Model of Information Security Risk Assessment based on Improved Wavelet Neural Network

Gang Chen and Dawei Zhao
College of Humanities & Sciences of Northeast Normal University, Jilin Changchun, China
Email: cghdm@163.com

Abstract—This paper concentrates on the information security risk assessment model utilizing the improved wavelet neural network. The structure of wavelet neural network is similar to the multi-layer neural network, which is a feed-forward neural network with one or more inputs. Afterwards, we point out that the training process of wavelet neural networks is made up of four steps until the value of error function can satisfy a pre-defined error criteria. In order to enhance the quality of information security risk assessment, we proposed a modified version of wavelet neural network which can effectively combine all influencing factors in assessing information security risk by linear integrating several weights. Furthermore, the proposed wavelet neural network is trained by the BP algorithm with batch mode, and the weight coefficients of the wavelet are modified with the adopting mode. Finally, a series of experiments are conduct to make performance evaluation. From the experimental results, we can see that the proposed model can assess information security risk accurately and rapidly.

Index Terms—Information Security Risk, Wavelet Neural Network, Basic Belief Assignment, Risk Factor

I. INTRODUCTION

With the rapid development of network technology, information quickly spreads with the help of the network, and the security of information systems has also been faced a wide range of threats. Therefore, how to guarantee the security of information systems is an important which should be well solved. In the research of system security of the past years, people find that the problem of information system security could not be completely solved only by technology, its solution involves all aspects of the regulations and policies, management, standards, technology. Particularly, any single level security measures are unlikely to provide the full range of security, information systems security problems should be considered in the perspective of systems engineering. In this systems engineering, information systems security risk analysis and assessment occupy an important position, and it is the basis and prerequisite of information systems security. Information system security risk analysis refers to a variety of objects including system architecture, instructional strategies, staff position, as well as various types of equipment such as workstations, servers, switches, database applications. According to the inspection results to the system administrator, it can provide a thorough and reliable security analysis. In order to improve the overall level of information security, the report provides an important basis. The risk assessment is an important technology in the network security defense, which is also an important part of the information security engineering. The principle of risk assessment is to review the security policy and regulations, find unreasonable aspects [1].

In the past few decades, information technology has undergone enormous change throughout the world. Information technology plays an increasingly important role in people’s production and daily life, and human beings are increasingly depending on IT products. The information industry has become an important pillar industry of the world economy based on information technology. The level of information industry development has become an important symbol of the strength of a country's comprehensive national strength and international competitiveness. In recent years, due to the problems of information system security, more and more people are paying attentions on the impact of information system security, which has become an important factor to influence the development of information technology. However, the traditional characteristics of constructing the information systems security architecture lie in the following parts: 1) the tradition method can not security issue in time; 2) the security solving process is passive. Therefore, the traditional methods can not meet the requirements of modern information security construction, and the traditional models are often lack of systematic consideration with a lot of blindness, and often spend a lot of little success to cause a huge waste of funds [2][3].

For today’s growing demand for information systems security, technical methods are not a fundamental solution to the information system security issues. The security of information systems should be solved through systems engineering, and the risk assessment of the systems engineering occupies an important position, and it is the basis and prerequisite of information systems security. Users can understand the system where the current and future risks to assess the potential security threat, and then provide the basis to determine the security policy. Information security risk assessment has become an increasingly important problem, which has been paid more attentions by many developed countries.

© 2013 ACADEMY PUBLISHER
doi:10.4304/jnw.8.9.2093-2100
As is well known that the development of information technology is a double-edged sword. Therefore, when information technology for the development of the world brings a lot of convenience to people's lives, at the same time, it can also give a negative impact to our daily lives in different ways [4]. With the great requirements of information systems in government departments, enterprises and institutions, financial institutions, security of information system has become an universal concern. Many countries have made the security of information and information systems in the height of maintaining social stability and national security. Information security risk assessment is the starting point of the security building, and it has a pivotal position in the information security.

Facing the increasingly serious problem of information security, simply technical approach can not the problem of information system security. On the other hand, there are more and more viruses, hackers and other attacks from the Internet, and the threats are more serious. Hence, we should regard the security of information systems at the point of view under the system engineering, and the risk assessment is the premise and foundation of information systems security. We can utilize risk assessment to comprehensively understand the organization in the security environment, and then find the hazards and safety issues. Afterwards, we can find the gap between system's security policy and actual demand. Next, users can know potential threat and the impacts of these risks. Based on the above measures, effective risk assessment can bring relevant security policies for decision-makers to determine the effective security measures, and to provide the basis for the safe operation of the information system. Information security risk assessment is the base of the security system construction where all security system should be built up on the basis of the information security risk assessment. Only comprehensive and correct analyzing risk can make valid decisions on risk prevention, control, transfer and reduction, and then determine what kind of response measures and control means [5] [6].

We can know the environment and the status of information security in the information security risk assessment, and then take measures to improve the protection of information security. It can be seen from the experience of information technology development in developed countries that we should pay more attention to the information security risk assessment. Without effective risk assessment method, security requirements and solutions will lead to serious detachment. In recent years, in developed countries, security risk assessment is enhanced by standard means, laws and regulations and other means.

Wavelet neural networks are a powerful computing tool which combines the theory of wavelets and neural networks together [7]. In this paper, we apply wavelet neural networks in the application of information security risk assessment.

The innovations of this paper lie in the following aspects: (1) We present a modified Wavelet neural network which can linear integrate several weights which is suitable to use in information security risk assessment, (2) We propose a novel training process of wavelet neural networks which are built by three-layer and implemented in four steps. (3) The metric basic belief assignment is used in performance evaluation of information security risk assessment problem.

Risk assessment is the key procedure of information security risk management. Management organizations utilize risk assessment to decide the risks within an information system and provide sufficient methods to cut down these risks.

Qian et al. built a system dynamics model using the Norwegian Oil and Gas Industry as the context. The Norwegian Oil and Gas Industry have started to adopt new information communication technology to connect its offshore platforms, onshore control centers, and suppliers. The system dynamics model can serve as a means to promote proactive investment in incident response capability [8].

Eren-dogu et al. present a novel approach using Bayesian Prioritization procedure to provide a more effective way of risk assessment than proposed by the conventional approaches used in AHP-GDM, which could offer a technical support for risk analysis by taking the judgements of managers and systematically calculating the relative risk values [9].

Li et al. summarized the current situation of risk assessment studies in terms of assessment standard, analysis technology and assessment framework. With studying and analyzing compositions and characteristics of cyberspace network, it reviews the security threats that may exist in the network [10].

In paper [11], the authors explored the utility of applying the well-established method of expert judgment elicitation to the field of information security. The instrument for eliciting the expert judgments was developed by two information security specialists and two expert judgment analysis specialists. The resultant instrument was validated using a small set of information security experts.

Kim et al. proposed a improved scenario-based SRA approach, which can create SRA reports using threat scenario templates and manage security risk directly in ISs. Furthermore, in order to show how to apply the proposed method in a specific environment, especially in a Broadband convergence Network (BcN) environment, a case study is present [12].

As the existing algorithms and instrumental security risk assessment tools mainly are dedicated to government institution or large-size companies. In paper [13], the authors proposed a risk assessment algorithm for medium and small companies. The algorithm consists of eight steps. The algorithm and methodology have been approved in the real small-size company.

Wang et al. investigated two session-level metrics reflecting users’ interactivity with a search engine: session length and query click rate. Drawing from information foraging theory, we find that session length can be characterized well by the Inverse Gaussian
distribution. Among three types of sessions on different topics, they find that healthcare sessions have the most queries and the highest query click rate, and information security sessions have the lowest query click rate [14].

Lo et al. present a hybrid procedure for evaluating risk levels of information security under various security controls. Firstly, this method procedure applies the Decision Making Trial and Evaluation Laboratory (DEMATEL) approach to construct interrelations among security control areas. Secondly, likelihood ratings are obtained through the Analytic Network Process method. Finally, the Fuzzy Linguistic Quantifiers-guided Maximum Entropy Order-Weighted averaging operator is used to aggregate impact values assessed by experts [15].

On the other hand, we will introduce the wavelet neural network, which generally includes a feed-forward neural network, with one hidden layer. The main application fields of wavelet neural networks are used in function estimation. Next, we will illustrate the applications of wavelet neural network.

In paper [16], the authors utilized wavelet transform to extract fault characteristics from the anomaly state. Fuzzy theory and neural network are employed to fuzzify the extracted information. Wavelet is then integrated with fuzzy neural network to form the wavelet fuzzy neural network (WFNN).

Pan et al. proposed a novel algorithm for vehicle license localization and character recognition which is based on adaptive wavelet neural networks. The authors used the wavelet transform to preprocess color vehicle image into index image which undergoes wavelet transform to obtain wavelet feature coefficients [17].

Huang et al. established immune genetic algorithm optimization of wavelet neural network model to predict the performance of centrifugal compressor, and the predicted results with the BP neural network model prediction results and the wavelet neural network model prediction results were compared [18].

Wei et al. proposed a wavelet-neural network hybrid modelling approach for monthly river flow estimation and prediction. The proposed method integrated discrete wavelet multi-resolution decomposition and a back-propagation feed-forward multilayer perceptron artificial neural network [19].

Senapati et al. proposed a novel learning technique for local linear wavelet neural network. The difference of the network with conventional wavelet neural network is that the connection weights between the hidden layer and output layer of conventional WNN are replaced by a local linear model. A hybrid training algorithm of Error Back propagation and Recursive Least Square is introduced for training the parameters of LLWNN [20].

Li et al. present a new network traffic prediction method, which method combined genetic algorithm and wavelet neural network to model and forecast the time series of network traffic data. Aiming at shortcomings of wavelet neural network, such as slow convergence speed, easy to be trapped into local minimum, and etc, the network traffic prediction model based on the genetic algorithm and wavelet neural network is built, in which Genetic algorithm with good global searching ability is adopted to optimize the initial weights and thresholds of neural networks [21].

Che et al. proposed a method of wavelet neural networks with data pre-filtering. The key idea is to use a spike filtering technique to detect spikes in load data and correct them. Wavelet decomposition is then used to decompose the filtered loads into multiple components at different frequencies, separate neural networks are applied to capture the features of individual components, and results of neural networks are then combined to form the final forecasts [22].

II. OVERVIEW OF WAVELET NEURAL NETWORK

The structure of a wavelet neural network is just like the multi-layer neural network. It is means that a feed-forward neural network with one or more inputs. Particularly, as is shown in Fig. 1, the wavelet neural network is allocated with a hidden layer and an output layer which is made up of one or more linear combiners. The hidden layer includes several neurons, of which activation functions are drawn from a wavelet basis. Furthermore, the wavelet neurons are often named wavelons.

In order to build wavelet neural networks, two methods could be utilized as follows.

1) The procedure of wavelet and the neural network creating process are executed separately. At first, the input signal is decomposed through some wavelet basis using the neurons which is located in the hidden layer. Next, the coefficients of wavelet are output to summers.

2) For the second method, the wavelets’ translation and dilation which are related to the summer weights are set by learning algorithms.

Function $\Psi(x)$ is used to build a family of wavelets, which could be confined in the mode of finite interval. Afterwards, $\Psi^{a,b}(x)$ are constructed by dilation (denoted as $a$) and translation (denoted as $b$). Particularly, an individual wavelet can be calculated as follows.

$$\Psi^{a,b}(x) = \left[\Psi(x) \frac{1}{a}\right] \cdot \Psi\left(\frac{x-b}{a}\right), a, b \in R^+, i \in Z \quad (1)$$
In Eq. 1, \( x, a_i \) and \( b_i \) are satisfied the following constraints.

\[
x = (x_1, x_2, \ldots, x_n)
\]

(2)

\[
a_i = [a_{i1}, a_{i2}, \ldots, a_{in}]
\]

(3)

\[
b_i = [b_{i1}, b_{i2}, \ldots, b_{in}]
\]

(4)

III. PROPOSED SCHEME

In this section, we will introduce the proposed information security risk assessment method utilizing wavelet neural network. In the problem of information security risk assessment, nonlinear relations and dynamic change rules are used in each evaluating index for the risk factors and the related risk levels. Therefore, wavelet neural network can be used to implement the complex non-linear mapping relation between the input information and output information.

Before perform the Information security risk assessment process, we should analyze the asset, threats, relationship to obtain risk factors. Next, the risk factors can be obtained (denoted as \( R = \{r_1, r_2, \ldots, r_n\} \) using fuzzy evaluation approach. Afterwards, the judgment set is constructed by calculated the value of integrity, availability and confidentiality. Hence, the comments for each index are given by dividing the comment of each index into a set \( S = \{s_1, s_2, \ldots, s_j\} \).

Particularly, the comment of each risk factor is obtained by a fuzzy mapping process, which can be represented as the following equation:

\[
f : R \rightarrow F(S)
\]

(5)

where \( F(S) \) denotes the entireness of the fuzzy set in \( S \).

The mapping function \( f() \) could map the risk factors \( r_i \) to each comment of the judgment set as follows.

\[
r_i \rightarrow f(u_i) = (x_{i1}, x_{i2}, \ldots, x_{in}) \in F(S)
\]

(6)

Assuming that the membership vector of risk factors \( r_i \) to the set of judgment \( S \) is denoted as \( X_i = \{x_{i1}, x_{i2}, \ldots, x_{in}\} \), and then the membership degree matrix \( X \) is defined as follows.

\[
X = \begin{bmatrix}
x_{11} & x_{12} & \cdots & x_{1n} \\
x_{21} & x_{22} & \cdots & x_{2n} \\
& \cdots & \cdots & \cdots \\
x_{m1} & x_{m2} & \cdots & x_{mn}
\end{bmatrix}
\]

(7)

As the risk could be influenced by the judgment set’s index. Assuming that the weight of right distribution is represented as \( Q = \{q_1, q_2, \ldots, q_m\} \). Using the operation of fuzzy transform, the following equation can be obtained as follows.

\[
W = Q \cdot X^T
\]

(8)

where \( W \) denotes the weight for every risk factor by specific evaluation method, the value of which is belonged to \((0,1)\).

Afterwards, \( W \) is used as the input of the wavelet neural network. In order to improve the performance of information security risk assessment, we propose a modified version of the standard wavelet neural network, of which the output is defined as follows.

\[
f(x) = \sum_{i=1}^{M} w_i \cdot \Psi_i (x) = \sum_{i=1}^{M} w_i \cdot [\alpha_i^1 \cdot \Psi(x - b_i / a_i)]
\]

(9)

In Eq. 16, \( \Psi_i (x) \) denotes the wavelet activation function for the \( i^{th} \) unit of a hidden layer, and \( w_i \) represents the weights which connect the output layer and \( i^{th} \) unit of a hidden layer.

To make the structure of wavelet neural network is more suitable to the application of information security risk assessment, we propose a modified version of wavelet neural network and the structure of the modified wavelet neural network is shown in Fig. 2. The modified wavelet neural network can effectively combine all influencing factors in assessing information security risk.

![Figure 2. The structure of modified wavelet neural network](image-url)

As is shown in Fig. 2, the weight of wavelet neural network is modified which can reflect many factors in information security risk assessment problem. The modified weight \( w_i \) is defined as follows.

\[
\bar{w}_i = w_{i1}x_1 + w_{i2}x_2 + \cdots + w_{im}x_m
\]

(10)

Hence, the Eq. 16 could be modified as follows.
\[ f(x) = \sum_{i=1}^{N} w_i \cdot \Psi_i(x) \]
\[ = \sum_{i=1}^{N} (w_{ih_i}x_i + \cdots + w_{im}x_m) |x_i|^{\frac{1}{2}} \cdot \Psi(x - \frac{b_i}{a_i}) \]  \hspace{2cm} (11)

Afterwards, the proposed wavelet neural network can be trained through BP algorithm with batch mode, and the weight coefficient of the wavelet is modified with adopting mode. The training process of the proposed wavelet neural networks which is built by three-layer (input layer, hidden layer and output layer) can be implemented as the following steps:

**Step 1**: Choose the number of hidden nodes according to application requirements, and set the parameters of dilation and translation for these hidden nodes, and the values of parameter are between 0 and 1.

**Step 2**: For a sample \( S_t \), where \( t = 1, \ldots, T \), and \( T \) denotes the number of samples which can be computed by Eq. 12.

\[ S_t = \frac{1}{V} \sum_{j=1}^{V} W_{ij} \cdot f(x) - b_j \]  \hspace{2cm} (12)

where \( V \) denotes the number of input nodes. Then function \( f(t) \) represents a Morlet mother wavelet which is calculated by the following equation:

\[ f(t) = \cos(\gamma \cdot t) \exp(-\frac{t^2}{2}) \]  \hspace{2cm} (13)

Where \( \gamma \) is a const to adjust the influence of function \( \cos() \) to \( f(t) \).

**Step 3**: Lower the prediction error through adjusting the parameter \( H_j, h_j, a_j, b_j \), utilizing \( \Delta H_j, \Delta h_j, \Delta a_j, \Delta b_j \), the process is shown in Eq. 14-Eq. 17.

\[ \Delta H_j(t+1) = -\nu \cdot \frac{\partial E}{\partial H_j(t)} + \varphi \Delta H_j(t) \]  \hspace{2cm} (14)

\[ \Delta h_j(t+1) = -\nu \cdot \frac{\partial E}{\partial h_j(t)} + \varphi \Delta h_j(t) \]  \hspace{2cm} (15)

\[ \Delta a_j(t+1) = -\nu \cdot \frac{\partial E}{\partial a_j(t)} + \varphi \Delta a_j(t) \]  \hspace{2cm} (16)

\[ \Delta b_j(t+1) = -\nu \cdot \frac{\partial E}{\partial b_j(t)} + \varphi \Delta b_j(t) \]  \hspace{2cm} (17)

where the parameter \( \nu \) and \( \varphi \) are the value of learning and momentum respectively.

**Step 4**: Goto step two, end the whole process until the value of error function \( \tau \) satisfies a pre-defined error criteria. Particularly, the error function \( \tau \) is defined as follows:

\[ \tau = \sqrt{\sum_{k=1}^{T} (V_k - V'_k)^2} \]  \hspace{2cm} (18)

### IV. Experiments

To testify the performance of the proposed method used in the application of information security risk assessment, we conduct a series of experiments. At first, the kinds of information security risk considered in our experiments are listed in Fig. 3.

As is shown in Fig. 3 the types of information security risk are main include five kinds, which are “I1: Information Security Risk Vulnerabilities”, “I2: Threat”, “I3: Capability loss”, “I4: Assets lost”, and “I5: System recovery loss”.

**Table I. The Evaluating Results of Information Security Risk Assessment by the Experts and Our Proposed Model**

<table>
<thead>
<tr>
<th>Group ID</th>
<th>Experts (%)</th>
<th>Our proposed model (%)</th>
<th>Error rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>45.64</td>
<td>43.47</td>
<td>4.76</td>
</tr>
<tr>
<td>2</td>
<td>33.65</td>
<td>34.78</td>
<td>3.35</td>
</tr>
<tr>
<td>3</td>
<td>36.33</td>
<td>37.43</td>
<td>3.03</td>
</tr>
<tr>
<td>4</td>
<td>9.48</td>
<td>9.00</td>
<td>5.99</td>
</tr>
<tr>
<td>5</td>
<td>57.10</td>
<td>56.85</td>
<td>0.3</td>
</tr>
<tr>
<td>6</td>
<td>34.37</td>
<td>33.28</td>
<td>1.1</td>
</tr>
<tr>
<td>7</td>
<td>1.53</td>
<td>1.60</td>
<td>4.59</td>
</tr>
<tr>
<td>8</td>
<td>44.75</td>
<td>44.40</td>
<td>0.77</td>
</tr>
<tr>
<td>9</td>
<td>58.92</td>
<td>61.03</td>
<td>3.58</td>
</tr>
<tr>
<td>10</td>
<td>47.57</td>
<td>48.40</td>
<td>1.76</td>
</tr>
<tr>
<td>11</td>
<td>43.34</td>
<td>41.51</td>
<td>2.27</td>
</tr>
<tr>
<td>12</td>
<td>34.99</td>
<td>35.91</td>
<td>2.62</td>
</tr>
<tr>
<td>13</td>
<td>26.31</td>
<td>27.34</td>
<td>3.13</td>
</tr>
<tr>
<td>14</td>
<td>6.27</td>
<td>6.15</td>
<td>1.91</td>
</tr>
<tr>
<td>15</td>
<td>38.21</td>
<td>38.66</td>
<td>1.20</td>
</tr>
<tr>
<td>16</td>
<td>72.15</td>
<td>75.14</td>
<td>3.15</td>
</tr>
<tr>
<td>17</td>
<td>56.45</td>
<td>55.74</td>
<td>1.25</td>
</tr>
<tr>
<td>18</td>
<td>13.48</td>
<td>13.86</td>
<td>2.79</td>
</tr>
<tr>
<td>19</td>
<td>93.40</td>
<td>96.70</td>
<td>3.54</td>
</tr>
<tr>
<td>20</td>
<td>18.57</td>
<td>18.95</td>
<td>2.05</td>
</tr>
</tbody>
</table>

In our experiments, we choose fifty groups input and output data for the training process of wavelet neural network. Particularly, the experiment data is selected from the evaluation results of some insurance enterprise, on the other hand, the input data of the wavelet neural network is the value of risk event, the output information is the evaluation result proposed by experts. Afterwards, we choose twenty groups as training samples, among which ten groups are used as checking the trained network. The evaluated results provided by experts in the train sample and the trained results of wavelet neural network are listed in Table 1.

From Table 1 we can see that the error rates for all groups between our proposed model and the results provided by experts is lower than 5%, and the average error rates for all the cases are 2.86%.

Next, the output error of the training set of wavelet neural network and the number of iterations are given in Fig. 4, of which the horizontal axis denotes the number of iteration, and the abscissa in Fig.4 is the number of cycle iteration, the longitudinal axis denotes the error rate.

Fig. 4 shows that given the predefined threshold (the value is 0.073) the error rate of our model could reach the
To illustrate the performance of the proposed model more specific, in the following parts, we will give a case study. A company with more one 200 professionals in more than 15 branches is used as a case, which serve millions of institutional and individual clients. Afterwards, we invited eight experts (denoted as $E_i$ to $E_8$) in the field of information system to analyze information security risk of the given company.

To make performance evaluation, several levels of security risk are defined, which are “Level 1: Very high risk” ($L_1$), “Level 2: high risk” ($L_2$), “Level 3: median high risk” ($L_3$), “Level 4: Low risk” ($L_4$), “Level 5: Very low risk” ($L_5$). The performance evaluation metric we used is the basic belief assignment (BBA), which is a function from $P(\Theta)$ to the range [0,1] and is defined as follows.

$$BBA : P(\Theta) \rightarrow [0,1], A \mapsto BBA(A)$$  \hspace{1cm} (19)$$

where $A$ is an element from the set $P(\Theta)$, and $\Theta$ denotes the set which could represent the frame of discernment. $P(\Theta)$ denotes the power set which includes all the possible subsets of $\Theta$. Particularly, the following conditions are satisfied:

$$\sum_{A \in P(\Theta)} BBA(A) = 1, \ BBA(\emptyset) = 0 \hspace{1cm} (20)$$

$BBA(i), i \in [1,n]$ denotes a basic belief assignment on the same frame of the discernment $\Theta$. In Table.2, we show the basic belief assignment for main assertion of information security risk.

To illustrate the performance of the proposed model more specific, in the following parts, we will give a case study. A company with more one 200 professionals in more than 15 branches is used as a case, which serve millions of institutional and individual clients. Afterwards, we invited eight experts (denoted as $E_i$ to $E_8$) in the field of information system to analyze information security risk of the given company.

To make performance evaluation, several levels of security risk are defined, which are “Level 1: Very high risk” ($L_1$), “Level 2: high risk” ($L_2$), “Level 3: median high risk” ($L_3$), “Level 4: Low risk” ($L_4$), “Level 5: Very low risk” ($L_5$). The performance evaluation metric we used is the basic belief assignment (BBA), which is a function from $P(\Theta)$ to the range [0,1] and is defined as follows.

$$BBA : P(\Theta) \rightarrow [0,1], A \mapsto BBA(A)$$  \hspace{1cm} (19)$$

where $A$ is an element from the set $P(\Theta)$, and $\Theta$ denotes the set which could represent the frame of discernment. $P(\Theta)$ denotes the power set which includes all the possible subsets of $\Theta$. Particularly, the following conditions are satisfied:

$$\sum_{A \in P(\Theta)} BBA(A) = 1, \ BBA(\emptyset) = 0 \hspace{1cm} (20)$$

$BBA(i), i \in [1,n]$ denotes a basic belief assignment on the same frame of the discernment $\Theta$. In Table.2, we show the basic belief assignment for main assertion of information security risk.
Based on the above case, we conduct an experiment to compare other two schemes, which are “Method 1” (Neural network based information security risk assess), “Method 2” (Wavelet neural network based information security risk assess) and “Our proposed model”. Using the average judgments of basic belief assignment by the eight experts (shown in Table 2) as the ground truth, we compare the error rate for the above three methods and the related experimental results are shown in Fig. 5.

From Fig. 5 we can see that the error rate for risk assessment is lowest using our proposed model and the performance of method 2 is better than method 1, the reason lies in the following aspects: (1) Wavelet neural network is an improved version of neural network which is made up three layers: input layer, hidden layer and output layer. All the units in each layer are connected to the nodes located its next layer. The output layer contains a single unit. Particularly, wavelet neural network is constructed with the Gaussian wavelet function. (2) Our proposed modified wavelet neural network can effectively integrate all influencing factors in assessing information security risk by linear integrating several weights.

Next, we will test the influence of the above five types of information security risks by our model under different risk level, the five risk type are “I1: Information Security Risk Vulnerabilities”, “I2: Threat”, “I3: Capability loss”, “I4: Assets lost”, and “I5: System recovery loss”(shown in Fig. 6). In Fig. 6 L."Ij" denote the case of j"th type of risk and l"th risk level.

Experimental results of Fig.6 show that all the risk type is set rightly for all the risk level, and considering the specific risk type can obviously reduce the error rate.

V. CONCLUSIONS

This paper studies on how to design an information security risk assessment model based on an improved wavelet neural network. The training process of wavelet neural networks is implemented by four steps until the value of error function can satisfy pre-defined error criteria. To promote the quality of information security risk assessment, we illustrate a modified version of wavelet neural network by combining all influencing factors in assessing information security risk through linear integrating several weights. The experimental results demonstrate the proposed model is effective and efficient.

TABLE II. BASIC BELIEF ASSIGNMENT FOR MAIN ASSERTION OF INFORMATION SECURITY RISK

<table>
<thead>
<tr>
<th>Experts</th>
<th>BBAL(1)</th>
<th>BBAL(2)</th>
<th>BBAL(3)</th>
<th>BBAL(4)</th>
<th>BBAL(5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1-BBA(1)</td>
<td>0.0863</td>
<td>0.1051</td>
<td>0.2197</td>
<td>0.2762</td>
<td>0.1756</td>
</tr>
<tr>
<td>E1-BBA(2)</td>
<td>0.0858</td>
<td>0.1057</td>
<td>0.2012</td>
<td>0.2771</td>
<td>0.1673</td>
</tr>
<tr>
<td>E1-BBA(3)</td>
<td>0.0861</td>
<td>0.1105</td>
<td>0.2055</td>
<td>0.2962</td>
<td>0.1764</td>
</tr>
<tr>
<td>E1-BBA(4)</td>
<td>0.0867</td>
<td>0.1095</td>
<td>0.2172</td>
<td>0.2772</td>
<td>0.1648</td>
</tr>
<tr>
<td>E1-BBA(5)</td>
<td>0.0911</td>
<td>0.1075</td>
<td>0.2184</td>
<td>0.3031</td>
<td>0.1654</td>
</tr>
<tr>
<td>E1-BBA(6)</td>
<td>0.0929</td>
<td>0.1078</td>
<td>0.2051</td>
<td>0.2898</td>
<td>0.1776</td>
</tr>
<tr>
<td>E1-BBA(7)</td>
<td>0.0908</td>
<td>0.1141</td>
<td>0.2185</td>
<td>0.2792</td>
<td>0.1743</td>
</tr>
<tr>
<td>E1-BBA(8)</td>
<td>0.0887</td>
<td>0.1091</td>
<td>0.2019</td>
<td>0.2900</td>
<td>0.1616</td>
</tr>
<tr>
<td>AVG</td>
<td>0.0886</td>
<td>0.1087</td>
<td>0.2109</td>
<td>0.2861</td>
<td>0.1704</td>
</tr>
</tbody>
</table>

Next, we test the influence of the above five types of information security risks by our model under different

REFERENCES

Transactions On Power Delivery, 24(3) pp. 1174-1181, 2009


