Proceedings of CECNet 2021
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA210449

Node Importance Based Protection in Power-Grid Optical Backbone Communication Networks

Xiaobo LI[a], Guoli FENG[a], Run MA[a], Lu LU[b], Kaili ZHANG[b], Xinnan HA[a], Wenbin WEI[a], Ning WANG[a], Xiaosong YU[b] and Yongli ZHAO[b,1]
[a] *State Grid Ningxia Electric Power Co. LTD, Information communication corporation, Yinchuan 750001, China*
[b] *Beijing University of Posts and Telecommunications, Beijing 100876, China*

Abstract. Power-grid optical backbone communication network is a special communication network serving for power system. With the development of new internet technology, there are more and more services carried by power-grid optical backbone communication networks. It plays an important role in the protection of nodes, especially important nodes which often carry important information of the network, when the network is under heavy traffic load. Hench, to solve this problem, we propose the concept of node importance and design a node importance-based protection algorithm under heavy traffic load scenario in power-grid optical backbone communication networks. Simulation results show that the proposed node importance based protection algorithm can obviously reduce blocking probability of the important nodes and improve the performance of the entire network in terms of blocking probability.

Keywords. Node importance, resource shortages, power grid, optical networks

1. Introduction

The security and stability of power-grid optical backbone communication networks play an important role in the whole power system. And the current power grid construction is constantly improving. The power communication system is becoming more and more complex, the scale of the power communication network continues to expand [1]. However, as the key service of power system increasingly depends on communication and information system, power system is more vulnerable to network attack [2]. In addition, in the scenario of heavy traffic, once a fault occurs in the network, it will bring more serious losses. They all pose challenge to the survivability of the power-grid optical backbone communication network. At the same time, with the development of big data, cloud services, artificial intelligence and other emerging technologies, networks can provide more diverse types of services [3]. And the establishment of core nodes, such as data center and control center, makes some nodes more important than others, and the traffic originating from or destining to these nodes needs to be guaranteed first.

[1] Corresponding Author, Yongli Zhao, Beijing University of Posts and Telecommunications, Beijing, 100876, China; E-mail: yonglizhao@bupt.edu.cn.

For the evaluation of node importance, several methods have been proposed. For example, in Ref [4], the authors proposed a weighted K-shell decomposition method, which combines the nodes in the network, the degree index and the number of iterations to rank the importance of nodes. Ref [5] analyzes the importance of nodes based on four indexes: feature vector centrality, proximity centrality, intermediary centrality. In this paper, we propose a new definition of node importance, which takes into account the nodes carrying important services. In addition, there are also many research on the survivability of network. In Ref [6], a flexible differentiated protection mechanism is proposed, which can switch between different path protection schemes (such as no protection, shared path protection and 1 + 1 protection) to adapt to different service availability. In Ref [7], the authors present ILP formulations to solve the multi-layer survivability problem. However, the protection of some nodes under heavy traffic load has not been studied yet.

To solve this problem of the protection of some nodes under heavy traffic load, in this paper, we propose the concept of node importance (NI) in *Section 2*, which gives different importance levels for network nodes. The corresponding routing and wavelength allocation strategy is designed in *Section 3* to ensure that nodes with different importance can be protected with higher requirements. *Section 4* gives the simulation settings and results which indicate that proposed node importance based protection (NIP) scheme can obviously improve the performance of important nodes in terms of blocking probability.

2. Problem Statement

Survivability mechanism includes protection mechanism and recovery mechanism. The basic idea of the protection mechanism is to reserve a part of redundant resources as the standby resources in advance. When the links or nodes fail, the main system affected by the failure will be quickly switched to the standby system. The protection mechanism can be divided into link protection, path protection and multi segment protection. But node-based protection schemes have not been widely studied. The algorithm proposed in this paper is a node-based protection strategy. Firstly, the concept of node importance is defined. For node importance, some studies define the node with the highest degree as important nodes, and some studies define the node with the largest traffic as important nodes. However, with the establishment of core nodes such as data center and control center, these nodes may not only carry the most traffic, but also often carry important service information in the network. Therefore, this paper defines those nodes responsible for core service as important nodes and gives priority to their protection.

In addition, the current routing and wavelength allocation schemes in power-grid optical backbone communication networks generally use Dijkstra algorithm or KSP algorithm to select the shortest route, and then use FF algorithm to select the wavelength that meets the requirements. This scheme is relatively simple to implement, but it ignores the traffic load distribution in the network and the load balance of the link. It is not flexible enough to deal with some problems in heavy traffic load scenarios. The traditional schemes treat all nodes equally, but in practice, the importance of network nodes is often not the same. In this paper, the nodes responsible for core services in the network are defined as important nodes. Since these nodes carry important services information in the network, the services originating from or sending to these nodes need to be guaranteed in priority, so we set higher node importance (NI) for these nodes. When

the network resources are abundant, the KSP algorithm is used to find the path and the FF algorithm is used to allocate the wavelength. When the adjacent links and secondary adjacent links of important nodes are short of resources, certain spectrum resources need to be reserved for the services of important nodes. At this time, only the services from / to important nodes are carried.

3. Node Importance based Protection (NIP) scheme

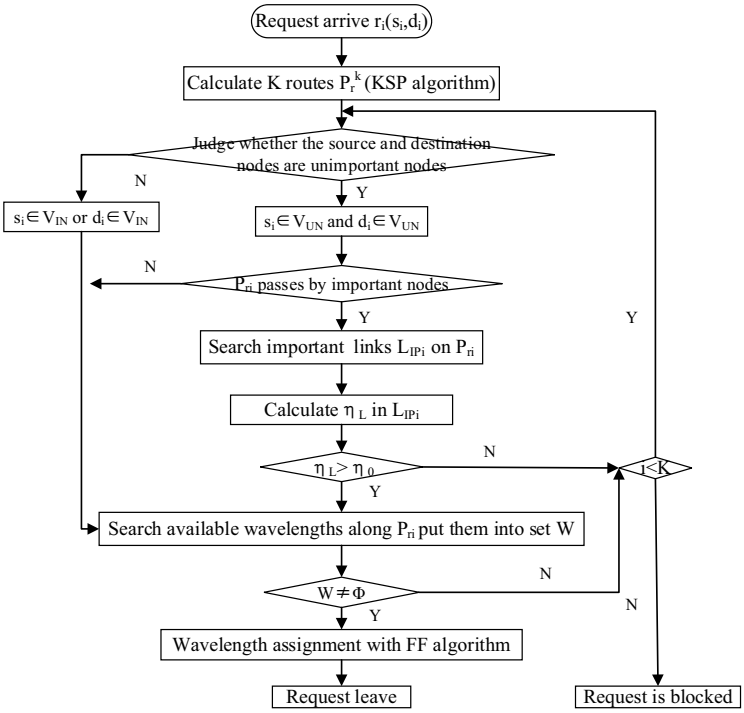

Figure 1. The flow chart of node importance based protection (NIP) scheme.

The flow chart of node importance based protection scheme is shown in Figure 1. In our algorithm, node importance has two levels: high and low. The nodes of different importance are called important nodes and unimportant nodes, respectively. When the network resources are sufficient, or the service only passes through low-importance nodes, we only need to allocate according to the KSP and First-fit algorithm. If the service passes through high-importance nodes and there are few remaining wavelengths in the adjacent links of these important nodes, we need to perform some additional processing to ensure that these resources are reserved for services from/ to important nodes. In the flow chart, the topology of the network is represented as $G(V, E)$, where V and E are the node set and link set respectively. The important node set in the network is $V_{IN} = \{v_{IN1}, v_{IN2}, \dots \dots v_{INn}\}$, the important link set is $E_{IN} = \{e_{IN1}, e_{IN2}, \dots \dots e_{IN2}\}$. The unimportant node set is $V_{UN} = \{v_{UN1}, v_{UN2}, \dots \dots v_{UNn}\}$, the unimportant link set is $E_{UN} = \{e_{UN1}, e_{UN2}, \dots \dots e_{UNn}\}$. The service request is denoted as $r_i(s_i, d_i)$,where s_i is the source node and d_i is the destination node.

After the service request arrives, firstly use KSP algorithm to calculate *K* shortest routes $P_r^k = \{P_{r1}, P_{r2}, \ldots \ldots P_{rn}\}$, and get the i_{th} (i< K) path P_{ri} from the path set. Then judge the type of source and destination nodes. If the source node or destination node is important node, search available wavelengths along P_{ri} and allocate wavelengths with FF algorithm directly. If the source node and destination node are unimportant node, then judge whether the path passes by important node, if not, try to allocate the wavelength. Otherwise, search important links L_{IPi} and calculate the percentage η_L of free wavelengths of each link in the important link set that the path passes through. If η_L is greater than the percentage of wavelengths reserved for important links η_0 , which indicates that there are sufficient wavelength resources on the important link, so this path is available and FF algorithm is used to allocate the wavelength. Until all *K* paths are executed, if all *K* paths are allocated unsuccessfully, the request is blocked.

4. Simulation Analysis

To evaluate the performance of the proposed *NIP algorithm*, we use the *14-node NSFNET topology* in our simulation. There are *80* wavelengths in each optical link, and each request demands for a single wavelength. *Node 5* and *Node 9* are set to be important nodes so that the traffic from/to *Node 5* or *Node 9* will be protected. *Figure 2-4* shows the simulation results under 3 different wavelength resources reserved percentages. *Figure 2, 3, 4* are under *4%, 3%, 2%* respectively. Blocking probability of important nodes are calculated by the number of requests and blocked requests that source node or/and destination node are important nodes. Also, blocking probability of unimportant nodes as well as the blocking probability of important and unimportant node, that is, entire network, are listed together. Besides, to evaluate the impact of adding important nodes on the entire network, a *Non-Node Importance based Protection (NNIP) algorithm* without considering important node is also simulated for comparison.

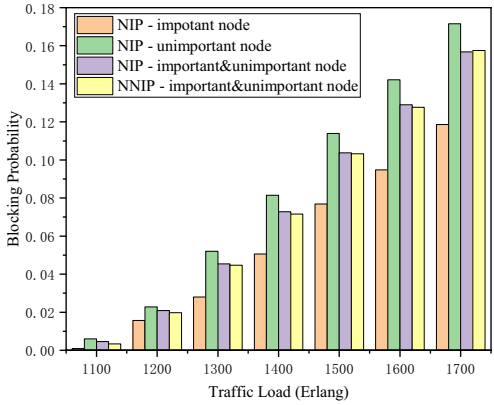

Figure 2. Blocking Probability of important nodes compared with unimportant nodes and the entire network when 4% wavelengths reserved for important links.

In *Figure 2*, we can see that the *NIP algorithm*, which considers reserving wavelengths can largely reduce the blocking probability of important nodes. As traffic load increases, blocking probability reduce more compared with the network blocking

probability. But for exchange, the blocking probability of unimportant nodes increases. It is inevitable that when the network under the high payload, important nodes will no more as the relay nodes. Absence of candidate paths will must lead to this result. As for the entire network, it shows that *NIP algorithm* leads to a slight rise of the network blocking probability than *NNIP* when traffic load is in the range of *1100-1600 Erlang*. When traffic load went to *1700 Erlang*, *NIP algorithm* achieves lower network blocking probability than *NNIP*. To further investigate the influence of the percentage of reserved resources in *NIP algorithm* on network blocking probability, we conduct the simulation when 3% and 2% wavelengths reserved for important links.

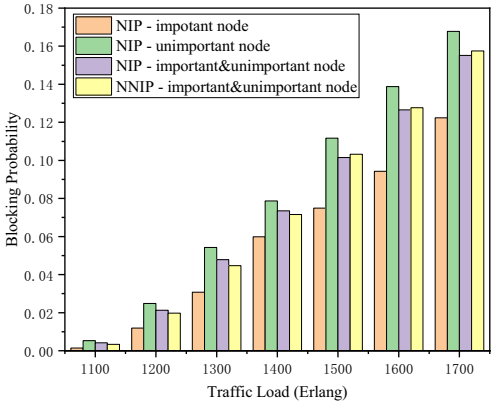

Figure 3. Blocking Probability of important nodes compared with unimportant nodes and the entire network when 3% wavelengths reserved for important links.

In *Figure 3*, it shows a similar trends as *Figure 2* that blocking probability of *NIP* with important node reduce more and with unimportant node increases more compared with total network blocking probability as traffic load increases. However, both of them is less than that in *Figure 2* when 4% wavelengths reserved, which means the protection effect to important nodes is weaken. When it comes to the network blocking probability, *NIP algorithm* achieves lower network blocking probability than *NNIP* under heavy payload situation, i.e., traffic load values from *1500* to *1700 Erlang.*

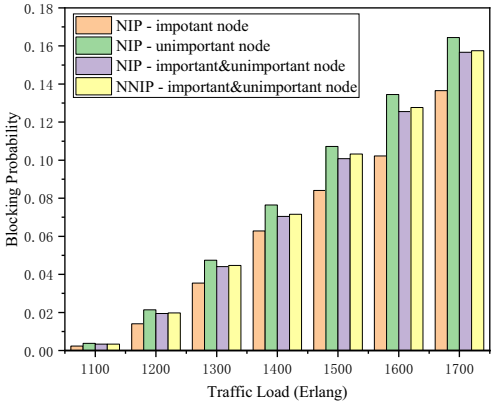

Figure 4. Blocking Probability of important nodes compared with unimportant nodes and the entire network when 2% wavelengths reserved for important links.

We have known that the blocking probability of entire network using *NIP algorithm* could be either higher or lower than using *NNIP algorithm* without considering important nodes. Comparing *Figure 2, 3* and *4,* it manifests that network blocking probability also related to the percentage of wavelengths reserved for important links. For example, in *Figure 2*, the blocking probability of network using *NIP algorithm* is mostly higher than that using *NNIP algorithm*. While in *Figure 4*, the situation is opposite to *Figure 2* that the blocking probability of network using *NIP algorithm* performs better in most cases (blocking probability of network using *NNIP algorithm* are same in *Figure 2, 3 and 4*). Over all, the performance of important nodes in all situations can be largely improved using the proposed algorithm, and only a few wavelengths reserved can improve the performance not only for important nodes, but for the entire network. If better protection to important nodes is needed, a little cost of the entire network should be paid.

5. Conclusions

This paper focus on the problem of protecting several core nodes in power-grid optical backbone communication networks under heavy traffic scenario. The concept of node importance is designed to distinguish important nodes with others. A node importance-based protection algorithm is proposed and evaluated under different resources reserved. It is found that the proposed algorithm could protected important nodes effectively, and can even improve the performance of the entire network in terms of blocking probability under heavy payload situation.

Acknowledgements: This work was supported by the Mass Science and Technology Innovation Project of Ningxia Electric Power Co., LTD. Information Communication Company of State Grid (No. 5229XT21000J).

References

[1] H. Ding, Y. Wang, A. Liu, D. Yang, D. Chen and R. Xiu. Review on Intelligent Optimization Technology for Survivability of Power Grid Backbone Communication Networks. 2021 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA); 2021 Jun 28-30; Dalian, China. p. 499-502.

[2] Y. Wu, H. Xu and M. Ni. Defensive Resource Allocation Method for Improving Survivability of Communication and Information System in CPPS Against Cyber-attacks. in Journal of Modern Power Systems and Clean Energy. 2020 Jul; 8(4): 750-759.

[3] X. Liu, D. Niu, H. Zhang and H. Dong. Analysis of Key Technologies in the Construction of Ubiquitous Power Internet of Things. Proceedings of 2019 2nd International Conference on Intelligent Systems Research and Mechatronics Engineering (ISRME 2019); 2019; Taiyuan, Shanxi. p.557-560.

[4] J. Xing, J. Chen, X. Sun, X. Zhang and R. Zhang. A K-shell Improved Method for the Importance of Complex Network Nodes. 2018 IEEE 7th Data Driven Control and Learning Systems Conference (DDCLS); 2018; Enshi, China. p. 639-643.

[5] X. Li, Y. Han, X. Wu and D. A. Zhang. Evaluating node importance in complex networks based on TOPSIS and gray correlation. 2018 Chinese Control and Decision Conference (CCDC); 2018; Shenyang, China. p. 750-754.

[6] X. Chen et al. Flexible Availability-Aware Differentiated Protection in Software-Defined Elastic Optical Networks. in Journal of Lightwave Technology. 2015 Sep; 33(18): 3872-3882.

[7] P. Papanikolaou, K. Christodoulopoulos, E. Varvarigos. Joint multi-layer survivability techniques for IP-over-elastic-optical- networks. in IEEE/OSA Journal of Optical Communications and Networking. 2017 Jan; 9(1):A85-A98.