Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2016, Article ID 9312476, 7 pages
http://dx.doi.org/10.1155/2016/9312476

Research Article

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

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 $\{e_1, e_2, \ldots, e_i, \ldots, e_N\}$ 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 $\{w_1, w_2, \ldots, w_i, \ldots, w_N\}$ be the weights of the basic attributes, where $0 \le w_i \le 1$. Assume that there are M evaluation grades $\{G_1, G_2, \ldots, G_j, \ldots, G_M\}$, where G_{j+1} is preferred to G_j. The assessment of e_i can be described as

$$S(e_i) = \left\{\left(G_j, \beta_i^j\right),\ j = 1, \ldots, M\right\} \quad i = 1, \ldots, N, \tag{1}$$

where β_i^j denotes the belief degree of the i basic attributes e_i which is assessed to the grade G_j, and $\sum_{j=1}^{M} \beta_i^j \le 1$. 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

$$m_i^j = w_i \beta_i^j, \tag{2}$$

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_i^G

$$m_i^G = 1 - \sum_{j=1}^{M} m_i^j = 1 - \sum_{j=1}^{M} w_i \beta_i^j = 1 - w_i \sum_{j=1}^{M} \beta_i^j, \tag{3}$$

where the remaining basic probability mass m_i^G refers to the degree unassigned to any grade for the basic attribute e_i. It can be divided into two parts:

$$\begin{aligned} \overline{m}_i^G &= 1 - w_i \\ \widetilde{m}_i^G &= w_i \left(1 - \sum_{j=1}^{M} \beta_i^j\right), \end{aligned} \tag{4}$$

where $\overline{m}_i^G$ denotes the unassigned basic probability mass which is generated because the sum of the weights is not equal to 1. $\widetilde{m}_i^G$ denotes the unassigned basic probability mass which is generated because of the uncertainty of assessment.

(3) The Integration of the Evidences. Let $m_{I(i)}^j$ be the integrate probability mass which refers to the degree of the first i basic attributes which supports the hypothesis that the attribute

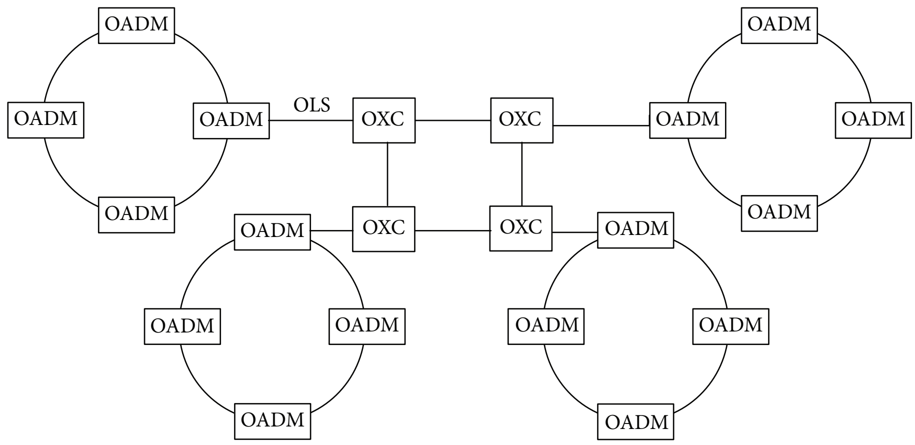

FIGURE 1: A simple structure of all-optical network.

is assessed to the grade G_j. The integrate process can be described as

$$m^j_{I(i+1)} = K_{I(i+1)} \left[m^j_{I(i)} m^j_{i+1} + m^G_{I(i)} m^j_{i+1} + m^j_{I(i)} m^G_{i+1} \right] \quad (5)$$

$$m^G_{I(i)} = \bar{m}^G_{I(i)} + \tilde{m}^G_{I(i)} \quad (6)$$

$$\tilde{m}^G_{I(i+1)} = K_{I(i+1)} \left[\tilde{m}^G_{I(i)} \tilde{m}^G_{i+1} + \tilde{m}^G_{I(i)} \bar{m}^G_{i+1} + \bar{m}^G_{I(i)} \tilde{m}^G_{i+1} \right] \quad (7)$$

$$\bar{m}^G_{I(i+1)} = K_{I(i+1)} \left[\bar{m}^G_{I(i)} \bar{m}^G_{i+1} \right] \quad (8)$$

$$K_{I(i+1)} = \left[1 - \sum_{k=1}^{M} \sum_{\substack{j=1 \\ j \neq k}}^{M} m^k_{I(i)} m^j_{i+1} \right]^{-1}. \quad (9)$$

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

$$\beta^j = \frac{m^j_{I(N)}}{1 - m^G_{I(N)}} \quad (10)$$

$$\beta^G = \frac{\tilde{m}^G_{I(N)}}{1 - \bar{m}^G_{I(N)}} \quad (11)$$

$$S(T) = \left\{ \left(G_j, \beta^j \right), \ j = 1, \ldots, M \right\}. \quad (12)$$

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 after the collection in order to extract the assessment evidences. The pretreatment form of the input data is as follows according to Figure 2:

$$\{e_1 \{e_{11}, e_{12}, e_{13}\}, e_2 \{e_{21}, e_{22} \{e_{221}, e_{222}, e_{223}\}\}\}, \quad (13)$$

where e_{11}, e_{12}, e_{13} denote the three faults on the different optical components and they are Boolean forms, 0 denotes no fault, and 1 denotes fault within 1 hour. $e_{221}, e_{222}, e_{223}$ denote the average frequency of the different attacks within 1 hour, and they are positive number. It is assumed that the maximum frequency of the service degradation is 6 times and the maximum frequency of the eavesdrop attacks is 10 times within 1 hour.

(3) The Formulation of the Assessment Rules. 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.

TABLE 1: The assessment rules of all-optical network.

	G_1 (excellent)	G_2 (good)	G_3 (general)	G_4 (bad)
e_{11}	$g^1_{11} = 0$	$g^2_{11} = 0$	$g^3_{11} = 1$	$g^4_{11} = 1$
e_{12}	$g^1_{12} = 0$	$g^2_{12} = 0$	$g^3_{12} = 1$	$g^4_{12} = 1$
e_{13}	$g^1_{13} = 0$	$g^2_{13} = 0$	$g^3_{13} = 0$	$g^4_{13} = 1$
e_{21}	$g^1_{21} = 0/h$	$g^2_{21} = 3/h$	$g^3_{21} = 6/h$	$g^4_{21} = 10/h$
e_{221}	$g^1_{221} = 0/h$	$g^2_{221} = 2/h$	$g^3_{221} = 4/h$	$g^4_{221} = 6/h$
e_{222}	$g^1_{222} = 0/h$	$g^2_{222} = 2/h$	$g^3_{222} = 4/h$	$g^4_{222} = 6/h$
e_{223}	$g^1_{223} = 0/h$	$g^2_{223} = 2/h$	$g^3_{223} = 4/h$	$g^4_{223} = 6/h$

(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.

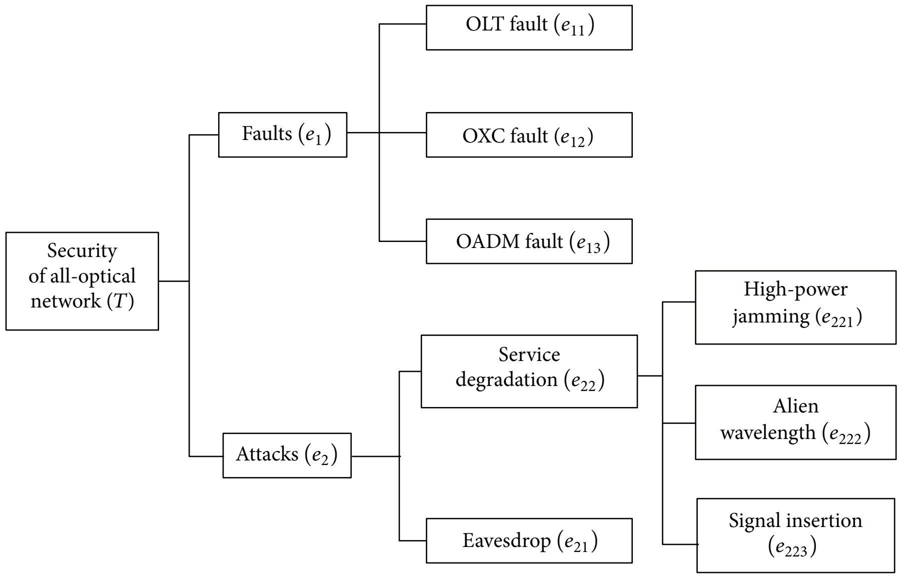

Figure 2: The basic attributes of the all-optical network security assessment.

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

	G_1 (excellent)	G_2 (good)	G_3 (general)	G_4 (bad)	G
$e_{11} = 0$	$\beta_{11}^1 = 0.7$	$\beta_{11}^2 = 0.3$	$\beta_{11}^3 = 0$	$\beta_{11}^4 = 0$	$\beta_{11}^G = 0$
$e_{11} = 1$	$\beta_{11}^1 = 0$	$\beta_{11}^2 = 0$	$\beta_{11}^3 = 0.3$	$\beta_{11}^4 = 0.7$	$\beta_{11}^G = 0$
$e_{12} = 0$	$\beta_{12}^1 = 0.8$	$\beta_{12}^2 = 0.2$	$\beta_{12}^3 = 0$	$\beta_{12}^4 = 0$	$\beta_{12}^G = 0$
$e_{12} = 1$	$\beta_{12}^1 = 0$	$\beta_{12}^2 = 0$	$\beta_{12}^3 = 0.2$	$\beta_{12}^4 = 0.8$	$\beta_{12}^G = 0$
$e_{13} = 0$	$\beta_{13}^1 = 0.9$	$\beta_{13}^2 = 0.1$	$\beta_{13}^3 = 0$	$\beta_{13}^4 = 0$	$\beta_{13}^G = 0$
$e_{13} = 1$	$\beta_{13}^1 = 0$	$\beta_{13}^2 = 0$	$\beta_{13}^3 = 0.1$	$\beta_{13}^4 = 0.9$	$\beta_{13}^G = 0$

The feature extraction can be realized through the following formula:

$$\begin{aligned} \beta_i^j &= \frac{g_i^{j+1} - V(e_i)}{g_i^{j+1} - g_i^j} \quad \left(g_i^j \le V(e_i) \le g_i^{j+1}\right) \\ \beta_i^{j+1} &= 1 - \beta_{j,i} \\ \beta_i^k &= 0 \quad \left(k = 1, \ldots, M,\ k \ne j, j+1\right), \end{aligned} \tag{14}$$

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 $G\{g_T^1 = 0, g_T^2 = 0.35, g_T^3 = 0.7, g_T^4 = 1\}$; 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

$$V(T) = \sum_{j=1}^{M} g_T^j \beta^j. \tag{15}$$

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 $\{e_1\{e_{11} = 0, e_{12} = 0, e_{13} = 1\}, e_2\{e_{21} = 5, e_{22}\{e_{221} = 3, e_{222} = 1, e_{223} = 5\}\}\}$ 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.

	G_1 (excellent)	G_2 (good)	G_3 (general)	G_4 (bad)	G
e_{221}	$\beta^1_{221} = 0$	$\beta^2_{221} = 0.5$	$\beta^3_{221} = 0.5$	$\beta^4_{221} = 0$	$\beta^G_{221} = 0$
e_{222}	$\beta^1_{222} = 0.5$	$\beta^2_{222} = 0.5$	$\beta^3_{222} = 0$	$\beta^4_{222} = 0$	$\beta^G_{222} = 0$
e_{223}	$\beta^1_{223} = 0$	$\beta^2_{223} = 0$	$\beta^3_{223} = 0.5$	$\beta^4_{223} = 0.5$	$\beta^G_{223} = 0$

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):

$$K_{I(222)} = \left[1 - \sum_{k=1}^{M}\sum_{\substack{j=1\\ j\neq k}}^{M} m^k_{I(221)} m^j_{222}\right]^{-1} = \left[1 - \sum_{k=1}^{M}\sum_{\substack{j=1\\ j\neq k}}^{M} m^k_{221} m^j_{222}\right]^{-1} = 1.0989. \tag{16}$$

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

$$\begin{aligned} m^j_{I(222)} &= K_{I(222)}\left[m^j_{221} m^j_{222} + m^G_{221} m^j_{222} + m^j_{221} m^G_{222}\right] \\ &= [0.0989, 0.2857, 0.1538, 0] \\ \widetilde{m}^G_{I(222)} &= K_{I(222)}\left[\widetilde{m}^G_{221}\widetilde{m}^G_{222} + \widetilde{m}^G_{221}\overline{m}^G_{222} + \overline{m}^G_{221}\widetilde{m}^G_{222}\right] \\ &= 0 \\ \overline{m}^G_{I(222)} &= K_{I(222)}\left[\overline{m}^G_{221}\overline{m}^G_{222}\right] = 0.4615 \\ m^G_{I(222)} &= \overline{m}^G_{I(222)} + \widetilde{m}^G_{I(222)} = 0.4615. \end{aligned} \tag{17}$$

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

$$K_{I(223)} = \left[1 - \sum_{k=1}^{M}\sum_{\substack{j=1\\ j\neq k}}^{M} m^k_{I(222)} m^j_{223}\right]^{-1} = 1.1607. \tag{18}$$

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

$$\begin{aligned} & m^j_{I(223)} \\ &\quad = K_{I(223)}\left[m^j_{I(222)} m^j_{223} + m^G_{I(222)} m^j_{223} + m^j_{I(222)} m^G_{223}\right] \\ &\quad = [0.0804, 0.2321, 0.2321, 0.0804] \\ & \widetilde{m}^G_{I(223)} \\ &\quad = K_{I(223)}\left[\widetilde{m}^G_{I(222)}\widetilde{m}^G_{223} + \widetilde{m}^G_{I(222)}\overline{m}^G_{223} + \overline{m}^G_{I(222)}\widetilde{m}^G_{223}\right] \\ &\quad = 0 \\ & \overline{m}^G_{I(223)} = K_{I(223)}\left[\overline{m}^G_{I(222)}\overline{m}^G_{223}\right] = 0.3750 \\ & m^G_{I(223)} = \overline{m}^G_{I(223)} + \widetilde{m}^G_{I(223)} = 0.3750. \end{aligned} \tag{19}$$

The above masses refer to the importance degree of the integrated evidences in the bottom layer for the decision. Then the belief degrees of the evidence e_{22} can be obtained by (10) and (11), as shown in Table 5.

(2) Integrating Evidences e_{21} and e_{22} in the Third Layer. In this layer, the first step is calculating the belief degrees of the evidence e_{21} by (14), as shown in Table 6.

Let the weights of the evidences e_{21} and e_{22} 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_{21} and e_{22} can be described as follows:

$$\begin{aligned} K_{I(22)} &= \left[1 - \sum_{k=1}^{M}\sum_{\substack{j=1\\ j\neq k}}^{M} m^k_{I(21)} m^j_{22}\right]^{-1} \\ &= \left[1 - \sum_{k=1}^{M}\sum_{\substack{j=1\\ j\neq k}}^{M} m^k_{21} m^j_{22}\right]^{-1} = 1.1669 \\ m^j_{I(22)} &= K_{I(22)}\left[m^j_{21} m^j_{22} + m^G_{21} m^j_{22} + m^j_{21} m^G_{22}\right] \\ &= [0.0634, 0.2636, 0.3441, 0.0634] \\ \widetilde{m}^G_{I(22)} &= K_{I(22)}\left[\widetilde{m}^G_{21}\widetilde{m}^G_{22} + \widetilde{m}^G_{21}\overline{m}^G_{22} + \overline{m}^G_{21}\widetilde{m}^G_{22}\right] = 0 \\ \overline{m}^G_{I(22)} &= K_{I(22)}\left[\overline{m}^G_{21}\overline{m}^G_{22}\right] = 0.2655 \\ m^G_{I(22)} &= \overline{m}^G_{I(22)} + \widetilde{m}^G_{I(22)} = 0.2655. \end{aligned} \tag{20}$$

The above masses refer to the importance degree of the integrated evidences $\{e_{21}, e_{22}\}$ for the decision. Then the belief degrees of the evidence e_2 can be obtained by (10) and (11), as shown in Table 8.

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

e_{221}	$m^1_{221} = 0$	$m^2_{221} = 0.2$	$m^3_{221} = 0.2$	$m^4_{221} = 0$	$\overline{m}^G_{221} = 0.6$	$\widetilde{m}^G_{221} = 0$
e_{222}	$m^1_{222} = 0.15$	$m^2_{222} = 0.15$	$m^3_{222} = 0$	$m^4_{222} = 0$	$\overline{m}^G_{222} = 0.7$	$\widetilde{m}^G_{222} = 0$
e_{223}	$m^1_{223} = 0$	$m^2_{223} = 0$	$m^3_{223} = 0.15$	$m^4_{223} = 0.15$	$\overline{m}^G_{223} = 0.7$	$\widetilde{m}^G_{223} = 0$

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

	G_1 (excellent)	G_2 (good)	G_3 (general)	G_4 (bad)	G
e_{22}	$\beta^1_{22} = 0.1286$	$\beta^2_{22} = 0.3714$	$\beta^3_{22} = 0.3714$	$\beta^4_{22} = 0.1286$	$\beta^G_{22} = 0$

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

	G_1 (excellent)	G_2 (good)	G_3 (general)	G_4 (bad)	G
e_{21}	$\beta^1_{21} = 0$	$\beta^2_{21} = 0.3333$	$\beta^3_{21} = 0.6667$	$\beta^4_{21} = 0$	$\beta^G_{21} = 0$

(3) Integrating Evidences e_{11}, e_{12}, and e_{13} in the Third Layer. In order to get the assessment results of e_1, 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 $\{e_1\{e_{11} = 0, e_{12} = 0, e_{13} = 1\}, e_2\{e_{21} = 5, e_{22}\{e_{221} = 3, e_{222} = 1, e_{223} = 5\}\}\}$ 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 the that 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):

$$V(T) = \sum_{j=1}^{M} g_T^j \beta^j = 0.4885. \tag{21}$$

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

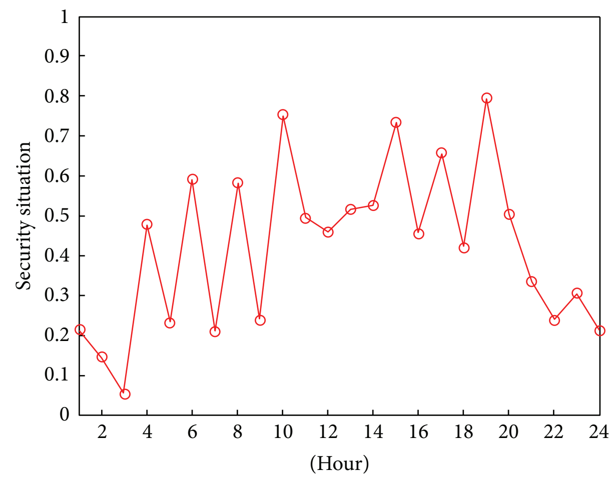

Figure 3: The security situation of the all-optical network in 24 hours.

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 manager. 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}.

e_{21}	$m_{21}^1 = 0$	$m_{21}^2 = 0.1167$	$m_{21}^3 = 0.2333$	$m_{21}^4 = 0$	$\overline{m}_{21}^G = 0.65$	$\widetilde{m}_{21}^G = 0$
e_{22}	$m_{22}^1 = 0.0836$	$m_{22}^2 = 0.2414$	$m_{22}^3 = 0.2414$	$m_{22}^4 = 0.0836$	$\overline{m}_{22}^G = 0.35$	$\widetilde{m}_{22}^G = 0$

Table 8: The belief degrees of the evidence e_2.

	G_1 (excellent)	G_2 (good)	G_3 (general)	G_4 (bad)	G
e_{22}	$\beta_2^1 = 0.0863$	$\beta_2^2 = 0.3589$	$\beta_2^3 = 0.4685$	$\beta_2^4 = 0.0863$	$\beta_2^G = 0$

Table 9: The belief degrees of the evidence e_1.

	G_1 (excellent)	G_2 (good)	G_3 (general)	G_4 (bad)	G
e_{22}	$\beta_1^1 = 0.4553$	$\beta_1^2 = 0.1376$	$\beta_1^3 = 0.0407$	$\beta_1^4 = 0.3664$	$\beta_1^G = 0$

Table 10: The belief degrees of security situation T.

	G_1 (excellent)	G_2 (good)	G_3 (general)	G_4 (bad)	G
T	$\beta^1 = 0.2715$	$\beta^2 = 0.2551$	$\beta^3 = 0.2469$	$\beta^4 = 0.2264$	$\beta^G = 0$

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

[1] X. Chen, J. Li, B. Guo et al., "All-optical OXC transition strategy from WDM optical network to elastic optical network," *Optics Express*, vol. 24, no. 4, pp. 4076–4087, 2016.

[2] S. Viciani, M. Lima, M. Bellini, and F. Caruso, "Observation of noise-assisted transport in an all-optical cavity-based network," *Physical Review Letters*, vol. 115, no. 8, Article ID 083601, pp. 1–5, 2015.

[3] S. Koohi and S. Hessabi, "All-optical wavelength-routed architecture for a power-efficient network on chip," *IEEE Transactions on Computers*, vol. 63, no. 3, pp. 777–792, 2014.

[4] Z. Qu, X. Zhang, S. Shi, Y. Cao, and M. Zhao, "Network coding based all-optical multicast in WDM networks," *Journal of China Universities of Posts & Telecommunications*, vol. 22, no. 1, pp. 89–94, 2015.

[5] T. Bass, "Intrusion detection system and multi-sensor data fusion: creating cyberspace situation awareness," *Communications of the ACM*, vol. 43, no. 4, pp. 99–105, 2000.

[6] G. Y. Hu, Z. J. Zhou, B. C. Zhang, X. Yin, Z. Gao, and Z. Zhou, "A method for predicting the network security situation based on hidden BRB model and revised CMA-ES algorithm," *Applied Soft Computing*, vol. 48, pp. 404–418, 2016.

[7] G. Y. Hu and P. L. Qiao, "Cloud belief rule base model for network security situation prediction," *IEEE Communications Letters*, vol. 20, no. 5, pp. 914–917, 2016.

[8] X.-Z. Chen, Q.-H. Zheng, X.-H. Guan, and C.-G. Lin, "Quantitative hierarchical threat evaluation model for network security," *Journal of Software*, vol. 17, no. 4, pp. 885–897, 2006.

[9] Z. Yong, X. Tan, and H. Xi, "A novel approach to network security situation awareness based on multi-perspective analysis," in *Proceedings of the International Conference on Computational Intelligence and Security (CIS '07)*, pp. 768–772, Harbin, China, December 2007.

[10] M. Liu, Q. Zhang, H. Zhao et al., "Network security situation assessment based on data fusion," in *Proceedings of the 1st International Workshop on IEEE Knowledge Discovery and Data Mining (WKDD '08)*, pp. 542–545, Adelaide, Australia, March 2008.

[11] J.-B. Yang and D.-L. Xu, "On the evidential reasoning algorithm for multiple attribute decision analysis under uncertainty," *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans*, vol. 32, no. 3, pp. 289–304, 2002.

[12] J.-B. Yang and D.-L. Xu, "Evidential reasoning rule for evidence combination," *Artificial Intelligence*, vol. 205, no. 12, pp. 1–29, 2013.

[13] H. Zuo and L. Ma, "Battlefield damage level assessment for submarine torpedo weapon system based on evidential reasoning algorithm," *Torpedo Technology*, vol. 16, no. 1, pp. 48–51, 2008.

[14] Z.-G. Zhou, F. Liu, L.-C. Jiao et al., "A bi-level belief rule based decision support system for diagnosis of lymph node metastasis in gastric cancer," *Knowledge-Based Systems*, vol. 54, pp. 128–136, 2013.

[15] Z.-J. Zhou, C.-H. Hu, B.-C. Zhang, D.-L. Xu, and Y.-W. Chen, "Hidden behavior prediction of complex systems based on hybrid information," *IEEE Transactions on Cybernetics*, vol. 43, no. 2, pp. 402–411, 2013.

[16] N. H. Pang, *Data Processing of Tunnel Monitoring System Based on ER Algorithm*, Huazhong University of Science & Technology, Wuhan, China, 2012.

[17] R. Rejeb, M. S. Leeson, C. M. Machuca, and I. Tomkos, "Control and management issues in all-optical networks," *Journal of Networks*, vol. 5, no. 2, pp. 132–139, 2010.

[18] M. Furdek, N. Skorin-Kapov, S. Zsigmond, and L. Wosinska, "Vulnerabilities and security issues in optical networks," in *Proceedings of the 16th International Conference on Transparent Optical Networks (ICTON '14)*, pp. 1–4, IEEE, Graz, Austria, July 2014.

[19] B. Everett, "Tapping into fibre optic cables," *Network Security*, vol. 2007, no. 5, pp. 13–16, 2007.

[20] C. Mas, I. Tomkos, and O. K. Tonguz, "Failure location algorithm for transparent optical networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 8, pp. 1508–1519, 2005.

[21] Y. Peng, Z. Sun, S. Du, and K. Long, "Propagation of all-optical crosstalk attack in transparent optical networks," *Optical Engineering*, vol. 50, no. 8, Article ID 085002, pp. 1–3, 2011.

[22] R. Aparicio-Pardo, P. Pavon-Marino, and S. Zsigmond, "Mixed line rate virtual topology design considering non-linear interferences between amplitude and phase modulated channels," *Photonic Network Communications*, vol. 22, no. 3, pp. 230–239, 2011.