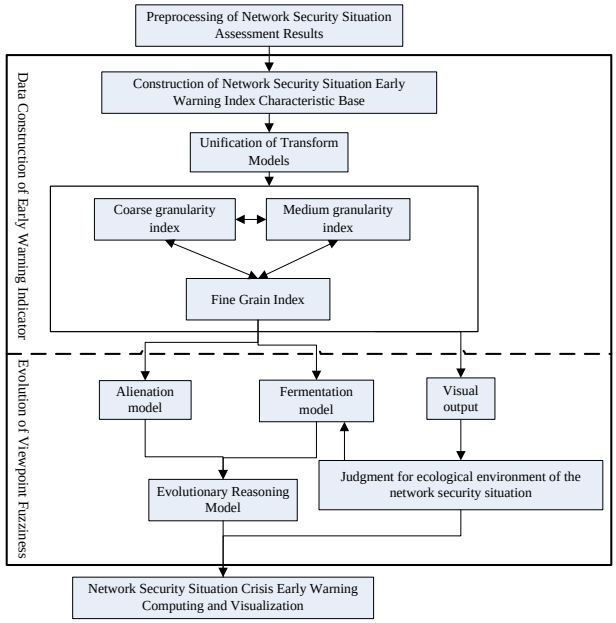

FIGURE V. FRAMEWORK OF WARNING MODEL FOR NETWORK SECURITY SITUATIONEARLY BASED ON FUZZY REASONING

IV. CONCLUSION

In the article, the research and construction of a network security situation early warning model based on fuzzy reasoning are completed. Firstly, we studied the related key technology and theory of network security situation early warning and fuzzy reasoning, and the relevant deduction framework of fuzzy reasoning and T-S fuzzy reasoning system model are emphatically analysed. The network security situation early warning model based on fuzzy reasoning is proposed. This paper constructs a hierarchical model framework of network security situation early warning model, which has good dynamic adaptability. Under given network conditions, stability and alarm accuracy have their unique advantages, which provide new ideas and new insights for the study of network security situation. However, some problems need to be further improved. The main contents that need further study are as follows.

A. The network security situation early warning model based on fuzzy reasoning in this paper only has many unique early warning advantages. However, the computational complexity for large-scale network node data will be very large, especially in the cloud environment, the runtime performance of the model will be affected by processing the large amount of massive data. In future studies, it will be further expanded and improved.

B. In future studies, we will further study a variety of intelligent reasoning algorithms, including neural networks, and explore more intelligent, efficient and accurate early warning methods.

REFERENCES

[1] Yiyu Zhang. Mobile Internet Security Situation Assessment Research Based on Fuzzy Hierarchical Algorithms [D]. Hunan University of Science and Technology, 2015.

[2] Xiaoli Zhu. Research on monitoring and early warning mechanism of information network security [A]. Third Institute of Public Security, Second National Conference on Information Security Grade Protection Technology [C]. Third Institute of Public Security, Beijing Editorial Department of Information Network Security, 2013:2.

[3] Ming Jiang. Research on Key Technologies of Network Security Multidimensional Dynamic Risk Assessment[A]. International Information and Engineering Association.Proceedings of 2018 7th International Conference on Advanced Materials and Computer Science(ICAMCS 2018)[C].International Information and Engineering Association: Computer Science and Electronic Technology International Society,2018:5.

[4] Fengli Zhang. Early warning and processing technology for network security incidents [A]. National Computer Network and Information Security Management Center, Communication Security Technical Committee of China Communication Society, National Symposium on Network and Information Security Technology, [C]. National Computer Network and Information Security Management Center, Communication Security Technical Committee of China Communication Society, 2004:5.

[5] Zengliang Miao. Development and Countermeasures of cyberspace situational awareness and early warning technology [A]. China Command and and Control Society. Papers of the Sixth China Command and and Control Congress (Volume 2) [C]. China Command and and Control Society: China Command and and Control Society, 2018:3.

[6] Gang Chen. RF-SVM Bsased Awareness Algorithm in Intelligent Network Security Situation Awareness System[A]. Institute of Management Science and Industrial Engineering.Proceedings of 2017 3rd Workshop on Advanced Research and Technology in Industry Applications(WARTIA 2017)[C].Institute of Management Science and Industrial Engineering:Computer Science and Electronic Technology International Society,2017:5.

[7] Duan Tao. RBF fuzzy reasoning flexible decision making method oriented to statistical information[A]. International Society of Informatization and Engineering.Proceedings of 2016 4th International Conference on Machinery,Materials and Information Technology Applications(ICMMITA 2016)[C].Computer Science and Electronic Technology International Society,2016:6.

[8] Qing Dai, Chengrui Ye, Yunfeng Ma. A navigation adaptive filtering algorithm based on fuzzy reasoning [J]. Journal of Xi'an Aeronautical College, 2018, 36 (03): 16-19.