Analysis on Invulnerability and Real-Time Performance for Smart Grid Network

Liu Xiaosheng[1], Hai Tianxiang[1], Zheng Jian[1]

[1] The Department of Electrical Engineering and Automation Harbin Institute of Technology ,Harbin, China
liuxsh@hit.edu.cn, haitianxiang9999@163.com, acmilan2290@126.com

Abstract - In the process of building strong smart grid, the communication technology becomes an important means that supports Intelligrid Architecture. Smart grid has strict requirements in the reliability and real-time performance of communication. MPLS can improve the service quality of power communication. Aiming at the MPLS area, this paper proposes a kind of artificial spider web topology and analyses the invulnerability. Based on this, the OPNET simulation is run for road-balancing and re-routing. The results show that the MPLS routing algorithm has strong ability of road-balancing and re-routing. It can be used to improve the real-time performance of communication.

Keywords - smart grid; artificial spider web topology; the degree of invulnerability; MPLS

1. Introduction

Intelligentization of smart gird is based on high-speed, real-time and bidirectional communication network. Communication is the core technology of smart grid which includes six links: Power generation, transmission, substation, distribution, electricity and scheduling. Power plants, substations, switching stations, big users and dispatching centers are major nodes in smart gird communication network which have a wide variety of communication services[1]. Generally, these major nodes are far away from each other and the lines between these nodes are likely to be affected by the environment. With increasing amount of transmission data and types of business, there will be problems of traffic overload and data congestion between major nodes. Therefore, it's necessary to establish a highly reliable and strong real-time network between these major nodes. This paper proposes the artificial spider web topology aiming network between major nodes.

The traditional topologies of power communication network mainly include star, ring and chain. These topologies can hardly meet the demands of smart grid communication that are mentioned before. Combined with the characteristics of power communication and modern bionics views, this paper proposes the artificial spider web topology aiming network between major nodes. It proves that the artificial spider web topology is more reliable than other topologies through the calculation of the degree of invulnerability. Also, it brings the MPLS(multi-protocol label switching) routing algorithm to deal with two possible failure of power communication. The OPNET simulation results show that the MPLS routing algorithm based on artificial spider web topology has strong ability of road balancing and re-routing.

2. The Spider Web Model

Natural spider web has not only elegant, symmetric structure, but also strong anti-destruction capacity. Currently, the studies on spider predation strategy and spider web structure characteristics mainly concentrate on military, biology and chemistry. However, it is still very rare that people apply the awareness of the spider web performance and structure to the field of communication studies.

As the spider web has the characteristics of strong anti-destruction capacity, this paper uses the topology in the smart grid communication network between major nodes to meet the requirements of communication reliability. To simple the natural spider web structure and extract several links and nodes, we get the typical signal-layer artificial spider web model shown as Figure.1. The signal-layer artificial spider web consists of a star structure and a number of ring structures and has the advantage of these two structures. Further, we can get the two-layer artificial spider web model after adding corresponding nodes outside the edge nodes.

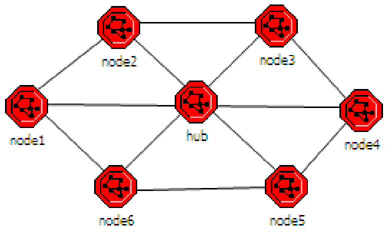


Figure.1: signal-layer artificial spider web model

3. The Calculation of the Degree of Invulnerability Based on Spider Web Model

A. The Analysis of Degree of Invulnerability

When the power communication network is impacted by external factors, the working section requires good connectivity[2]. Invulnerability is an important aspect of reliability. The degree of invulnerability is the measurement of invulnerability which represents the ability to maintain or keep an acceptable working condition when network is broken down. The analysis based on network's degree of invulnerability can measure network's invulnerability well.

The analysis on the degree of invulnerability is shown below when there is no failure nodes and links in the network:

(1) Calculate the connectivity when the network is normal.

(2) Calculate the importance of all nodes in the network and delete the most important node and relative links.

(3) Judge whether there is node connection in the network. If yes, skip to step (1). If no, skip to step (4).

(4) Calculate the sum of the connectivity when the network is normal and damaged. The result is the degree of invulnerability.

As is mentioned before, calculating the importance of nodes is the most important step. So, it's first to introduce the calculation about the importance of nodes and then analyze the calculation about the degree of invulnerability.

1) The calculation about the importance of nodes: There are certain hops between any two nodes in the network. It is called hop plane nodes which have the same hop with the node i[3]. The relationship between node i and other nodes is converted to the relationship among all other nodes. Thus, we obtain the formula of the importance of nodes shown below:

$$P_i = \sum_{j=1}^{N} p_{ij} \qquad (1)$$

In the formula (1), Pi means the importance of node i, N means the hops between node i and the farthest hop plane nodes. Pij means the connectivity between node i and hop plane j.

As the relationship between node i and other nodes is converted to the relationship among all other nodes and all hop planes are connected in series, the connectivity between node i and hop plane j is shown as formula (2).

$$\begin{cases} p_{i1} = p_{01} \\ p_{i2} = p_{i1} \Box p_{12} \\ \vdots \\ p_{i(m+1)} = p_{im} \Box p_{m(m+1)} \end{cases} \qquad (2)$$

In the formula (2), p01 means the connectivity between node i and hop plane nodes which hop is 1 namely pi1. pm(m+1) means the connectivity between hop planes with the hop of m and m+1. pm(m+1) is shown as formula (3).

$$p_{m(m+1)} = \frac{l_m}{n_m(N-1)} \qquad (3)$$

In the formula (3), lm means links between two hop planes. nm means the amount of nodes that are on the hop plane m. N means the amount of all nodes in the network.

2) The calculation about the degree of Invulnerability: Supposing that the amount of nodes in the network G is n, the network is G_k after deleting k nodes and the amount of nodes before all nodes isolate is m. The connectivity NC_k(i,j) between node i and j is defined below:

$$NC_k(i,j) = \sum_{t=1}^{q} \frac{1}{JN(t)} \qquad (4)$$

In the formula (4), the amount uncrossed route between node i and j is q. The hop of t-path between node i and j is JN(t). We choose the path with the minimal hop when two or more paths are through the same intermediate node.

The connectivity CM(k) with k nodes deleted is defined below:

$$CM(k) = \sum_{i=1}^{n-k-1} \sum_{j=i+1}^{n-k} NC_k(i,j) \qquad (5)$$

Finally, we reach the formula of invulnerability SM(G) after weighted summation of CM(k).It is shown below:

$$SM(G) = \sum_{k=0}^{m-1} CM(k)B(k) \qquad (6)$$

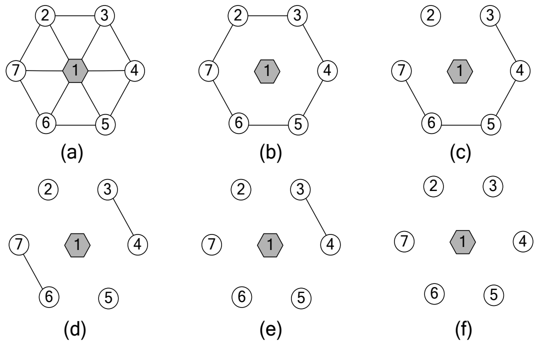


Figure.2: the invulnerability calculation of signal-layer artificial spider web topology

In the formula (6), SM(0) means the degree of invulnerability. The steps on calculating the invulnerability of the spider web are shown in the Figure.2. According to the calculation mentioned before, calculating the degree of invulnerability including star, ring, double-star and the spider web. The calculation result is shown as Table I.

TABLE I Invulnerability of different topologies

Topology	Invulnerability
star	13.5
ring	23.12
double-star	47.5
single-layer spider web	56.32
two-layer spider web	247.16

From Table.1, spider web structure especially the two-layer spider web shows better ability of invulnerability than other topologies. The variation that the connectivity of different topologies reduces with increasing deleted nodes is shown as Figure.3.The abscissa means the amount of deleted nodes and the ordinate means the connectivity of network. With the amount of deleted nodes increasing, the connectivity of two-layer spider layer is still high

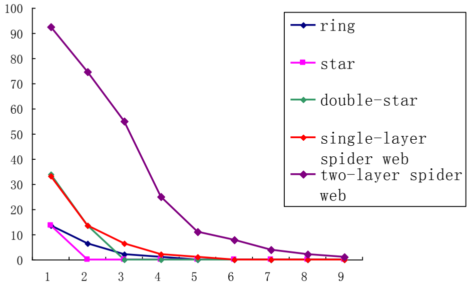


Figure.3: the variation of different topologies.

4. The Power Spider Web Traffic Algorithm Based on MPLS

A. The Power Communication Model Based on the Artificial Spider Web Structure

Combining MPLS with the spider web, considering actual smart grid communication situation, we build the power communication model based on the artificial spider web structure shown in the Figure.4.

The access router of the major nodes is defined as LER. Its function is to complete IP packet grouping and add labels[4]. The router of the province backbone network is defined as LSR. It will complete forward and switch according to the label routing table.

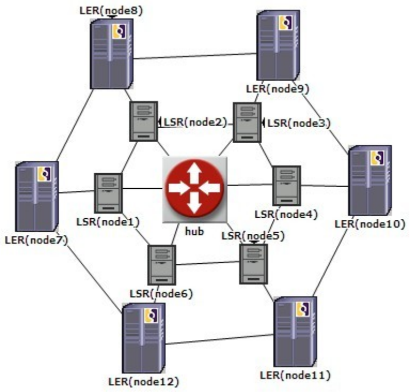
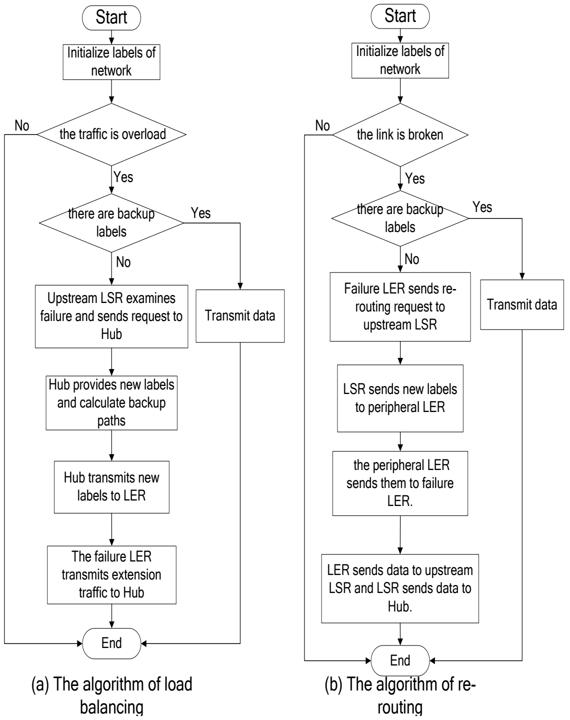


Figure.4: the power communication model based on artificial spider web structure

In order to verify the effectiveness and real-time performance, this paper builds an actual power communication model by OPNET. In Figure 4, every LER and LSR composes the MPLS area with artificial spider web structure. Each LSR is defined as backbone switch connecting relative LER, LSR and the center router. LSR is defined as an upstream node of relative LER to examine whether the major nodes are broken down[5,6]. Even certain major node are broken down, the relative LER can create a backup path to transfer the traffic to the backup path.

B. The Spider Web Traffic Algorithm based on MPLS

In the components of MPLS Traffic-Engineering, load balancing and re-routing are two most important aspects[7]. The network resource can be optimized by using MPLS load balancing strategy. Also, if there is link or node failure in the network, the traffic can be transferred in the backup path by using re-routing strategy. The flowchart of the algorithm on load balancing and re-routing are shown in the Figure 5.


Start
Initialize labels of network
the traffic is overload
No
Yes
there are backup labels
Yes
No
Upstream LSR examines failure and sends request to Hub
Transmit data
Hub provides new labels and calculate backup paths
Hub transmits new labels to LER
The failure LER transmits extension traffic to Hub
End
Start
Initialize labels of network
the link is broken
No
Yes
there are backup labels
Yes
No
Failure LER sends re-routing request to upstream LSR
Transmit data
LSR sends new labels to peripheral LER
the peripheral LER sends them to failure LER.
LER sends data to upstream LSR and LSR sends data to Hub.
End

(a) The algorithm of load balancing

(b) The algorithm of re-routing

Figure.5: The flowchart of the algorithm on load balancing and re-routing

C. The Simulation Analysis

1) The Simulation Assumptions: According to the model created in the section 4.1 and actual stratification of power communication network, we set that the width of each link is 9.6kbps and the size of model is 20km×20km.In the light of actual communication situation, we set the traffic threshold of backbone layer with 16000bps higher than the one of access layer with 8000bps[8].At the beginning of the simulation, there is no failure nodes or links in the network.

2) The SimulationProcess: The total simulation time is set as 2500s.At the time of 500s, traffic between node1 and node 7 is more than the link's threshold. At the time of 1000s, the link between node1 and node 7 is broken down. The simulation model is shown in the Figure.4 to verify the communication performance of the two-layer spider web.

In the Figure.6(a), the blue curve represents the traffic from node7 to node1, the red curve represents the traffic from node7 to node8 and the green traffic represents the traffic from node7 to node12. Within 500s, the traffic through node7 is 8000bps without exceeding its threshold. In the Figure.6(b),the traffic from node7 to node1 remains 8000bps without losing packets. However, from 500s to 1000s, the traffic from node7 to node1 increases to 16000bps abruptly with exceeding its threshold. As the upstream node of node7, node1 examines failure and sends load-balancing request to Hub. Hub will distribute new labels for newly added data groups and send new labels to node7 through the original path. When node7 receives new labels, it will switch new traffic to LER(node 8,node12) according the path assigned by the labels. In the Figure.6(a), from 500s to 1000s, the traffic from node7 to node1 doesn't change. On the other hand, the traffic from node 7 to node 8 and node 7 to node12 is respectively distributed 3200bps and 4800bps.In this period, traffic of each link doesn't exceed its threshold so there is no packet loss.

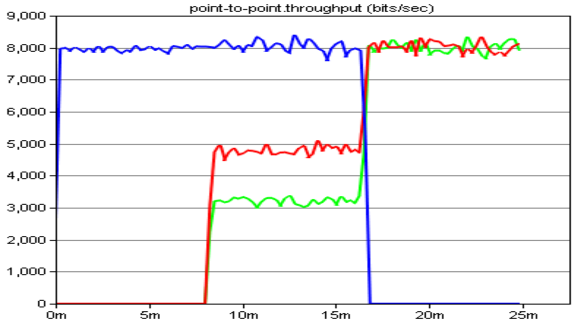


Figure.6 (a) The variation of traffic

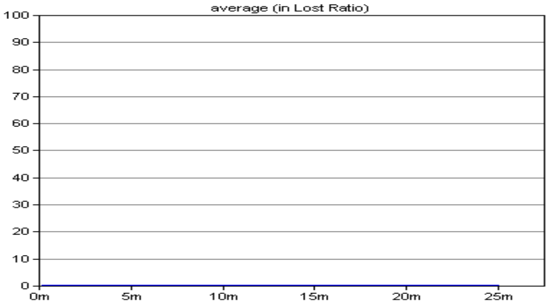


Figure.6 (b) The variation of packet loss

Figure.6: The simulation results of MPLS algorithm

From 1000s to 1500s, the link between node1 and node7 is broken down. As the upstream node of node7, node1 examines failure and sends new labels to LER(node 8,node12) through node2 and node6. Node7 switches traffic to node8 and node12 according to the new labels. In the Figure.6(a), we can see that traffic of node7→node8 and node7→node12 increases to 8000bps respectively and the function of re-routing is realized. In this period, traffic of each link doesn't exceed its threshold so there is no packet loss.

From the simulation results, we can see the spider web traffic algorithm based on MPLS can realize load balancing and re-routing and can be used in power communication.

5. Conclusion

Aiming at node's failure, traffic overload and data congestion in the smart grid communication network, this paper proposes the artificial spider web topology with high reliability. By calculating the degree of invulnerability, it can be proved that the invulnerability of artificial spider web is higher than other topologies. When major nodes in the communication network are broken down, the network remains high connectivity. Based on two-layer spider web topology, this paper proposes the power spider web traffic algorithm based on MPLS together with the OPNET simulation of load balancing and re-routing. From the simulation results, the algorithm can realize load balancing and re-routing which can be used between major nodes to improve the real-time performance of communication.

6. Acknowledgment

This paper was sponsored by National Natural Science Foundation of China (51277042).

7. References

[1] YU Yi-xin and Luan Wen-peng, "Summary of smart grid," Proceedings of the CSEE, 2009,(34).

[2] YU Nan-hua and CHEN Yun-rui, "Communication technology", Beijing, China Electric Power Press, 2012, 1-4.

[3] LIN Jian-wei, "Research on Artificial Spider Web Routing Algorithms oriented smart gird", Harbin Institute of Technology, 2011.

[4] LIU Xiao-sheng, ZHAO Zhen-feng, ZHANG Peng-yu and REN Hui-fen, "Study on reliability of a novel Electric Power Data Network for smart grid," Power Electronics and Motion Control Conference (IPEMC), 2012 7th International , vol.3, no., pp.2305-2310, 2-5 June 2012.

[5] NA Lin, TAO Yang and LI Xue-song, "A New QoS Multicast Routing Algorithm for MPLS-TE," Measuring Technology and Mechatronics Automation (ICMTMA), 2010 International Conference, vol.1, no., pp.192-195, 13-14 March 2010.

[6] TRAN Cong-hung, Nguyen Hoang-thanh, Nguyen Duc-thang, HAE Won-jung, Tae Kim, Sung Hei-kim and Woo Jin-yang, "Advanced Routing Algorithms and Load Balancing on MPLS," Advanced Communication Technology, The 9th International Conference , vol.3, no., pp.1886-1891, 12-14 Feb. 2007.

[7] Inoue, S., Ueno, N., Amamiya, M. and Kakuda, Y., "Multianent-based path rerouting method in MPLS," Autonomous Decentralized Systems, 2005. ISADS 2005. Proceedings, vol., pp.562-656, 4-8 April 2005.

[8] Tong Xiaoyang, Liao Chensong, Zhou Lilong, etal. The simulation of substation communication network based on IEC61850-9-2 [J]. *Automation of Electric Power Systems*, 2010, 34(2): 69-74.