Business-based analysis of electric power communication network vulnerability in multiple scenarios

Ran Wang, Xuelian Gao

School of Electrical and Electronic Engineering, North China Electric Power University, Beijing 102206, China;

w1091230118@163.com

Keywords: Power communication network, Fuzzy analytic hierarchy process, Reliability, Vulnerability, Business risk value.

Abstract. In order to research the reliability of electric power communication network, this paper proposes a kind of vulnerability analysis method based on business. Firstly, it applies the improved fuzzy analytic hierarchy process to evaluate electric power business importance. Secondly, the business importance is taken as a network parameter to establish two models: the network topology model based on business, and the deliberately attack model based on edge betweenness. Finally, it simulates and analyzes the loss of business importance in two scenarios when a certain area network topology is attacked. Furthermore, the sensitive path is searched for strategy optimization, therefore the vulnerability of network decreases when it is deliberately attacked, which could improve the reliability of network.

1. Introduction

Electric power communication network is the private communication network. Its reliability will directly affect the safe and stable operation of the power grid. The network can be analyzed from invulnerability [1], robustness [2] and vulnerability [3]et al. Currently, there are some researches on the reliability of electric power communication network. Ref. [4] introduces the series system model to assess the vulnerability of wide-area measurement system (wams); Ref. [5] evaluates each index of the communication network with fuzzy analytic hierarchy process (FAHP). However, most existing literatures are based on the physical topology and logical structure, and rarely consider the effect of failure network to the business. Based on the improved FAHP, this paper firstly assesses the business importance. Secondly, it establishes a network model based on business importance and an attack model based on edge betweenness (EB). Thirdly, it brings the concept of polymorphic networks to simulate the attack on the network in multiple scenarios. Thus, it can reduce the vulnerability of network, and improve the reliability. Finally, numerical simulation verifies the effectivity of the analysis method.

2. Business Importance

There are some methods to calculate the business importance, such as analytic hierarchy process (AHP)[6], objective index evaluation method[7]. But the evaluation of traditional AHP is based on the expert assessment principle, which has a strong subjectivity. This paper uses the consistency-based FAHP as an evaluation method, which reduces the influence of subjective factor on the evaluation results in a certain degree. The result is shown in Table 1:

Table 1 Business importance

Service[1]	RP	SS	AU	EM	PI	DT	LL
Result	1.0000	0.8880	0.8880	0.5098	0.1000	0.5447	0.1883

[1] RP: Relay Protection ,SS: Safe System ,AU: Automation, EM: Energy Metering, PI: Protection of Information ,DT: Dispatching telephone, LL: Lightning Location

Table 1 indicates that the importance of relay protection business is the highest, and the second one is the safe system. Compared to protection information management system, lightning location system needs more real-time capability. Thus, the result conforms to the actual requirement.

3 Network Relationship

3.1 The network business model

$G = (V, E, S)$ is defined as the network topology, V represents the sets of vertices, E indicates the undirected-link sets, and S is the business sets. W stands for the distribution of business importance's node pairs between source and destination (s-d) in network. In order to improve the real-time transfer efficiency, it defaults all the business channels are the shortest paths between s-d node pairs. The s-d node pair sets and business sets are represented by the matrix $D_{w\times s}$. Where the row vector corresponding to the s-d node pairs in the network is (s,d), and the column vector corresponding to the network business is S_i. When the m node pairs of (s,d) run the business of S_n, $d_{mn}=1$. It can be set as:

$$W(s,d) = \sum_{n=1}^{N} SI_n \cdot d_{mn} \qquad n = 1,2,\ldots,N \tag{1}$$

Equation (1) shows the sum of all business importance m node pairs between (s-d), and SI_n indicates the business importance of business S_n.

3.2 The link weight and failure probability

It has a certain practical significance for Ref. [14] to bring EB into the calculation of the link weight. However, network is the carrier of business, and the business link of actual operation is more important than the business link of idle one. Hence, it would be more realistic to analyze the link weight from the view of business. It can be calculated as:

$$EW = \sum_{i=1}^{I} SI_i \cdot n_i \qquad i = 1,2,\ldots,I \tag{2}$$

EW of Equation (2) shows the sum of all business importance which passes link E, and n_i is the number of business S_i. The weight of link E_m can be expressed as:

$$\omega_m = \frac{EW_m}{\sum_{m=1}^{M} EW_m} \qquad m=1,2,\ldots,M \tag{3}$$

Power communication network commonly uses optical cable as transfer carrier. Therefore, outage probability of optical cable is closely related to its length, type, running time, and environmental factors. In this paper, it selects the length and running time as the decisive factors. Where the outage probability of attacked link can be defined as:

$$P_i = \frac{l_i}{\max(l_1, l_2, \ldots, l_i)} \cdot \rho \cdot T_i \tag{4}$$

In Equation (4), $0 < \rho < 1$, where ρ is the intensity of attack. T_i represents the influence of time factor on the link. It can be counted by:

$$T_i = \begin{cases} 1 & t \in [0,5] \\ e^{\frac{5-t}{T}} & t \in [5,\infty) \end{cases} \tag{5}$$

In Equation (5), t indicates the running time of link, and T is the service life of optical cable.

3.3 The risk value of network business

The paper uses the influence value of business importance as the influence value of risk. The risk value of link E_i can be set as:

$$R_i = EW_i \cdot P_i \tag{6}$$

The risk value of network business:

$$R = \sum_{i=1}^{I} R_i \cdot \omega_i \tag{7}$$

3.4 Attack Model

Network topology consists of nodes and links. Most of nodes distribute in the substation with the specialist protection, Thus, it can assume the failure probability of nodes is 0, that means this paper only considers the influence of the deliberately attack on power communication network. According to the confidentiality of grid system, the attacker controls plenty of the physical layer topology information, and it will attack network base on the physical layer. This paper establishes an attack model based on EB, and it analyzes the losses of network business by deliberately attack. Where E_x is the maximum number of x EB link sets, and $x \in \{1,2,3...N\}$. At the time of $x \geq 1$, the links are attacked by the strength of ρ. It supposes the links are dependent on each other, and the loss degree of business can be defined as:

$$S_{\text{loss}} = \frac{\sum [1 - \prod_{1}^{x} (1 - P_i)] \cdot W(s,d)}{\sum_{s,d \in V} W(s,d)} \tag{8}$$

4. Network Analysis

The configuration of Network Simulation is as follows. The network topology is an instance of power communication network topology structure in an area. Furthermore, it consists of 10 nodes and 15 links. The number above the link is the actual distance between two nodes. Where No. 1 is the province dispatch center, No. 3 is the backup dispatch center, and the rest nodes are respectively 500kV or 220kV substations.

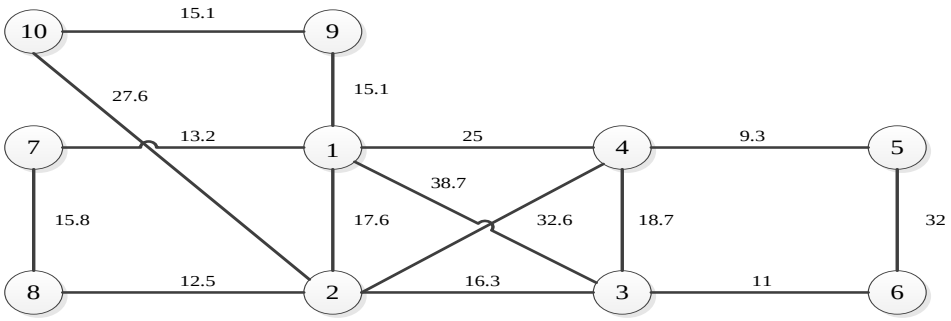

Fig. 1 Network topology

According to the definition of EB in Fig. 1, it can obtain the order of EB which is shown in Table 2.

Table 2 EB results

Edge	E(1,7)	E(3,6)	E(1,4)	E(4,5)	E(3,4)	E(2,8)	E(1,3)	E(2,3)
Order	1	2	2	3	4	4	4	5
Edge	E(9,10)	E(7,8)	E(1,9)	E(2,10)	E(2,4)	E(1,2)	E(5,6)	
Order	5	6	7	7	7	8	9	

On the basis of the network business model, it can create the business distribution matrix which is shown in Table 3.

Table 3 Business distribution list

W(s,d)	S1	S2	S3	S4	S5	S6	S7	W(s,d)	S1	S2	S3	S4	S5	S6	S7
W(1,2)	1	1	1	0	0	1	1	W(2,4)	0	0	1	0	0	1	0
W(1,3)	1	1	1	0	1	1	1	W(2,10)	0	0	1	0	0	1	0
W(1,4)	1	1	1	1	0	1	1	W(3,4)	1	1	1	1	1	1	0
W(1,5)	1	1	1	1	1	1	1	W(3,6)	1	1	1	1	1	1	0
W(1,6)	1	1	1	0	0	1	1	W(3,9)	1	1	1	0	0	1	0
W(1,7)	1	1	1	0	0	1	1	W(4,5)	0	0	0	0	1	1	0
W(1,8)	1	1	1	0	0	1	1	W(4,7)	0	0	0	1	1	1	0
W(1,9)	1	1	1	0	1	1	1	W(5,6)	0	0	0	0	0	1	0
W(1,10)	1	1	1	0	1	1	1	W(7,8)	0	0	0	0	0	1	0
W(2,3)	1	0	0	0	0	1	0	W(9,10)	0	0	0	0	0	1	0

According to table 3 and equation (1), the summation of network business importance ($W(s,d)$) is equal to 50.3009. The following assumptions are made to simplify the calculation:

(1) The malfunction probability of network links is 0 under the natural condition.

(2) The length of all links is equal, and the usage time of optical cable is less than 5 years.

$P_i = \rho$ can be obtained from assumption (2) and formula (4) and (5).Thus, the deliberated attack to this attack model can be simulated with two scenarios.

1) Scenario 1

It supposes the attack links are the first x edges of the maximum EB. In addition, it makes $x = 6$, and sets the strength of attack - ρ. During attacking, it remains the attack links invariant, and the attack strength (ρ) keeps increasing from 0 to 1.The loss of business is measured by equation (8) which can be seen in Fig. 2.The business loss degree continues increasing with the accretion of attack strength when the number of attack links is invariant. At the point of $\rho = 1$, the business loss degree has been 74.81%, which means the network is basically in a state of paralysis.

2) Scenario 2

It assumes the attack strength (ρ) is equal to 1.The attack links are the first x edges of the maximum EB. During the process of attack, the attack strength is invariable, and the attack edges are increased. According to equation (8), the business loss degree can be shown in Fig. 3.The business loss degree increases greatly when the network is attacked. When $x = 6$, the business loss degree reaches 74.81%. The network is nearly paralytic. Because the small EB link carries the lower business importance, the business loss becomes flat in the subsequent attack.

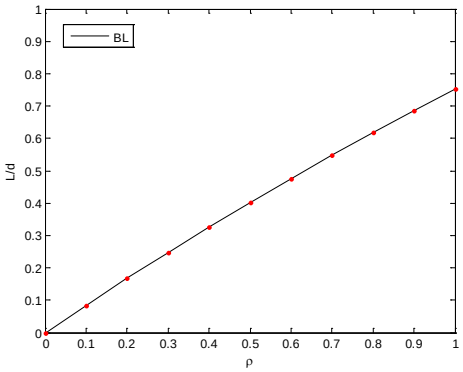

Fig. 2 Increase attack strength

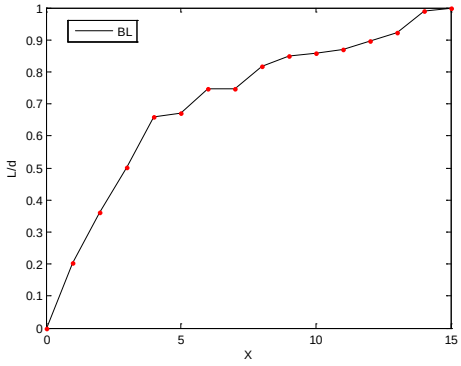

Fig. 3 Increase the number of attacking links

5. Strategy Optimization

According to the above analysis, due to the higher fitting degree of business distribution and EB-based network topology path, the vulnerability of network is higher. The attack edges (x) and the attack strength (ρ) are the important factors that affect the business loss degree. Since the attack strength can not be controlled and the topology structure of physical layer is so difficult to

change, it can reduce the business loss degree in the deliberate attack by optimizing business strategies.

Optimization strategy uses reducing the value of network business risk as a benchmark. The relatively sensitive path is $E(1,9)$ by the comprehensive analysis of big data. Therefore, it can be improved as follow. The business path of initial s-d node pairs ($W(1,10)$) is $1-9-10$, and the optimized path is $1-2-10$. Similarly, the business path of initial s-d node pairs ($W(3,9)$) is $1-2-10$, and the optimized path is $3-2-10-9$. When we keep $\rho=1$, the value of network business risk changes from 7.0601 to 6.1036 by equation (7) with optimization strategy. The curve of business loss degree is shown in Fig. 4.

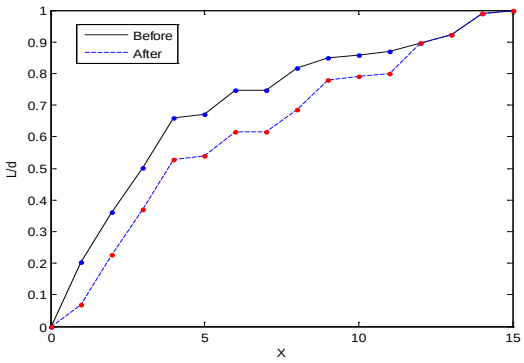

Fig. 4. Comparison before and after optimization strategy.

When the first three links are attacked, the business loss is 18.605, which accounts for 37.21% of the total business importance. Hence, it has been optimized to a certain extent. When $x=6$, the business loss degree is 61.53%. The loss degree of business importance has a significantly abasement after optimization. The vulnerability of network recedes, and the reliability greatly increase.

6. Summary

It improves the traditional evaluation method of business and simplify the calculation. Moreover, it establishes the attack model and proposes to use the business importance of links as a weight factor for the assessment of network business risk value. Additionally, it simulates the business loss state of network by varying the attack sides and strength in multiple scenarios, and synthesizes data to analyze the vulnerability of network. Based on the principles of reducing the network business risk value, it optimizes the network business, which makes the business distribution more balanced, the vulnerability more lower, and the reliability more incremental. Finally, it concludes that this method shows the effectiveness and versatility, and the reliability analysis of power communication network has a practical significance.

Reference

[1].Bing Fan, Liangrui Tang. Electric power communication network vulnerability analysis [J]. Proceedings of the csee, 2014, 07: 1191-1197.

[2].Wei Wang, Hao Yu. A kind of electric power fiber optic communication network Anti-destroying ability evaluation algorithm [J]. Electric power science and engineering, 2014, 03: 64-67.

[3].Yanqing Li, huaqiang Li, Qian Li, et al. Based on the comprehensive vulnerability branch grid anti-destroying ability analysis [J]. Power system protection and control, 2014, 07: 80-85.

[4]. Bing Fan Ying Zeng, Liangrui Tang, et al. Vulnerability assessment of power communication network based on information entropy [J]. Journal of electronics and information technology, 2014, 09: 2138-2144.

[5]. Liming Wang, Hong Bing. Structure and robustness of multiple network [J]. Journal of complex

systems and complexity science, 2015, 02: 32-37+59.

[6].Jing Peng, Lu Jiping, Yang Wang, et al. Risk assessment of backbone communication network in WAMS [J]. Proceedings of the csee, 2010, 84: 84-90.

[7].Ziyan Zhao, Jianming Liu. A new service risk balancing based method to evaluate reliability of electric power communication network [J]. Power grid technology, 2011, 10, 209-213.