Advances in Engineering Research, volume 181

International Conference on Electronical, Mechanical and Materials Engineering (ICE2ME 2019)

A Software-Defined Traffic Differential Protection Mechanism of Power Grid Communication Networks

Chuan Liu[1,2], Xin Xu[3], Jing Tao[1,2] and Shidong Liu[1,2]

[1]Global Energy Interconnection Research Institute co,.Ltd, Nanjing ,China

[2]State Grid Laboratory of Electric Power Communication Network Technology, Nanjing, China

[3]State Grid Chongqing Electric Power co. Electric Power Research Institute, Chongqing, China

***Abstract*—With the rapid growth of various kinds of services demands, the traditional power network architecture has faced many problems and challenges. The software defined network (SDN) architecture has the advantages of flexibility, programmability and centralized control, which can be applied to power grid communication networks and solve the problems. Based on the common link failure problems in the network, the traditional 1+1 protection mechanism has fast switching speed, but it has very low utilizations of links. Based on SDN and the traffic characteristics of power grid communication networks, this paper proposes a traffic differential protection mechanism, which utilizes different protection mechanisms for different traffic flows. The simulation results show that the proposed protection mechanism can effectively reduce the link resource overhead and ensures reliable recovery of control traffic and other types of traffic flow. It achieves a good balance between resource overhead and delay of network.**

Keywords—power communication network; SDN; link protection; traffic differential protection

I. INTRODUCTION

Smart grid is an important direction for the future development of electric power industry. It is the product of traditional power grid organically combining advanced technology in information technology, automatic control, sensors and other fields. Compared with the traditional power grid, smart grid has more flexible and comprehensive distribution network control, realizing the bidirectional flow of energy and information in the network. With the continuous development and expansion of smart grid, it has more and more essential improvements in power supply reliability, operational efficiency, system security and so on. As an important part of smart grid, the success of power communication network development will largely determine the security, efficiency and scientificity of power generation and supply. Therefore, the promotion and development of power communication network will be particularly important. Although the traditional power grid has been greatly improved in the aspect of intellectualization, there is still a big gap from the real smart grid.

Software Definition Networking (SDN) achieves a more open network architecture by decoupling control plane and data plane. It can effectively solve the problem of coupling and solidification between systems and devices in the current power grid. SDN enables the power communication network to achieve more comprehensive and flexible control through the control plane of logical centralization. In addition, its open programming interface allows the power grid to bear more new business and to support more new functions.

II. SOFTWARE-DEFINED TRAFFIC DIFFERENTIAL PROTECTION MECHANISM

A. Service Analysis of Power Communication Network

According to the voltage level and the scattered coverage of the network, China's power communication network is mainly divided into backbone communication network, medium voltage communication network and low-voltage communication network separately. The backbone communication network mainly carries two kinds of business, one is the dispatch or transmission of line protection communication and control flow, the other is some office and management data with large amount of data. Medium-voltage communication access network is the extension of backbone communication network. It carries the key business of power communication network. It is similar to the backbone communication network, including distribution automation and interactive business. The main business of low-voltage communication access network is collecting information, including electricity information collection, charging pile measurement and monitoring, etc.

In the services carried by power communication network, the operation control services have very strict requirements on delay and bit error rate. Generally, the delay is less than tens of milliseconds and the bit error rate is less than 10^{-8}. Information acquisition services have a high demand for bandwidth of approximately several megabytes, with the requirement of delay within several hundred milliseconds and the requirement of bit error rate less than 10^{-6}. Intelligent interaction services have high tolerance for delay, although they do not need to reserve network resources, they require high loss rate of packet.

B. Technology of Traffic Differential Protection Based on Software Defined Networking

For the protection of single link failure, a common scheme is 1 + 1 path protection, which means that the sender transmits the same data on the main and standby paths, and the receiver normally chooses the data on the main path and discards the packet data on the backup path. When the main path of the link fails, the receiver switches to the backup path to restore the main service. This protection switching method is fast and easy to operate, but it increases the transmission of data and reduces the utilization of the link.

Based on the classification of the aforementioned services, the power communication network can be artificially divided into three levels in terms of delay, bandwidth and importance. The business priority level of control class is set to 2, that of information collection class is set to 1, and that of interaction class is set to 0.

According to the problems existing in the traditional 1+1 protection mechanism and the result of traffic priority division, a differential protection mechanism based on traffic priority level is proposed in this paper where different protection mechanisms are applied to three main types of traffic in SDN controller.

Firstly, header information of traffic flow is sent to SDN controller through switch. The controller determines the type of service and the priority level of its division according to its header information, and then puts the same priority business data into the cache queue. Secondly, flow protection and control are mainly embodied in the following two aspects. For control flow, considering the need and importance of low latency, Dijkstra algorithm is used to pre-calculate the shortest shared path (no common path) of backup and store it in the flow table rules of SDN controller. In case of failure, the local handover method is adopted to switch the new path quickly. This method has less delay, and could quickly recover the link failure. For the flow of information collection class and interaction class, because of its low delay requirement, the reactive protection strategy is adopted, that is, when the link fails, the shared backup path is calculated again in the existing network topology to realize the bypass of the failed link.

As is shown in Figure I. Suppose the source switch and the destination switch is S1 and S7 respectively. When network runs normally, the shortest path policy is stored in the flow table. When < S1, S3 > link failures occur, the local handover paths < S1, S2, S7> are used for control traffic. The shortest paths < S1, S4, S5, S7> are calculated for collection and interaction traffic in the remaining paths, thus achieving more accurate differential protection for different traffic flows and improving the utilization of links. The flow chart of the shortest path algorithm is shown in Figure II.

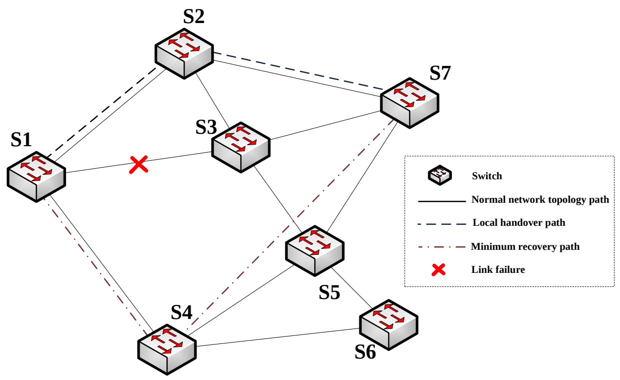

FIGURE I. EXAMPLE OF TRAFFIC DIFFERENTIAL PROTECTION

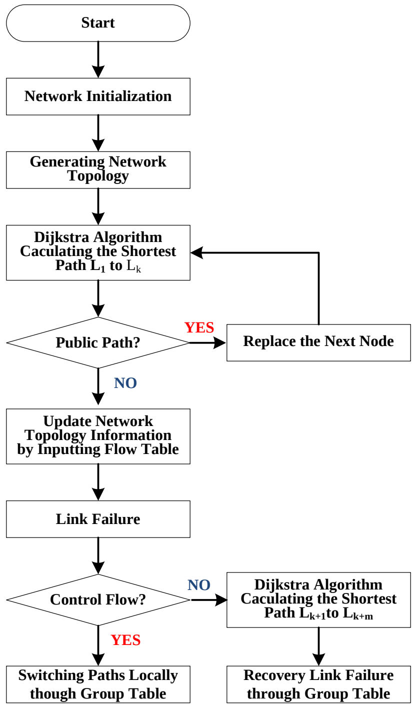

FIGURE II. FLOW CHART OF BACKUP PATH ALGORITHM

III. SIMULATION EXPERIMENT AND RESULT ANALYSIS

In this section, we will simulate and analyze the mechanism of differential current protection control using backup path algorithm proposed above. The main evaluation parameters are the average end-to-end delay and bandwidth consumption based on backup path calculation.

A. Setting of Simulation Parameters

Firstly, a network topology graph is generated. The number of nodes is set to 12, the traffic flow is set to Poisson distribution, the link bandwidth is set to 2.5M, and the packet size is set to 200 bytes and 600 bytes of bimodal distribution.

The main indicators for evaluating the network performance change after the implementation of the strategy are average transmission delay and bandwidth consumption rate. The average end-to-end delay refers to the delay between the sending node and the target node. The smaller the delay, the better the performance of backup path selection. Average bandwidth consumption rate refers to the phenomenon of packet loss caused by link congestion which illustrating by the ratio of data streams consume bandwidth and total specified bandwidth. Network load refers to the ratio of the number of traffic generated in the carrier network divided by the reference number of traffic. The network topology generated in the simulation is shown in Figure III.

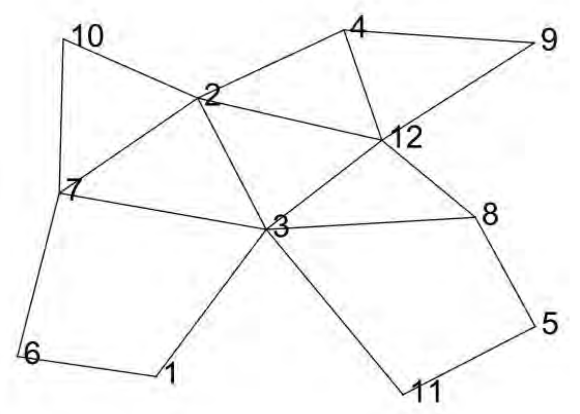

FIGURE III. NETWORK TOPOLOGY

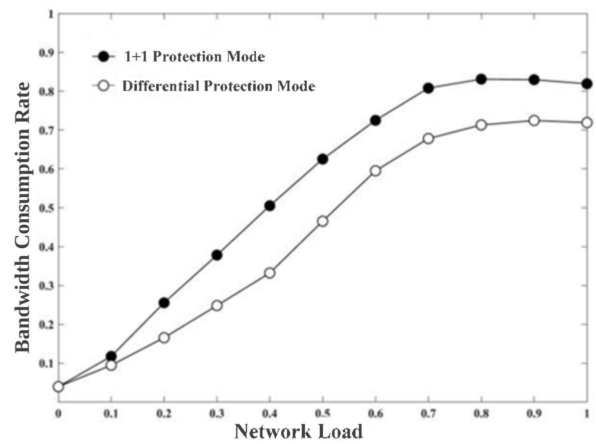

FIGURE IV. COMPARISON OF BANDWIDTH CONSUMPTION RATE

B. Simulation Experiment and Result Analysis

In the simulation of network topology, a path is randomly disconnected to simulate a single data link failure scenario, and then the performance of the network under five experiments is evaluated.

The Figure IV shows the simulation of bandwidth consumption rate under the traditional 1+1 protection switching mode and traffic differential protection mode. As can be seen from the figure, with the increasing network load, the bandwidth consumption rate under both schemes is increasing. Under the same network load, the bandwidth consumption rate of traffic differential protection is significantly lower than that of traditional 1 + 1 protection. According to the statistics of bandwidth consumption under different loads, the average bandwidth consumption rate of traffic differential protection mechanism is 12.62% lower than that of dedicated 1 + 1 protection mechanism. The reason for this situation is that when a single link fails, the differential protection mechanism adopts local handover protection for control traffic, while the lower-level interactive and acquisition traffic uses rerouting recovery protection. Compared with the 1+1 protection mechanism, the former has fewer redundant backup paths, and only when the link fails, handover beforehand. The backup path stored in the flow table is protected, rather than always transferring the same data under the primary and standby paths. Therefore, the differential protection mechanism has a significant reduction in bandwidth consumption compared with the 1 + 1 protection mechanism.

The Figure V shows the average end-to-end delay curves of differential protection schemes and 1+1 dedicated protection schemes. As can be seen from the figure, the end-to-end latency of both mechanisms increases with the increase of network load. Under the same load, the delay of 1+1 protection mechanism is shorter than that of differential protection mechanism. According to the statistical data, the average delay of differential protection mechanism is 29.4 ms longer than that of 1+1 special protection. This is determined by the principles of the two mechanisms. Differential protection mechanism uses reactive route recovery mode in the protection of uncontrolled traffic flow, which has higher delay than the main and standby path switching mode of 1+1 protection mechanism. Therefore, the difference of delay between the two mechanisms is mainly reflected in that the former needs to calculate the path when the link fails.

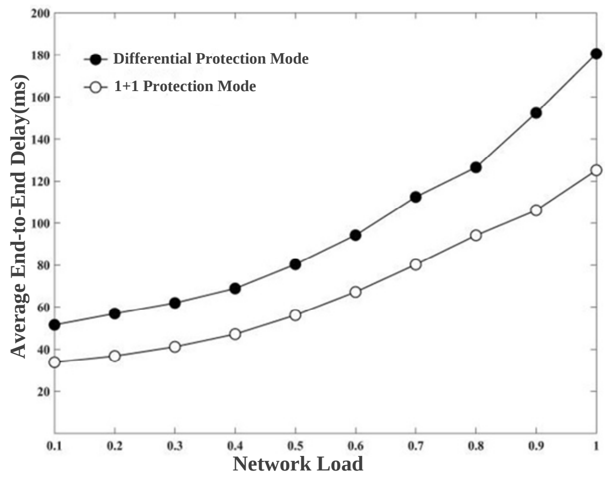

FIGURE V. COMPARISON OF AVERAGE END-TO-END DELAY

IV. CONCLUSION

This paper introduces some problems existing in traditional power communication network and the concept and application advantages of power communication network architecture based on software-defined architecture. Based on the idea of SDN, this paper adopts an overlapping and integrated network control architecture to realize the collection of different functions of each network in the power grid. Aiming at the reliability requirement of this architecture, this paper proposes a flow differential protection control strategy for single data link failure, which classifies the traffic flow in power communication network for different fault recovery.

Finally, the simulation results show that the scheme can achieve different types of traffic recovery in case of link failure. The bandwidth consumption rate is 12.62% lower than that of 1+1 protection mechanism. Although the average end-to-end delay of this mechanism is about 30 ms longer than that of dedicated 1+1 protection, this differential protection mechanism based on traffic type will better differentiate the protection of different traffic flows. On the premise of fast switching path for control traffic with high delay requirement, backup path is calculated for traffic flow with low delay tolerance to achieve link delay recovery. In fact, compared with 1+1 protection mechanism and computed shortest path recovery mechanism, this mechanism achieves a better balance in both delay and bandwidth consumption on the premise of ensuring network reliability.

ACKNOWLEDGMENT

This work was supported by State Grid Corp Science and Technology, China (no. GCQDK00DWJS1800037).

REFERENCES

[1] Liu Chuan, Li Binglin, Lou Zheng, et al. Analysis on Time Delay Performance of SDN Controller Supporting Power Service Planning[J]. Automation of Electric Power System, 2017,41(17), 142-147.

[2] Zhang Lei, Zhan Zhenbin, Wei Luping, et al. Test and Analysis of Piecewise Delay in Wide Area Measurement System.[J]. Automation of Electric Power System, 2016, 40(6), 101-106.

[3] He Linbo, Jiang Dingde, Zhong Weijia, et al. A Routing Optimization Algorithm Based on Energy Efficiency and Frequency Effect[J]. Journal of Electronics, 2016,44 (10):2314-2322.

[4] J.Medved,R. Varga,A. Tkacik and K. Gray. OpenDaylight: Towards a Model-Driven SDN Controller architecture. Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, Sydney, NSW, 2014, pp. 1-6.

[5] Jia Huibin, Xue Kaifu, Ma Jing, et al. Improved Ant Colony Algorithm for Multi-path Routing Selection in Wide-area Protection Communication System[J]. Automation of Electric Power System. 2016,40(22):22-26.