Comprehensive Vulnerability Assessment and Optimization Method for Smart Grid Communication Transmission Systems

Chenchen Ji,Peng Yu,Wenjing Li,Puyuan Zhao,Xuesong Qiu
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing, China

***Abstract*—Vulnerability assessment and optimization for wide area monitoring, protection and control system (WAMPAC) can enhance the robustness and sustainability of network. However, current assessment methods are incomplete and optimization methods ignore dynamic process. A comprehensive vulnerability assessment and optimization method is proposed. Firstly, for assessment, a comprehensive vulnerability indicator is designed to assess vulnerability of nodes and edges in the network integrating static and dynamic aspects. And then, to relieve unbalanced vulnerability distribution in the network, a routing optimization method is proposed by reconfiguring service routes on the edge with high vulnerability. Finally, the simulation is taken under a real system. Vulnerability assessment with the defined indicator is executed, and its correctness is proved as well. Then with the optimization method, the network vulnerability can be balanced, which takes on effective theoretical and practical significance.**

Keywords—smart grid; WAMPAC; comprehensive vulnerability; vulnerability balance

I. INTRODUCTION

Currently, power grid operation are more complex. Requirements of stable running and reliable power supply become higher [1]. By utilizing WAMPAC system, smart grid communication transmission systems can make real-time judgment and implement protection control measures based on the advanced measurements, communications, and online analysis techniques, which has better effect to maintain stability and integrity of power system [2].

In WAMPAC system, vulnerability of the system is denoted by nodes and edges vulnerability generally. It can be defined as the decreased degree of the network performance after the removal of the nodes or edges [5]. According to the results of the system vulnerability analysis, we can identify the weakness in the network, which provides the basis for the system management and optimization.

Vulnerability assessment of communication network is mainly based on complex network theory so far, and further, there are three methods. The first is the structural vulnerability assessment method based on classical complex network theory. Literature [6] use some parameters related to complex network to analyze the network. Although the method breaks limitation of the network scale, it can only reveal the structural vulnerability of the network topology. The second approach combines complex network theory with traditional reliability calculation. Literature [8] combines physical vulnerability based on reliability calculation with structural vulnerability, but still ignores the important differences of services and the nodes. The third assessment method considers the service influence and complex network theory. Service importance is taken as an important basis for evaluating the vulnerability in [10], but it does not consider the importance of nodes and edges. In addition to above problems, above researches for vulnerability assessments are short of the consideration of availability and other dynamic indicators. Two countermeasures, named High Degree nodes Protection (HDP) strategy and Low Degree nodes link Addition (LDA) strategy, are proposed to improve structural vulnerability of power communication network [12]. But both of them need to upgrade the existing network structure, which will bring additional manpower and investment.

Based on the above analysis, this paper puts forward a comprehensive vulnerability assessment and optimization method of smart grid transmission system, WAMPAC. In the assessment, the influence factors of vulnerability are analyzed from two aspects: static factors and dynamic factors. Further, to resolve the unbalanced vulnerability problem, a routing optimization method based on vulnerability balance is proposed. It reconfigures the routes of key services on the high vulnerable edges to achieve vulnerability equilibrium of the whole network.

II. VULNERABILITY ASSESSMENT MODEL

A. Network Topology and Service Model

Firstly, we model the network topology of WAMPAC systems as a weighted and undirected network. The weight of the edge is determined by the transmission delay on the link. Network can be expressed to a weighted and undirected network $G=(V, E)$ containing N nodes and M edges. V and E represent the set of nodes and links. $A=\{a_{ij}\} \subset R^{N\times N}$ is adjacency matrix of network. The service modeling is defined as a set $S=\{s_k\}$.

B. Static Vulnerability Factors

The static vulnerability of the nodes and edges is determined by the network topology and the service.

1) Network Topology Vulnerability

The betweenness $B(v_i)$ of node v_i is defined as the proportion of the number of shortest paths through v_i relative to the number

of the all shortest paths in the network. It is more accurate and reasonable that node uses the betweenness as an importance indicator to reflect its topological vulnerability. Edge uses the $B(e_{ij})$ to reflect its topological vulnerability as well.

2) Service Vulnerability

The influence of the service should be considered when analyzing the vulnerability. The service vulnerability can be evaluated through service categories and numbers on different nodes and edges. Here Node Pressure (*NP*) and Edge Pressure (*EP*) are used to represent the service vulnerability of the node and edge. Here we use $EP(e_{ij})$ and $NP(v_i)$ to denote the pressure indicator as below.

$$NP(v_i) = \sum_{k=1}^{Q} n_k(v_i) \times C_k \tag{1}$$

$$EP(e_{ij}) = \sum_{k=1}^{Q} n_k(e_{ij}) \times C_k \tag{2}$$

Here k is the service category which is from 1 to Q. n_k is the number of services whose type is k. C_k is the service importance for service category k.

3) Static Vulnerability Factors

The Node Static Vulnerability (*NSV*) and Edge Static Vulnerability (*ESV*) are composed of the network topology vulnerability and the service vulnerability, which is determined by the betweenness and pressure. The expression is as follows:

$$NSV(v_i) = B(v_i) \times NP(v_i) \tag{3}$$

$$ESV(e_{ij}) = B(e_{ij}) \times EP(e_{ij}) \tag{4}$$

C. Dynamic Vulnerability Factors

As malfunction of the transmission equipment and the link loading service is random, reliability of the transmission equipment and the links in the network is a time varying parameter. The higher the reliability is, the smaller the vulnerability is. Hence, the dynamic vulnerability of nodes and edges can be expressed by the reciprocal of reliability of the transmission equipment and the link.

1) Importance and Availability

The reliability of transmission equipment is determined by Equipment Importance (*EI*) and the Actual Equipment Availability (*AEA*). The reliability of the link is composed of the Link Importance (*LI*) and the Actual Link Availability (*ALA*).

Let $AEA_{v_i}(t)$ and $ALA_{e_{ij}}(t)$ be the actual availability of the node v_i and edge e_{ij} at time point t. Their values are shown below.

$$AEA_{v_i}(t) = \frac{\sum_{r=0}^{\infty} TA_{v_i}(r;t)}{\sum_{r=0}^{\infty} [TA_{v_i}(r;t) + TB_{v_i}(r;t)]} \tag{5}$$

$$ALA_{e_{ij}}(t) = \frac{\sum_{r=0}^{\infty} TA_{e_{ij}}(r;t)}{\sum_{r=0}^{\infty} [TA_{e_{ij}}(r;t) + TB_{e_{ij}}(r;t)]} \tag{6}$$

Here $AEA_{v_i}(t)$, $TA_{v_i}(r;t)$ and $TB_{v_i}(r;t)$ are the actual availability of v_i at time point t, the r-th trouble-free time, and the r-th fault repair time respectively. And $ALA_{e_{ij}}(t)$, $TA_{e_{ij}}(r;t)$ and $TB_{e_{ij}}(r;t)$ are the actual availability of e_{ij} at time point t, the r-th trouble-free time and the r-th fault repair time respectively.

2) Dynamic Vulnerability factors

Node Dynamic Vulnerability (*NDV*) and Edge Dynamic Vulnerability (*EDV*) are as follows. $NR(t)$ and $EP(t)$ are the reliability of nodes and edges.

$$NDV_{v_i}(t) = \frac{1}{NR_{v_i}(t)} = \frac{1}{EI(v_i) \times AEA_{v_i}(t)} \tag{7}$$

$$EDV_{e_{ij}}(t) = \frac{1}{ER_{e_{ij}}(t)} = \frac{1}{LI(e_{ij}) \times ALA_{e_{ij}}(t)} \tag{8}$$

D. Comprehensive Vulnerability Indicator

Here, Node Comprehensive Vulnerability (*NCV*) and Edge Comprehensive Vulnerability (*ECV*) are defined as vulnerability indicator which combine dynamic factors and static factors as below.

$$NCV_{v_i}(t) = NSV(v_i) \times NDV_{v_i}(t) = \frac{B(v_i) \times NP(v_i)}{EI(v_i) \times AEA_{v_i}(t)} \tag{9}$$

$$ECV_{e_{ij}}(t) = ESV(e_{ij}) \times EDV_{e_{ij}}(t) = \frac{B(e_{ij}) \times EP(e_{ij})}{LI(e_{ij}) \times ALA_{e_{ij}}(t)} \tag{10}$$

When the vulnerability distribution of the network is not balanced, network performance will decline fast by attacking those nodes or edges whose vulnerability is larger. Here Vulnerability Balance Degree (*VBD*) is defined as an indicator of overall network vulnerability using the sum of the standard deviation of *NCV* and *ECV* expressed as follows:

$$VBD = \sqrt{\frac{1}{N} \sum_{v_i \in V} (NCV_{v_i} - \overline{NCV})^2} + \sqrt{\frac{1}{M} \sum_{e_{ij} \in E} (ECV_{e_{ij}} - \overline{ECV})^2} \tag{11}$$

E. Vulnerability Assessment Method

1) Improved Network Performance Function

Efficiency function $E(G)$ in complex network is always used to evaluate the efficiency of the network in physical topology. We use the sum of service importance as an indicator of network performance. Finally, Comprehensive Network Performance (*CNP*) is obtained combining the physical topology and service as below and here ε_{ij} represents the communication efficiency between two nodes, which is inversely proportional to the shortest distance between two nodes.

$$CNP(G) = E(G) \times (\sum_{k=1}^{Q} n_k \times C_k) = [\frac{1}{n(n-1)} \sum_{i,j \in G, i \neq j} \frac{1}{d_{ij}}] \times (\sum_{k=1}^{Q} n_k \times C_k) \tag{12}$$

2) Attack Model

The attack model used here is divided into random attack and deliberate attack. The attack process is to select nodes and edges to be removed sequentially, and then calculate the decline of *CNP*. Random attack can be used to simulate the random failures in the network, and it is random to select nodes and

edges to remove. The deliberate attack is to select the node and the edge which has some features to attack preferentially. In this paper, we use three kinds of deliberate attack models to compare the difference of network performance decline: high betweenness attack, high pressure attack and high vulnerability attack.

III. ROUTE OPTIMIZATION METHOD BASED ON VULNERABILITY BALANCE

Algorithm detailed steps are as follows.

Step 1: **Definition**: Establish a vulnerability weight matrix W= $\{w_{ij}\}$ and a vulnerability balance degree array ***VB***, here $w_{ij}=ECV(e_{ij})+NCV(v_j)$ and ***VB***= $\{VBD_x\}$, which is used to store the changes of *VBD* after each route optimization. The VBD_1 is the initial *VBD*;

Step 2: **Select edge**: Select the most vulnerable edge e_{ab} again. Let $w_{ab}=w_{ba}=inf$, which means that e_{ab} is deleted from the network topology for the new route adjustment; note that the most vulnerable edge may change after a service route optimization and updating the network vulnerability.

Step 3: **Select service**: Store services, whose route is through the edge e_{ab} into a set of service $S=\{s_y\}$. Extract s_1 from the set S and extract the start and the end of s_1;

Step 4: **Rerouting**: Complete the re-routing of the service s_1 with the optimization goal of the minimum cumulative vulnerability. Reroute according to vulnerability weight matrix W using Floyd algorithm to get the new route R^* of s_1;

Step 5: **Update**: Calculate the vulnerability of the nodes and edges in the network, NCV^* and ECV^*;

Step 6: **Calculate:** Calculate standard deviation of NCV^* and ECV^*, and vulnerability balance degree VBD_x;

Step 7: **Compare**: If VBD_x decrease, the *VBD* is down and this service route optimization is successful. Repeat step 1 to step 6, change vulnerability weight matrix W. Select the most vulnerable edge and complete a rerouting of a service on this edge. If $VBD_x > VBD_{x-1}$, it shows that the optimization of the service routing fails, the optimal path is not accepted, and the algorithm is terminated.

IV. SIMULATION RESULT

Taking part of a real transmission system from a power grid in China called network A as the simulation scenario shown in Fig.1 as follows. There are 17 nodes and 25 edges in A.

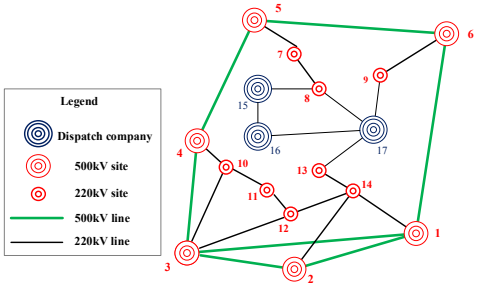

Fig. 1. Topology of Network A

The service set S includes 20 services got from the real network, whose service importance consult the paper.

A. Simulation of Vulnerrability Assessment of Nodes and Edges

Taking the node 8 as example, the comprehensive vulnerability of node 8 is shown below in Fig. 2.

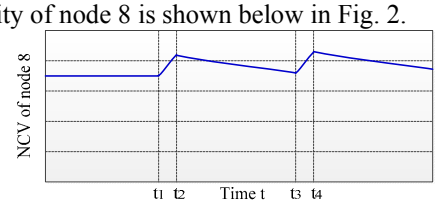

Fig. 2. *NCV* of node 8

The time 0-t_1, t_2-t_3 and after t_4 are fault-free time and the time t_1-t_2, t_3-t_4 are fault time. t_1 and t_3 is the time point of fault occur. t_2 and t_4 is the time point of fault repair. When the fault occurs at t_1 and t_3, the vulnerability increases and when the fault repair, the vulnerability is down slowly, but it is still higher than the value of the vulnerability before the fault.

The network is attacked by four attack modes shown in Fig.3 and Fig.4. From figures, we can see the decline of *CNP* under the deliberate attack is faster than the random attack. In the three deliberate attacks, the high vulnerability attack has the greatest impact on the network performance, and the rationality of the definition of the vulnerability indicator is verified.

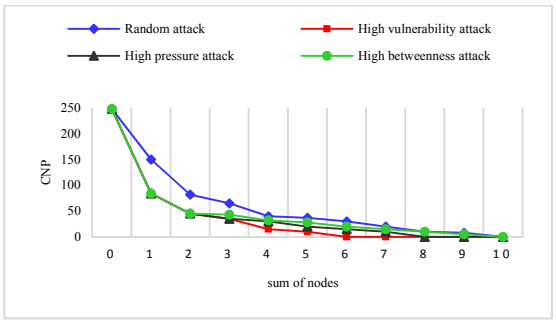

Fig. 3. Comparison of *CNP* descent curves under four attack modes to nodes

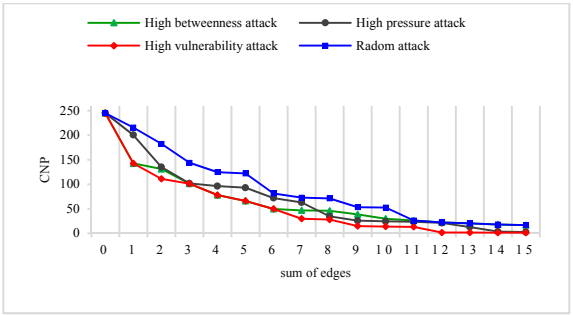

Fig. 4. Comparison of *CNP* descent curves under four attack modes to edges

B. Simulation of routing optimization method based on vulnerability balance

The edge between node 13 and 14 has the biggest *ECV*. Therefore, the route of the service on this edge is optimized first. Algorithm simulation process is shown in the table I.

From the table, *VBD* is decreased by 70.41%, the standard deviation of the node and edge vulnerability is decreased by 35.48% and 81.6% from the first optimization to the 10th optimization process. That is to say, with the optimization of the service path, the network tends to be balanced.

TABLE I. PROCESS OF TOUTING OPTIMIZATION METHOD

Time	Edge before	service	Initial route	New route	VBD_i	Edge after
1	$e_{13\text{-}14}$	S_6	2-14-13-17-8-15	2-3-4-5-7-8-15	11.4111	$e_{13\text{-}14}$
2	$e_{13\text{-}14}$	S_7	3-12-14-13	3-1-6-9-17-13	11.3911	$e_{13\text{-}14}$
3	$e_{13\text{-}14}$	S_8	3-12-14-13-17-9	3-2-1-6-9	10.2823	$e_{13\text{-}17}$
4	$e_{13\text{-}17}$	S_9	3-12-14-13-17-16	3-4-5-7-8-15-16	9.1985	$e_{13\text{-}17}$
5	$e_{13\text{-}17}$	S_{10}	10-11-12-14-13-17	4-5-7-8-17	9.0429	$e_{13\text{-}17}$
6	$e_{13\text{-}17}$	S_{14}	5-7-8-17-13-14-12	5-4-3-12	8.3685	$e_{13\text{-}17}$
7	$e_{13\text{-}17}$	S_{15}	5-7-8-17-13-14-2	5-6-1-2	8.1826	$e_{12\text{-}14}$
8	$e_{12\text{-}14}$	S_{11}	4-10-11-12-14	4-3-2-14	8.1537	$e_{13\text{-}17}$
9	$e_{13\text{-}17}$	S_{18}	6-9-17-13-14-12-11	6-1-3-10-11	6.9638	$e_{13\text{-}17}$
10	$e_{13\text{-}17}$	S_{19}	15-18-17-13-14	15-8-7-5-6-1-14	6.8603	$e_{7\text{-}8}$
11	$e_{7\text{-}8}$	S_6	2-3-4-5-7-8-15	2-14-13-17-16-15	8.0737	$e_{13\text{-}17}$

In the process of optimization, not only *VBD* becomes small, but also the maximum value of *ECV* continues to decrease and begins to rise after the eleventh optimization. It is shown in Fig.5. The edge with biggest vulnerability is not always single and it is the reason why have to update *NCV* and *ECV* after a service route optimization.

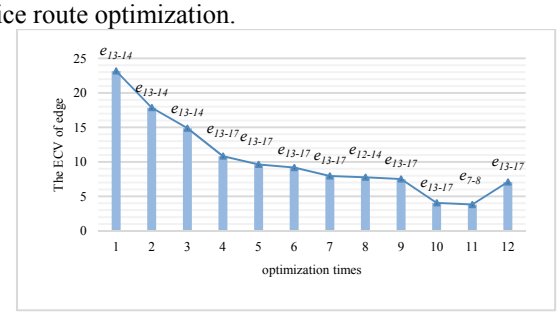

Fig. 5. The change of max(*ECV*)

In order to get the robustness of network after optimization, the network is attacked by random node attack, and compared with the former. The attack selects 10 nodes randomly, and the change curve of *CNP* after the attack is shown in Fig.6.

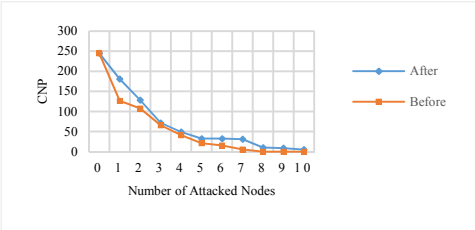

Fig. 6. The change of *CNP* descent curves under random node attack

According to the simulation results, after the first random node attack, the network completed the optimization, *CNP* decreased by 26.20%, while the *CNP* before optimization decreased by 48.38%, and the performance was improved by 43% after optimization. The robustness of network is improved after optimization.

V. CONCLUSION

The effect factors of vulnerability in the WAMPAC system are summarized in this paper. According to the static and dynamic factors, the vulnerability assessment method is established, and the rationality of the assessment system is verified by different attack models. Aiming at uneven distribution of vulnerability, a dynamic service routing optimization method based on vulnerability balance is proposed. In the future there are still a few points need to studied. For vulnerability assessment, we will continue to improve the evaluation indicators, and promote it to power distribution and utilization networks. Still, to get a most balanced network fast when faults come, we will research overall optimization methods for unbalanced distribution of vulnerability through some intelligent optimization algorithms.

ACKNOWLEDGEMENT

The authors would like to thank the reviewers for their detailed reviews and constructive comments. This work was supported by Research on Communication Architecture and Hardware-In-The-Loop Simulation for Real-Time Wide Area Stability Control of Electric Power System (SGGSXT00GCJS1600065) and Wide Area Security and Stability Control and 863 Program (2015AA01A705).

REFERENCES

[1] Kounev V, Lévesque M, Tipper D, "Reliable Communication Networks for Smart Grid Transmission Systems," Journal of Network and Systems Management, 2016, 24(3):629-652.

[2] Yu Quan, Huangsheng Hua, "Research and practice of multi-level wide area protection and control system architecture," Power System Protection and Control,2015,43(5):112-122

[3] Xiaona Ren, "Research on Power Grid Vulnerability Assessment Based on Complex Network Theory," Guangdong University of Technology, 2012.

[4] Min Ou-Yang, Qi Fei, Minghui Yu, Enjie Luan, "Survey on Efficiency and Vulnerability of Complex Network.," Computer Science, 2008, 06:1-4.

[5] Jing Guo, "The Vulnerability Analysis on Power Communication Networks Based on Complex Networks Theory," North China Electric Power University (HeBei), 2010.

[6] Bing Fan, Ying Zeng, Liangrui Tang, "Vulnerability Assessment of Power Communication Network Based on Information Entropy," Journal of Electronics and Information Technology, 2014, 09:2138-2144.

[7] Dichen Liu, Xingpei Ji, Bo Wang, Fei Tang, "Topological Vulnerability Analysis and Countermeasures of Electrical Communication Network Based on Complex Network Theory," Power System Technology, 2015, 12:3615-3621.