Risk Assessment and Optimization for Key Services in Smart Grid Communication Network

Puyuan Zhao, Xingyu Chen, Peng Yu, Wenjing Li, Xuesong Qiu, Shaoyong Guo

State Key Laboratory of Networking and Switching Technology

Beijing University of Posts and Telecommunications

Beijing 100876, China

***Abstract*—This paper proposes a risk assessment model of key service and optimization methods to reduce service risk in smart grid communication network. Firstly, we analyze the probability of failure of communication link and node which is induced by external factors, like natural disaster, human attack and system disturbances. Then using importance of services, links and nodes, we build the risk model of failure for key services. Further, we propose optimization methods based on Dijkstra algorithms to reduce the risk of key services. Finally, based on part of smart grid communication network topology structure from a Chinese province, the simulation results show that the risk of key services and whole network are reduced.**

Keywords—smart grid communication network; risk assessment; risk optimization; key services

I. INTRODUCTION

Electrical power grids are utilizing information and communication technologies (ICT) to develop smart grid which can enable active voltage control, improve power quality and capacity, and enhance ability to defense natural disaster, cyber-attack, and system interruption. Besides the power grid, Wide Area Monitoring, Protection, and Control (WAMPAC) system is also playing an increasingly critical role in smart grid communication network [1]. In WAMPAC, the Supervisory Control and Data Acquisition (SCADA) system is utilized to monitor and control the power grid. [2] There are some key services such as relay protection, dispatching automation transformed on the SCADA system, which provide information from local measurement and communicate through channels to protect the power grid safety. The SCADA system is inevitably affected by external factors, so that the key services will break up and control center cannot receive local messages and make a response to this failure. Then the SCADA system will lose the control of the power grid, which leads smart grid to face high risks. In our paper, we will discuss the reliability of service against to the external disturbance.

For the related work, there are some achieved results of risk analysis of service in communication network. A risk balance route allocation mechanism is proposed in [3], it focused to reduce of communication circuit and the overall risk of the network, but lacked the study of interruption caused by external factors. A method to evaluate the impact of communication system interruption on the WAMPAC based on the risk index is proposed in [4]. However, this paper lacked the consideration about the services carried on the communication links and nodes. Therefore, our paper will integrate service importance and the number of services to calculate the service risk caused by link interruption.

In our previous work[5], we have built the failure probability model about three external factors: nature factor, device factor and equipment factor. Depending to the risk theory, we calculate the risk of service based on importance of link, node, and service. For the service risk, we proposed optimization method to decrease service risk. However, our work can still be improved in many aspects. In this paper, we still concern about this risk of service, modify and enhance some work. The function of the relationship between equipment factor and failure probability is updated by 'bathtub curve', rather than basic exponential functions. For service risk, we utilize multiplication to build the model between service risk and element risk. And this results in an updated optimization methods based on our previous work.

II. SERVICE RISK ASSESSMENT OF POWER COMMUNICATION NETWORK

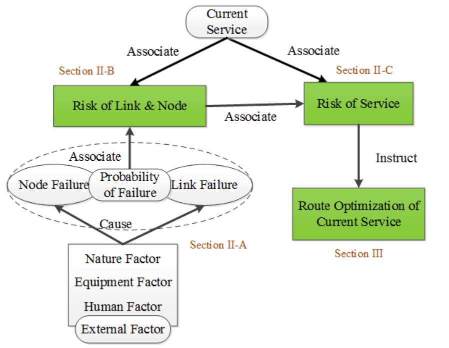

Fig.1 The relationship between each section

Service risk is one of the research objects of network risk management. The assessment of ICT network service risk aims to understand what is the current and future risk and assesses the impact of this risk. Thus, risk index can be used to develop risk control strategies. In Fig.1, it describes the relationships between each section. According to graph theory, we define $\boldsymbol{G}(\boldsymbol{V}, \boldsymbol{E})$ as the topology of the communication network, where $\boldsymbol{V}$ and $\boldsymbol{E}$ represent the set of nodes and communication links.

A. Correlation between External Factors and Equipment Failure

Firstly, we analyze the failure probability of link and node. The external factors which cause link interruption can be classified by nature factor, equipment factor and human factor.

1) For nature factor i:

We define $n_i(t)$ as the number of its occurrence during the time interval (0, t). All nature factors form a set $N = \{1, 2, \ldots, i\}$. Different levels of nature factors can have different damage and the difference between levels is almost increased by exponential. We set the level of nature factor at time t is l_i, then the probability of occurrence of nature factor i at time t can be:

$$p_i(t) = f(l_i, t)\frac{n_i(t)}{\sum_{i\in N} n_i(t)} \tag{1}$$

where, $f(l_i,t)$ is the impact of nature factor i with the level l_i.[5]

2) For equipment factor i:

Aging and defects of equipment and wires are gradually strengthening and increasing as time goes by. The changes always comply with the principle of 'bathtub curve' which comprises three parts presented on Fig.2.

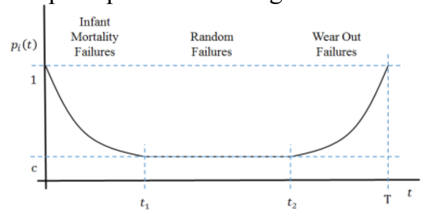

Fig.2 The classical bathtub curve

In different periods, the failure probability of equipment is not the same. The probability of occurrence $p_i(t)$ within time interval (0, t_1) and (t_2, T) can be defined as exponential functions, then the $p_i(t)$ within (0, t) is defined as:

$$p_i(t) = \begin{cases} e^{-\frac{t}{T_i}}, & 0 \le t < t_1 \\ c, & t_1 \le t \le t_2 \\ e^{\frac{t-T_i}{T_i}}, & t_2 < t \le T_i \end{cases} \tag{3}$$

where, T_i is a specification duration (e.g. working life), and c is a constant which can be obtained by $e^{-\frac{t_1}{T}}$ or $e^{\frac{t_2-T}{T}}$.

3) For human factor i:

Similarly, we define $n_i(t)$ as the number of times which it occurs in the time interval (0, t). Since human factor is always random, its process can be considered as the Poisson Distribution. Then $p_i(t)$, the probability of occurrence of human factor i, is defined as:

$$p_i(t) = 1 - e^{-\lambda_i n_i(t)} \tag{4}$$

where, λ_i is the average arrival rate of human factor i.

Suppose all kinds of factors are independent of each other. Also in the set of the same kind of factors, factors are mutually exclusive. We set $\boldsymbol{M}$ as the total number of external factors which cause link and equipment failure, n_f as the kind of factor. And all external factors form a set called $\boldsymbol{F} = \{1, 2, \ldots, \boldsymbol{F}_k\}$, where $\boldsymbol{F}_k$ represents different kinds of external factors.

For fault G_j (including link and node failures), according to historical data and experience analysis, define $\boldsymbol{F}_G$ as the set of external factors which may cause failures, and i as factor of the set. Suppose $P_j^{\mathrm{G}}(t)$ as the probability of occurrence of faults and $p_{kj}^{\mathrm{F}}(t)$ as the probability of occurrence of factors from $\boldsymbol{F}_G$ .Then the probability of occurrence of fault G_j can be defined as:

$$P_j^{\mathrm{G}}(t) = 1 - \prod_{F_k \in \boldsymbol{F_G}} (1 - p_{kj}^{\mathrm{F}}(t)) \tag{5}$$

B. Risk Index of Communication Link and Node Failure

From [5], we can obtain the risk index of link failure $R_{e_{ij}}$ and node failure R_{v_i} can be expressed as

$$R_{e_{ij}} = P_{e_{ij}} \cdot C_{e_{ij}} = P_{e_{ij}}^{G}(t) \cdot C_{e_{ij}} \tag{6}$$

$$R_{v_i} = P_{v_i} \cdot C_{v_i} = P_{v_i}^{G}(t) \cdot C_{v_i} \tag{7}$$

where $C_{e_{ij}}$ and C_{v_i} are the risk consequence of link failure and node failure, respectively, $P_{e_{ij}}(t)$ and $P_{v_i}(t)$ are the probabilities of communication link e_{ij} interruption or node v_i failure, respectively.

C. Risk Index of Service Failure

Communication service is carried from one site to another, and must go through at least one communication line. When link interrupts or nodes failure happens, the service transmitted will be interrupted. Therefore, the risk of service interruption is related to the risk of link and node which it is passed through. We suppose that communication links and nodes are alternately connected with each other to form a path w. The path which service s passes is defined as w_s, $w_s = \{V_s, E_s \mid v_i \in V_s, e_{ij} \in E_s\}$, and there are $|V_s|$ nodes and $|E_s|$ links on the path w_s. Since service is carried on the path, the service risk can be defined from different angles. Followings are the definitions:

1) Sum all the link risk and node risk

The risk of service s passing through path w_s, R_s can be calculated by summing all the link risk and node risk on the path, represented as:

$$R_s = \sum_{v_i \in V_s} R_{v_i} + \sum_{e_{ij} \in E_s} R_{e_{ij}} \tag{8}$$

2) Multiply the link risk and node risk

We suppose that risk of nodes and links are independent of each other. And the risk of service s can be calculated by multiplying every element of the path, represented as:

$$1 - R_s = \prod_{v_i \in V_s, e_{ij} \in E_s} \left(1 - R_{v_i}\right)\left(1 - R_{e_{ij}}\right) \tag{9}$$

The relative algorithms to search service path can only add weight, so before path optimization, we need to transform the 'product' of risk to the 'addition' of that. we also take the negative logarithm on both sides of (14) and the value ranges of the two sides is mapped into [0,+∞].

3) Select the maximum among link risk and node risk

The maximum among the risk of links and nodes on the path is considered as the risk of service *s*, $R_s^{'}$ represented as:

$$R_s^{"} = \max\left(R_{v_i}, R_{e_{ij}} \mid v_i \in V_s, e_{ij} \in E_s\right) \tag{11}$$

III. An Optimization Algorithm about Service Risk based on Risk Index

The service risk can be calculated by the risk of link and node on the service path. Based on the link risk and node risk, we optimize the risk of the service which is transferred between two nodes based on Dijkstra Algorithm to obtain the minimum risk value.

A. Sum Optimization Method (SOM)

Sum Optimization Method is improved from original Dijkstra Algorithm. Original Dijkstra Algorithm produces the shortest path according to the increment of path length. In SOM, the selection weight is defined as the risk rather than path length. Also, the selecting weight of the improved algorithm is the sum of link risk and node risk instead of the weight of link.

The services in the network is arranged in descending order, and the service with the largest service risk is optimized at first. After we obtain the optimized path, we arrange it into the network and the number of service running on the link and node is changed, resulting in the variation of link risk and node risk. Thus for the next service, the optimization method will utilize the updated link risk and node risk and obtain the optimized path and so on until the last service.

B. Multiplication Optimization Method (MUOM)

MUOM is similar with the sum optimization method, and the differences are that: firstly, the selection weight is changed to the negative logarithmic of link risk and node risk, like $-\ln\left(1-R_{v_z}\right)$ instead of R_{v_z}.

C. Maximum Optimization Method (MAOM)

Since the third way is to select the maximum among link risk and node risk to be the service risk, MAOM will avoid the link or node with the largest risk, and select a new path. In this method, we not only consider the risk of service, time delay, one of service QoS, is also considered. The optimization method is shown as follow:

1. Initialize and set network $\boldsymbol{G}(\boldsymbol{V},\boldsymbol{E},\boldsymbol{W})$, where $\boldsymbol{V}$ is the set of nodes, $\boldsymbol{E}$ is the set of links and $\boldsymbol{W}$ is the set of weight of each element including links and nodes. $\boldsymbol{W}(v_i)$ and $\boldsymbol{W}(e_{ij})$ represent the two dimensional weights of node v_i and link e_{ij}, while in $\boldsymbol{W}(v_i)=\{w_1(v_i), w_2(v_i)\}$, w_1 is the time delay of node v_i and w_2 is the risk of that. Also, set the service list (v_s, v_t) in descending order, where v_s and v_t are the source and destination nodes of service.

2. Select the current and un-optimized service from the service list, and label the elements (node or link) *EL* with the largest risk R_0.

3. Delete *EL* from $\boldsymbol{G}$ and obtain a new network $\boldsymbol{G_2}$, where if EL is link, delete these links from network, or if EL is node, delete the node and links connected with the node from the network.

4. Replace the risk with time delay as the weight in the sum optimization method of Section III-A, and apply the updated method to search a new path with the smallest time delay $path_1$, and the service risk of $path_1$, R_{path1} is the maximum among the link risk and node risk. And if the method cannot search any path, output the original service path as $path_1$ and its risk as R_{path1}.

5. Compare R_{path1} of $path_1$ and R_0 of original path. If $R_{path1} < R_0$, then output $path_1$ as the optimized path for this service and allocate $path_1$ into network $\boldsymbol{G}$. Or if $R_{path1} > R_0$, return step3.

6. If the service in service list is still not optimized, return step2.

IV. Case Analysis

A. Description of Simulation Scenarios

We choose part of power communication network topology graph to do case analysis. The topology schematic diagram is shown in Fig.3 which is simplified from the practical topology. There are 20 paths of relay protection service running on the network, and we need to search paths for them to deliver messages with lower risks. In our previous work[5], we have obtained the records of equipment failures, and calculated risk of each link and node, so we will not introduce any example about them here.

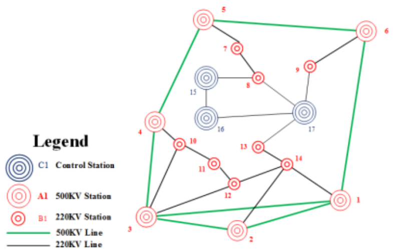

Fig.3 The topological diagram of part of a power grid

B. Comparisons among The Three Optimization Methods

From (10) (12), the risk of link and node is related with link importance, node importance, service importance and service number, and according to [6], the service importance of relay protection is 10. And in [6], for different levels of stations and links, their importance index is defined. When the 20 services of delay protection are allocated to the network, the service number of each node and link are defined. Thus we can calculate the risk of link and node.

1) Differences between risk of initial paths and optimized paths:

For these services, we use the 3 optimization methods: SOM, MUOM, and MAOM in Section III before. Fig.4 shows the differences between risk of initial paths and optimized paths for the three methods. The service is in descending order at service risk. The three optimization methods, especially MAOM can reduce the service risk for the service with high risk initially. And for the service with rather lower risk initially, the effect of optimization method is not clear. Overall, more service risk can be reduced by MAOM and SOM for service with high risk initially.

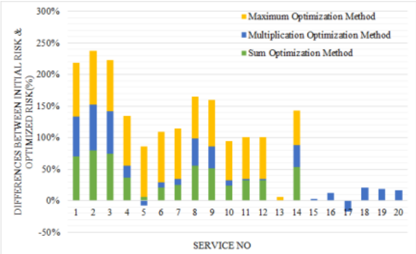

Fig.4 Differences (%) between risk of initial paths and optimized paths for 3 optimization methods

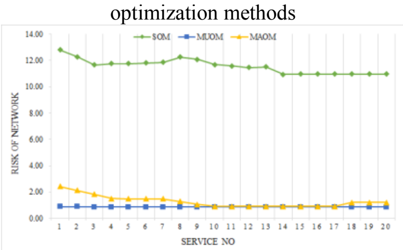

Fig.5 The trends of network services after service path updating for 3 different optimization methods

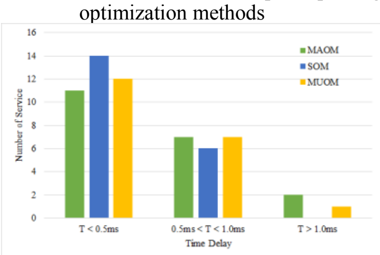

Fig.6 Comparision of time delay for 3 optimization methods

2) Trends of network services after path updating:

In this paper, the optimized path for one service will be allocated to the network before we search path for another service. The optimized path may be different from the original path, so the service number of link and node will be changed which decides the link risk and node risk. We can get the network risk from (14) (15) (17) in which the risk of service is change to that of network. In Fig.5, the network services for the three optimization methods are all descending. The network risk can be reduced by 50.00% using MAOM mostly. SOM can reduce the network risk by 14.24%. And MUOM can reduce network risk by 0.17%. Thus, MAOM has more advantages in network risk reduction than SOM and MUOM.

3) Comparision of time delay:

Time delay, is one of the index to evaluate quality of service. We calculate the time delay of each service path for three optimization methods shown in Fig.6. In Fig.6, most of the services are within 1.0ms for the three methods. Differences of distribution range and number among three methods are rather small. The average time delay of SOM is 0.40ms, the average time delay of MUOM is 0.49ms and that of MAOM is 0.53ms. Thus the messages carried by service will not be delayed using the optimized paths.

In conclusion, MAOM, MUOM, and SOM can reduce the service risk largely when risk of initial path is large. And MAOM has a better reduction in network risk. There is almost no difference in time delay for the three optimization methods.

V. Conclusion

The purpose of this paper is to analyze the risk of service in the network, and optimize the path of the service in risk. Firstly, we quantify the external factors and calculate the probability of failure of node and link which is the caused by different kinds of factors, like nature factors, equipment factors and human factors. Using failure probability and risk consequence value, we build the model of risk of node and link, then the risk of service according to the service path. Finally, we use three optimization methods to reduce the service risk based on Dijikstra Algorithm with different weights. Case analysis shows that the three optimization methods can all reduce the service risk and the network risk. The optimized paths are all within time delay standard.

Though the network risk and service risk can be reduced using the optimization methods, the risk equalization among link risk and node risk is not taken into consideration. In our future study, except risk equalization, we will concentrate on handling mechanism of smart grid for different states, like maintenance mode, work mode and etc.

Acknowledgment

This work was supported by Project of State Grid Corporation of China: Research on Communication Architecture and Hardware-In-The-Loop Simulation for Real-Time Wide-Area Stability Control of Electric Power System (SGGSXT00GCJS1600065), the 863 Program (Grant No.2015AA01A705), and National Natural Science Foundation of China (NSFC) (Grant No.61271187).

References

[1] V. Kounev, M. Lévesque, D. Tipper, and T. Gomes, "Reliable Communication Networks for Smart Grid Transmission Systems," *Journal of Network and Systems Management,* vol. 24, pp. 629-652, 2016.

[2] Shin, D. H., He, S., & Zhang, J., "Robust and cost-effective architecture design for smart grid communications: A multi-stage middleware deployment approach," in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications,* pp. 2822-2830, April, 2014.

[3] ZENG Qingtao, QIU Xuesong, GUO Shaoyong, QI Feng and MENG Luoming, "Risk Balancing Based Routing Mechanism for Power Communications Service," *Journal of Electronics & Information Technology*, pp. 1318-1324, June, 2013.

[4] Yan Jiamei, Xu Jianbing, NI Ming and YU Wenjie, "Impact of communication system interruption on power system wide area protection and control system," *Automation of Electric Power System*, pp. 17-24, 2016.

[5] ZHAO Puyuan, YU Peng, JI Chenchen, FENG Lei, and LI Wenjing, "A Routing Optimization Method based on Risk Prediction for Communication Services in Smart Grid", *12th International Conference on Networking and Service Management (CNSM), GISN and ManSDN/NFV workshops*, accepted, pp.1-6, 2016.

[6] ZHAO Ziyan, and LIU Jianming, "A new service risk balancing based method to evalute reliability of electric power communication network," *Power System Technology*, pp. 209-213, October, 2011