Security Situation Assessment of All-Optical Network Based on Evidential Reasoning Rule

Zhong-Nan Zhao, Pei-Li Qiao, Jian Wang, and Guan-Yu Hu

School of Computer Science and Technology, Harbin University of Science and Technology, Harbin, Heilongjiang 150080, China

Correspondence should be addressed to Zhong-Nan Zhao; piconet@126.com

Received 22 March 2016; Accepted 16 August 2016

Academic Editor: Anna M. Gil-Lafuente

Copyright © 2016 Zhong-Nan Zhao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

It is important to determine the security situations of the all-optical network (AON), which is more vulnerable to hacker attacks and faults than other networks in some cases. A new approach of the security situation assessment to the all-optical network is developed in this paper. In the new assessment approach, the evidential reasoning (ER) rule is used to integrate various evidences of the security factors including the optical faults and the special attacks in the AON. Furthermore, a new quantification method of the security situation is also proposed. A case study of an all-optical network is conducted to demonstrate the effectiveness and the practicability of the new proposed approach.

1. Introduction

With the development of network demand, increasingly importance has been attached to optical fiber communication. Under such background, all-optical network (AON) in which all facilities of the communications are built on the optical fibers is developed, and it has become a trend for the future network systems [1–3]. Some types of the all-optical network have already run in practice, such as WDM-AON [4]. However, the security of the all-optical network should be paid more attention to, because the features of the optical components are very different from the electro- or electrooptical network systems. In some cases, the all-optical network is more vulnerable than other networks. Therefore, it is necessary to assess the security situations of the all-optical network.

The network security situation is a quantized value or interval which can reflect the security status [5–7] of the network platform. Currently, there are many approaches which can assess the network security situation, such as the hierarchical assessment model [8], multiperspective analysis model [9], and data fusion model [10]. But the existing approaches still have some problems.

(1) The above assessment models lack the capacity to process the uncertain and fuzzy information.

(2) There is no security situation assessment approach for all-optical network.

In order to solve the above problems, a new approach of the security situation assessment to the all-optical network is developed in this paper. To solve the first problem, the evidential reasoning (ER) rule is used in the new approach. ER rule is proposed by Yang [11, 12] in 2006, and it has been applied in many fields [13–16]. The ER rule can describe the ignorance and the uncertain information in multiple attribute decision-making.

For the second problem, the assessment process of the all-optical network is very different from other network systems because of the optical components and the optical properties. Therefore, it is necessary to discuss the security assessment method for the all-optical network. In the new proposed approach, many special security factors including special attacks and optical faults are considered in order to obtain the security situations of the all-optical network. The main innovation of the presented work can be concluded as follows:

(1) The security situation assessment for all-optical network is first considered in this paper.
(2) The proposed security situation assessment model which used ER rule can utilize the semiquantitative information and various types of uncertainty.

This paper is organized as follows. In Section 2, the problem for security situation assessment of the all-optical network is formulated. In Section 3, the assessment process based on ER rule is described, and the new quantification method of the security situation is proposed. In Section 4, a case study for assessing the security situations of the all-optical network is given, and the assessment results are analyzed. Finally, the paper is concluded in Section 5.

2. Problem Formulation

2.1. All-Optical Network. As mentioned above, the all-optical network is a special network where the communication nodes do not need optoelectronic conversion and switching. A simple structure of the all-optical network is described in Figure 1, where OXC denotes the optical cross-connect which is used to switch the high-speed optical signals and OADM denotes the optical add-drop multiplexer which is used to multiplex and route different optical channels in WDM systems.

OXC and OADM are significant nodes in all-optical network. They consist of optical multiplexer/demultiplexer, optical switching matrix, wavelength shifter, and node management systems. OLS in Figure 1 denotes the optical line system, which is responsible for the transmission of the optical signal.

2.2. The Security Problem of All-Optical Network. The all-optical network is more vulnerable to hacker attacks and faults in some cases, because the features of the optical components are different from the electrical device. A concept which called survivability is proposed in [17] to describe the security ability of the all-optical network. The survivability includes two parts: fault survivability and attack survivability. The objective of the former refers to locating and restoring the faults. The objective of the latter refers to avoiding the network attacks. Based on the above concept, the security problem of the all-optical network can also be divided into two aspects: the optical faults and the optical attacks.

There are three faults which need to be considered in the all-optical network: OLT fault, OXC fault, and OADM fault, which occurred on the corresponding device. These faults can cause different effects for the all-optical network. Some faults may cause the paralysis of the network transmission.

The network attacks in the all-optical network can be divided into two types [18]: (1) eavesdrop attack which can obtain the optical signal through illegal access [19]; (2) service degradation attack which includes high-power jamming attack (include high-power jamming attack within band and out of band) [20, 21], alien wavelength attack, and signal insertion attack [22].

The purpose of the proposed approach is to assess the security levels of the all-optical network through the above security factors and the ER rule. Furthermore, the quantitative security situation of the all-optical network can also be obtained.

3. Assess the Security Situation of the All-Optical Network by ER Rule

3.1. ER Rule. Assume that there are \( N \) basic attributes \( \{e_1, e_2, \ldots, e_N\} \) of a general attribute \( T \) in a two-level hierarchy, and \( T \) also denotes the security situation grades of the all-optical network in this paper. Let \( \{w_1, w_2, \ldots, w_1, \ldots, w_N\} \) be the weights of the basic attributes, where \( 0 \leq w_i \leq 1 \). Assume that there are \( M \) evaluation grades \( \{G_1, G_2, \ldots, G_2, \ldots, G_M\} \), where \( G_{P,1} \) is preferred to \( G_J \). The assessment of \( e_i \) can be described as

\[
S(e_i) = \{(G_p, \beta^i_j), j = 1, \ldots, M\}, \quad i = 1, \ldots, N,
\]

where \( \beta^i_j \) denotes the belief degree of the \( i \) basic attributes \( e_i \) which assessed to the grade \( G_p \), and \( \sum_{j=1}^{M} \beta^i_j \leq 1 \). If \( \sum_{j=1}^{M} \beta^i_j = 1 \), the assessment of \( T \) is complete. If \( \sum_{j=1}^{M} \beta^i_j < 1 \), the assessment of \( T \) is incomplete.

The ER rule is used to calculate the belief degrees of all the basic attributes by aggregating the assessments. The reasoning process is described as follows [11].

(1) The Calculation of the Basic Probability Mass \( m^i_j \)

\[
m^i_j = w_i \beta^i_j,
\]

where the basic probability mass \( m^i_j \) refers to the degree of the basic attribute \( e_i \) which supports the hypothesis that the attribute is assessed to the grade \( G_J \).

(2) The Calculation of the Remaining Basic Probability Mass \( m^G_i \)

\[
m^G_i = 1 - \sum_{j=1}^{M} m^i_j = 1 - \sum_{j=1}^{M} w_i \beta^i_j = 1 - w_i \sum_{j=1}^{M} \beta^i_j,
\]

where the remaining basic probability mass \( m^G_i \) refers to the degree unassigned to any grade for the basic attribute \( e_i \). It can be divided into two parts:

\[
\overline{m}^G_i = 1 - w_i \left( 1 - \sum_{j=1}^{M} \beta^i_j \right),
\]

where \( \overline{m}^G_i \) denotes the unassigned basic probability mass which is generated because the sum of the weights is not equal to 1. \( \hat{m}^G_i \) denotes the unassigned basic probability mass which is generated because of the uncertainty of assessment.

(3) The Integration of the Evidences. Let \( m_{i(\overline{G})} \) be the integrate probability mass which refers to the degree of the first \( i \) basic attributes which supports the hypothesis that the attribute
is assessed to the grade $G_j$. The integrate process can be described as

$$m^j_{i+1} = K_{i+1} [m^j_{i+1}G + m^j_{i+1}G + m^j_{i+1}G]$$

$$m_{i+1}^G = m_{i}^G + m_{i+1}^G$$

$$m_{i+1}^G = K_{i+1} [m_{i+1}^G + m_{i+1}^G + m_{i+1}^G]$$

$$m_{i+1}^G = K_{i+1} [m_{i+1}^G]$$

$$K_{i+1} = \left[1 - \sum_{k=1}^{M} \sum_{j=1}^{M} m^k_{i+1}m^j_{i+1} \right]^{-1}$$

(4) The Integration of the Belief Degree. According to the above process, the final belief degrees of the general attribute $T$ can be obtained:

$$\beta^j = \frac{m^j_{i+1}}{1 - m_{i+1}^G}$$

$$\beta^G = \frac{m_{i+1}^G}{1 - m_{i+1}^G}$$

$$S(T) = \{(G_j, \beta^j), j = 1, \ldots, M\}.$$  

3.2. Security Situation Assessment of the All-Optical Network with ER Rule. As mentioned above, the security situation of the all-optical network can be assessed by ER rule. The details of the process are shown as follows.

(1) The Setting of the Basic Attributes. The basic attributes of the assessment include the faults and the attacks, as shown in Figure 2.

(2) The Collection and Pretreatment of All-Optical Network Data. The data of the all-optical network should be pretreated

<table>
<thead>
<tr>
<th>$G_1$ (excellent)</th>
<th>$G_2$ (good)</th>
<th>$G_3$ (general)</th>
<th>$G_4$ (bad)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e_{11}$</td>
<td>$g_{11} = 0$</td>
<td>$g_{11} = 0$</td>
<td>$g_{11} = 1$</td>
</tr>
<tr>
<td>$e_{12}$</td>
<td>$g_{12} = 0$</td>
<td>$g_{12} = 0$</td>
<td>$g_{12} = 1$</td>
</tr>
<tr>
<td>$e_{13}$</td>
<td>$g_{13} = 0$</td>
<td>$g_{13} = 0$</td>
<td>$g_{13} = 1$</td>
</tr>
<tr>
<td>$e_{21}$</td>
<td>$g_{21} = 0/\ h$</td>
<td>$g_{21} = 3/\ h$</td>
<td>$g_{21} = 6/\ h$</td>
</tr>
<tr>
<td>$e_{22}$</td>
<td>$g_{22} = 0/\ h$</td>
<td>$g_{22} = 2/\ h$</td>
<td>$g_{22} = 4/\ h$</td>
</tr>
<tr>
<td>$e_{23}$</td>
<td>$g_{23} = 0/\ h$</td>
<td>$g_{23} = 2/\ h$</td>
<td>$g_{23} = 4/\ h$</td>
</tr>
</tbody>
</table>

3.3. Evaluation Rules Formulation. In this paper, the evaluation grades are set to $G_1 = \text{excellent}$, $G_2 = \text{good}$, $G_3 = \text{general}$, $G_4 = \text{bad}$. Let $g$ be the reference values of the input data, and its subscript has the same meaning as in $e$. The assessment rules can be established through the evaluation grades, as shown in Table 1.

(4) The Feature Extraction. The features of the input data need to be extracted in order to get the belief degrees of the evaluation grades through the above assessment rules.
4 Mathematical Problems in Engineering

Security of all-optical network (T)

Service degradation (e_{12})

Attacks (e_2)

Faults (e_1)

OADM fault (e_{13})

OLT fault (e_{11})

High-power jamming (e_{21})

Alien wavelength (e_{22})

Signal insertion (e_{23})

Figure 2: The basic attributes of the all-optical network security assessment.

<table>
<thead>
<tr>
<th>Security of all-optical network (T)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OADM fault (e_{13})</td>
</tr>
<tr>
<td>OXC fault (e_{12})</td>
</tr>
<tr>
<td>Faults (e_1)</td>
</tr>
<tr>
<td>Service degradation (e_{12})</td>
</tr>
<tr>
<td>Attacks (e_2)</td>
</tr>
</tbody>
</table>

Table 2: The belief degrees of e_{11}, e_{12}, e_{13} given by experts.

<table>
<thead>
<tr>
<th></th>
<th>G_1 (excellent)</th>
<th>G_2 (good)</th>
<th>G_3 (general)</th>
<th>G_4 (bad)</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>e_{11} = 0</td>
<td>\beta_{11} = 0.7</td>
<td>\beta_{11} = 0.3</td>
<td>\beta_{11} = 0</td>
<td>\beta_{11} = 0</td>
<td>\beta_{11} = 0</td>
</tr>
<tr>
<td>e_{11} = 1</td>
<td>\beta_{11} = 0</td>
<td>\beta_{11} = 0</td>
<td>\beta_{11} = 0.3</td>
<td>\beta_{11} = 0.7</td>
<td>\beta_{11} = 0</td>
</tr>
<tr>
<td>e_{12} = 0</td>
<td>\beta_{12} = 0</td>
<td>\beta_{12} = 0</td>
<td>\beta_{12} = 0</td>
<td>\beta_{12} = 0</td>
<td>\beta_{12} = 0</td>
</tr>
<tr>
<td>e_{12} = 1</td>
<td>\beta_{12} = 0</td>
<td>\beta_{12} = 0</td>
<td>\beta_{12} = 0.2</td>
<td>\beta_{12} = 0.8</td>
<td>\beta_{12} = 0</td>
</tr>
<tr>
<td>e_{13} = 0</td>
<td>\beta_{13} = 0</td>
<td>\beta_{13} = 0</td>
<td>\beta_{13} = 0</td>
<td>\beta_{13} = 0</td>
<td>\beta_{13} = 0</td>
</tr>
<tr>
<td>e_{13} = 1</td>
<td>\beta_{13} = 0</td>
<td>\beta_{13} = 0</td>
<td>\beta_{13} = 0.1</td>
<td>\beta_{13} = 0.9</td>
<td>\beta_{13} = 0</td>
</tr>
</tbody>
</table>

The feature extraction can be realized through the following formula:

\[ \beta^k_i = \frac{g_{i}^{k+1} - V(e_i)}{g_{i}^{k+1} - g_{i}^k} \quad (g_i^k \leq V(e_i) \leq g_i^{k+1}) \]  

\[ \beta_i^{k+1} = 1 - \beta^k_{ji} \]  

\[ \beta_i^k = 1 \quad (k = 1, \ldots, M, \ k \neq j, j + 1) \]

(14)

where \( V(e_i) \) denotes value of the evidence \( e_i \).

The evidences with Boolean form cannot be used in the above equation. Therefore, the belief degrees of \( e_{11}, e_{12}, e_{13} \) should be given by experts directly, as shown in Table 2.

(5) The Assessment Process with ER Algorithm. When the belief degrees are obtained through (14), the general attribute \( T \) which denotes the security situation grades of the all-optical network can be calculated by ER rule, as described in the above section, where the weights can be given by the experts according to the experience. Note that the assessment process should be carried out layer by layer, which means that the evidences \( e_{221}, e_{222}, e_{223} \) in the bottom layer will be integrated first.

(6) The Quantification of the Security Situation. The final belief degrees of the general attribute \( S(T) = \{(G_j, \beta^j), \ j = 1, \ldots, M\} \) can be obtained through step (5). Let reference values of security situation be \( G(g_j^1 = 0, g_j^2 = 0.35, g_j^3 = 0.7, g_j^4 = 1) \); a new method which can calculate the quantization value \( V(T) \) of the security situation in all-optical network is proposed in this paper, as shown in

\[ V(T) = \sum_{j=1}^{M} g_{ij} \beta^j_i. \]  

(15)

4. Case Study

In this section, the assessment of the security situation in an all-optical network platform is studied in order to demonstrate the effectiveness of the new proposed approach. An all-optical network platform as shown in Figure 1 is established, and the data as shown in (13) are collected within 24 hours.

In order to get the assessment results of the security situations in the all-optical network, the procedure of the evidence integration should be carried out layer by layer. Take a data within 1 hour as an example; the form of the data is \( \{e_1|e_{11} = 0, e_{12} = 0, e_{13} = 1\}, e_2|e_{21} = 5, e_{22} = 3, e_{22} = 1, e_{223} = 5\} \) which means that OADM fault occurred, and there are 5 eavesdrop attacks, 3 high-power jamming attacks, 1 alien wavelength attack, and 5 signal insertion attacks within 1 hour.

Firstly, the bottom layer \( \{e_{221} = 3, e_{222} = 1, e_{223} = 5\} \) should be integrated by ER rule in order to get the assessment result of the service degradation \( e_{22} \). The belief degrees of the bottom layer can be calculated by (14) according to the assessment rules, as shown in Table 3.

Let the weights of the evidences in the bottom layer be \( \{w_{221} = 0.4, w_{222} = 0.3, w_{223} = 0.3\} \), which are given by
Table 3: The belief degrees of the bottom layer.

<table>
<thead>
<tr>
<th></th>
<th>G₁ (excellent)</th>
<th>G₂ (good)</th>
<th>G₃ (general)</th>
<th>G₄ (bad)</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>e₂₁₂</td>
<td>β₂₁₂ = 0</td>
<td>β₂₁₂ = 0.5</td>
<td>β₂₁₂ = 0.5</td>
<td>β₂₁₂ = 0</td>
<td>β₂₁₂ = 0</td>
</tr>
<tr>
<td>e₂₂₂</td>
<td>β₂₂₂ = 0.5</td>
<td>β₂₂₂ = 0.5</td>
<td>β₂₂₂ = 0</td>
<td>β₂₂₂ = 0</td>
<td>β₂₂₂ = 0</td>
</tr>
<tr>
<td>e₂₂₃</td>
<td>β₂₂₃ = 0</td>
<td>β₂₂₃ = 0</td>
<td>β₂₂₃ = 0.5</td>
<td>β₂₂₃ = 0.5</td>
<td>β₂₂₃ = 0</td>
</tr>
</tbody>
</table>

Experts. Then the basic probability mass can be calculated by (2), as shown in Table 4.

Then the integration process of \( \{ e_{221} = 3, e_{222} = 1, e_{223} = 5 \} \) with ER rule can be described as follows.

(1) Integrating Evidences in the Bottom Layer. The first step is integrating \( \{ e_{221}, e_{222} \} \) in the bottom layer and calculating \( K_{I(222)} \) by (9):

\[
K_{I(222)} = \left[ 1 - \sum_{k=1}^{M} \sum_{j=1}^{M} m_{R_{221}}^k m_{j_{222}}^j \right]^{-1}
\]

(16)

And then the basic probability mass of the integrated evidences \( \{ e_{221}, e_{222} \} \) can be calculated by (5)–(8):

\[
m_{I(222)}^j = K_{I(222)} \left[ m_{221}^j m_{222}^j + m_{221}^G m_{222}^j + m_{221}^j m_{222}^G \right]
\]

(19)

\[
\bar{m}_{I(222)}^G = K_{I(222)} \left[ \bar{m}_{222}^G + \bar{m}_{221}^G m_{222}^G + \bar{m}_{221}^G m_{222}^G \right] = 0
\]

(17)

\[
m_{I(222)}^G = \bar{m}_{I(222)}^G = \bar{m}_{222}^G = 0.4615
\]

(18)

The above masses refer to the importance degree of the integrated evidences \( \{ e_{211}, e_{222} \} \) for the decision. The second step is integrating \( \{ e_{221}, e_{222} \} \) and \( \{ e_{223} \} \) and calculating \( K_{I(223)} \) by (9):

\[
K_{I(223)} = \left[ 1 - \sum_{k=1}^{M} \sum_{j=1}^{M} m_{R_{222}}^k m_{j_{223}}^j \right]^{-1}
\]

(19)

And then basic probability mass of integrated evidence \( \{ e_{221}, e_{222} \} \) and \( \{ e_{223} \} \) can be calculated by (5)–(8):

\[
m_{I(223)}^j = K_{I(223)} \left[ m_{I(222)}^j m_{223}^j + m_{I(222)}^G m_{223}^j + m_{I(222)}^j m_{223}^G \right]
\]

\[
\bar{m}_{I(223)}^G = K_{I(223)} \left[ \bar{m}_{I(222)}^G + \bar{m}_{I(222)}^G m_{223}^G + \bar{m}_{I(222)}^G m_{223}^G \right] = 0
\]

(19)

\[
m_{I(223)}^G = \bar{m}_{I(223)}^G = \bar{m}_{223}^G = 0.2655
\]

The above masses refer to the importance degree of the integrated evidences \( \{ e_{211}, e_{222} \} \) for the decision. Then the belief degrees of the evidence \( e_2 \) can be obtained by (10) and (11), as shown in Table 5.

(2) Integrating Evidences \( e_2 \) and \( e_2 \) in the Third Layer. In this layer, the first step is calculating the belief degrees of the evidence \( e_2 \) by (14), as shown in Table 6.

Let the weights of the evidences \( e_2 \) and \( e_2 \) be \( \{ w_{21} = 0.35, w_{22} = 0.65 \} \), which mean that the service degradation attack has more threat than the eavesdrop attack. Then the basic probability mass can be calculated by (2), as shown in Table 7.

Thus, the integrating procedure of \( e_2 \) and \( e_2 \) can be described as follows:

\[
K_{I(22)} = \left[ 1 - \sum_{k=1}^{M} \sum_{j=1}^{M} m_{R_{222}}^k m_{j_{222}}^j \right]^{-1}
\]

(19)

\[
m_{I(22)}^j = K_{I(22)} \left[ m_{221}^j m_{222}^j + m_{221}^G m_{222}^j + m_{221}^j m_{222}^G \right]
\]

\[
\bar{m}_{I(22)}^G = K_{I(22)} \left[ \bar{m}_{222}^G + \bar{m}_{221}^G m_{222}^G + \bar{m}_{221}^G m_{222}^G \right] = 0
\]

(17)

\[
m_{I(22)}^G = \bar{m}_{I(22)}^G = \bar{m}_{222}^G = 0.2655
\]

(18)
Table 4: The basic probability mass of the bottom layer.

<table>
<thead>
<tr>
<th>$e_{221}$</th>
<th>$m_{221}^1 = 0$</th>
<th>$m_{221}^2 = 0.2$</th>
<th>$m_{221}^3 = 0.2$</th>
<th>$m_{221}^4 = 0$</th>
<th>$\bar{m}_{221}^G = 0.6$</th>
<th>$\bar{m}_{221} = 0$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e_{222}$</td>
<td>$m_{222}^1 = 0.15$</td>
<td>$m_{222}^2 = 0.15$</td>
<td>$m_{222}^3 = 0$</td>
<td>$m_{222}^4 = 0$</td>
<td>$\bar{m}_{222}^G = 0.7$</td>
<td>$\bar{m}_{222} = 0$</td>
</tr>
<tr>
<td>$e_{223}$</td>
<td>$m_{223}^1 = 0$</td>
<td>$m_{223}^2 = 0.15$</td>
<td>$m_{223}^3 = 0.15$</td>
<td>$m_{223}^4 = 0$</td>
<td>$\bar{m}_{223}^G = 0.7$</td>
<td>$\bar{m}_{223} = 0$</td>
</tr>
</tbody>
</table>

Table 5: The belief degrees of the evidence $e_{22}$.

<table>
<thead>
<tr>
<th>$G_i$ (excellent)</th>
<th>$G_2$ (good)</th>
<th>$G_3$ (general)</th>
<th>$G_4$ (bad)</th>
<th>$G$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e_{22}$</td>
<td>$\beta_{22}^1 = 0.1286$</td>
<td>$\beta_{22}^2 = 0.3714$</td>
<td>$\beta_{22}^3 = 0.3714$</td>
<td>$\beta_{22}^4 = 0.1286$</td>
</tr>
</tbody>
</table>

Table 6: The belief degrees of the evidence $e_{21}$.

<table>
<thead>
<tr>
<th>$G_i$ (excellent)</th>
<th>$G_2$ (good)</th>
<th>$G_3$ (general)</th>
<th>$G_4$ (bad)</th>
<th>$G$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e_{21}$</td>
<td>$\beta_{21}^1 = 0.3333$</td>
<td>$\beta_{21}^2 = 0.6667$</td>
<td>$\beta_{21}^3 = 0$</td>
<td>$\beta_{21}^G = 0$</td>
</tr>
</tbody>
</table>

(3) Integrating Evidences $e_{11}, e_{12},$ and $e_{13}$ in the Third Layer. In order to get the assessment results of $e_{11}$, the evidences $e_{11}, e_{12},$ and $e_{13}$ must be integrated first. As mentioned above, these evidences reflect the faults of all-optical network, and they are Boolean forms, which mean that the belief degrees are given by experts directly, as shown in Table 2. The integration process of the evidences $e_{11}, e_{12},$ and $e_{13}$ is the same as other evidences. Let the weights be $\{w_{11} = 0.3, w_{12} = 0.3, w_{13} = 0.4\}$; here the assessment results are given directly, as shown in Table 9.

(4) Getting the Final Assessment Result by Integrating Evidences $e_1$ and $e_2$ in the Second Layer. In this step, the final assessment result can be obtained, as shown in Table 10. In Table 10, the assessment result of the all-optical network based on the condition $[e_1 \land e_{12} = 0, e_{13} = 1, e_2 \land (e_{221} = 5, e_{222} = 3, e_{223} = 1, e_{223} = 5)]$ is obtained, where the proportion of excellent level is 27.15%, the proportion of good level is 25.51%, the proportion of general level is 24.69%, the proportion of bad level is 22.64%, and the remaining belief degree is 0%, which means that the assessment is complete. It can be seen that the network managers are inconvenient to make decision by using the above assessment result. Therefore, it is necessary to calculate the quantization value of the all-optical network security situation.

(5) Calculating the Quantization Security Situation of the All-Optical Network. The quantization security situation of the all-optical network can be calculated by (15):

$$V(T) = \sum_{j=1}^{M} a_j^i b_j^i = 0.4885.$$  \hspace{1cm} (21)

This situation is only one of the values in 24 hours, and the complete situations are shown in Figure 3.

5. Conclusions

It is difficult to assess the all-optical network security situation because of the complex factors including the optical faults and the special attacks. In this paper, the ER rule which can integrate various evidences is first used to establish the assessment model of the all-optical network. The belief degrees of the security levels can be obtained by using the ER rule. But the results with belief degrees are inconvenient to make decision for network managers. Therefore, a new quantification method of all-optical network security situation is proposed. The uncertain information and the ignorance are well handled in the new proposed approach including the ER rule and the quantification method. The advantages and limitations of the proposed method in this paper can be concluded as follows:

(1) The assessment method can integrate a variety of different types of characteristic factors which include quantitative data and qualitative knowledge.

(2) The assessment method is not suitable to solve the dynamic problems and need expert guidance to determine the weight of the factors.

The case study in Section 4 demonstrates the effectiveness and the practicability of the approach.

Competing Interests

The authors declare that there are no competing interests regarding the publication of this manuscript.
Table 7: The basic probability mass of the evidences $e_{21}$ and $e_{22}$.

<table>
<thead>
<tr>
<th>$e_{21}$</th>
<th>$m_{21}^1$</th>
<th>$m_{21}^2$</th>
<th>$m_{21}^3$</th>
<th>$m_{21}^4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_1$</td>
<td>0</td>
<td>0.1167</td>
<td>0.2333</td>
<td>0</td>
</tr>
<tr>
<td>$G_2$</td>
<td>0.0836</td>
<td>0.2414</td>
<td>0.2414</td>
<td>0.0836</td>
</tr>
</tbody>
</table>

Table 8: The belief degrees of the evidence $e_2$.

<table>
<thead>
<tr>
<th>$G_1$ (excellent)</th>
<th>$G_2$ (good)</th>
<th>$G_3$ (general)</th>
<th>$G_4$ (bad)</th>
<th>$G$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\beta^1_2 = 0.0863$</td>
<td>$\beta^2_2 = 0.3589$</td>
<td>$\beta^3_2 = 0.4685$</td>
<td>$\beta^4_2 = 0.0863$</td>
<td>$\beta^4_G = 0$</td>
</tr>
</tbody>
</table>

Table 9: The belief degrees of the evidence $e_1$.

<table>
<thead>
<tr>
<th>$G_1$ (excellent)</th>
<th>$G_2$ (good)</th>
<th>$G_3$ (general)</th>
<th>$G_4$ (bad)</th>
<th>$G$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\beta^1_1 = 0.4535$</td>
<td>$\beta^2_1 = 0.1376$</td>
<td>$\beta^3_1 = 0.0407$</td>
<td>$\beta^4_1 = 0.3664$</td>
<td>$\beta^4_G = 0$</td>
</tr>
</tbody>
</table>

Table 10: The belief degrees of security situation $T$.

<table>
<thead>
<tr>
<th>$G_1$ (excellent)</th>
<th>$G_2$ (good)</th>
<th>$G_3$ (general)</th>
<th>$G_4$ (bad)</th>
<th>$G$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\beta^1_T = 0.2715$</td>
<td>$\beta^2_T = 0.2551$</td>
<td>$\beta^3_T = 0.2469$</td>
<td>$\beta^4_T = 0.2264$</td>
<td>$\beta^4_G = 0$</td>
</tr>
</tbody>
</table>

Acknowledgments

This present research work was supported by the National Natural Science Foundation of China (61403109) and the Scientific Research Fund of Heilongjiang Provincial Education Department (12541169).

References


