Warship Power System Survivability Evaluation Based on Complex Network Theory

Huiying He[1,a], Hongjiang Li[1], Shaochang Chen[1] and Hao Xiong[1,2,b]

[1]Naval University of Engineering, Wuhan, 430033, China

[2]Huazhong University of Science and Technology, Wuhan, 430074, China

[a]yinger5316@qq.com, [b]howell76@sina.com

Keywords: Survivability evaluation, Warship, Power system, Complex network theory

Abstract. This paper analyzes the characteristics of warship power network based on complex network theory, obtains the commonly statistical properties of the ship power system, applies them to the research for survivability of warship power system, concludes that a ship power grid has the characteristics of scale-free networks and it has strong robustness to random attacks but poor to deliberate attacks, and suggests that the it reduce the nodes with higher “degree” in a warship power network during ship power network design to improve and optimize the performance of the network.

Introduction

A warship power network is divided into the basic network and the distribution network. The characteristics of the basic network are that the basic network generally employs the ring network, the electric energy always flows from a generator to a main switchboard between, and the state changes of the switches between the generators and the main switchboards make the connection relationship uncertain so that it is uncertain for the flow direction of the current and power between the main distribution boards. The characteristics of the distribution network are that the distribution network generally adopts the main and feeder lines hybrid distribution network, the current always flows from an upper layer distribution board to a lower one, the distribution network has the "tree" type hierarchy, and an important distribution board is supplied by the dual power supply and the dual power switches are not closed simultaneously [1]. Hence a typical warship power network structure model is established as follows, shown in Fig. 1.

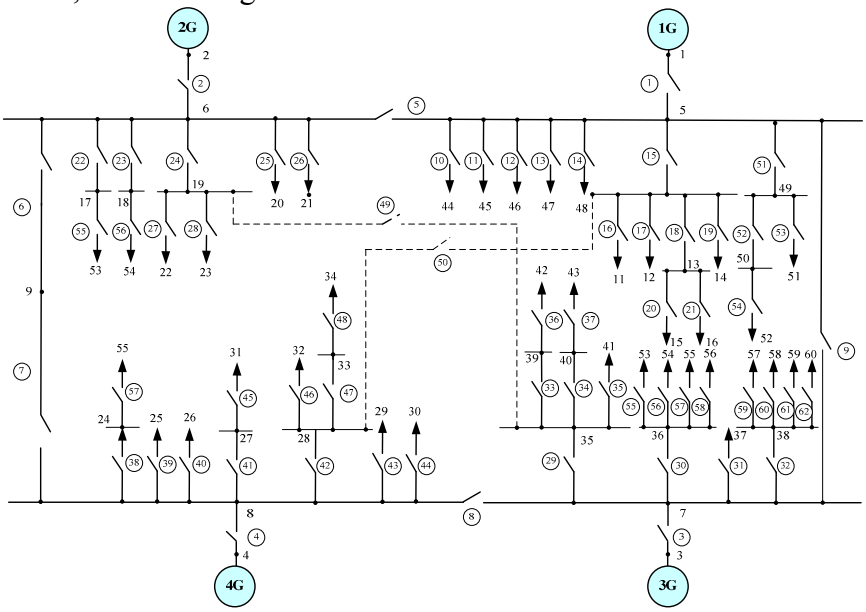
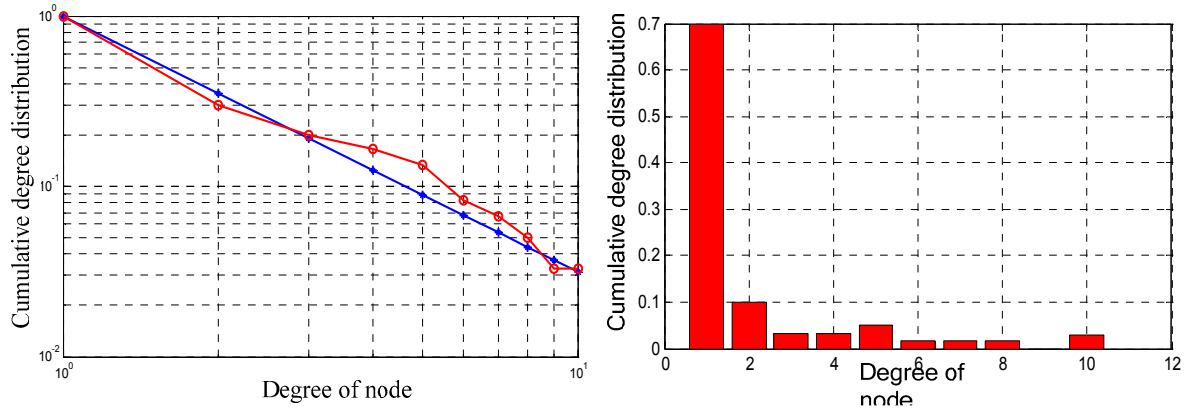


Fig.1 Network model of a warship power system

Topology Parameter Analysis of Shipboard Power Network Model Features

Degree. The degree of a node is defined as the number of the other nodes connected to the node. The average value of the degrees of all nodes in the network is called the average degree of the network, and denoted by $< k >$. The distribution function $p(k)$ represents a probability that the degree of a randomly chosen node is exactly k. The cumulative degree distribution function $P_k = \sum_{k'=k}^{\infty} p(k')$ represents the probability distribution of the nodes whose degrees are not less than k [2]. Based on the power network model in Fig. 1, the power network includes 60 nodes and 62 edges. The average value of the degrees of all nodes $< k >= 2.07$, and the power law function is $y = k^{-1.5}$. In the log-log coordinate system the cumulative degree distribution curve is plotted in Fig. 2. In Fig. 2, it is plotted by "o" mark for the cumulative degree distribution curve of the ship power network model and "*" mark for the power law function curve.



(a) Cumulative degree distribution curve of node (b) bar chart of node degree distribution

Fig. 2 Cumulative degree distribution curve of node and bar chart of node degree distribution

Fig. 2 (a) shows that the degree distribution of the model possesses the characteristics of a scale-free network while Fig. 2 (a) indicates that the ship power network model has the following characteristics: it has some nodes with higher "degree" value; most of the nodes have far lower "degree" value, which proves a shipboard power network is a non-uniform network with the characteristics of a scale-free network.

Average Path Length. Distance d_{ij} between two nodes i and j in the network is defined as the number of edges on the shortest path connecting these two nodes. The average path length L of the network is defined as the average value of the distance between any two nodes [3], i.e. $L = \frac{1}{\frac{1}{2}N(N+1)} \sum_{i \geq j} d_{ij}$. Herein N is the number of nodes in the network [2]. This paper uses Dijkstra algorithm to calculate the average path length of the model and the average path length of the ship power network model is obtained L = 3.57, which shows the model network having a smaller average path length.

Betweenness. Betweenness is divided into the node and edge betweenness. A node betweenness is a proportion of the shortest path through the node versus all shortest path in the network. The definition of an edge betweenness is similar. Betweenness reflects the role and influence of a node or an edge in the network. In a power system, the line betweenness is the number of the shortest paths between all the generators and loads in the network passing the line. The cumulative betweenness distribution of the ship network model shown in Fig. 1 is calculated and plotted in a log-log coordinate system as shown in Fig. 3. Therein, it is plotted by "o" mark for the cumulative betweenness distribution fitting curve of the model and "*" mark for the power law function curve: $y = k^{-1.1}$. It is obvious from Fig. 3 that the cumulative betweenness distribution of the model has a trend of an approximate power law function, which proves that the betweenness distribution of

the model possesses the characteristics of a scale-free network: (1) it has some nodes with higher "betweenness" value; (2) most of the nodes have far lower "betweenness" value.

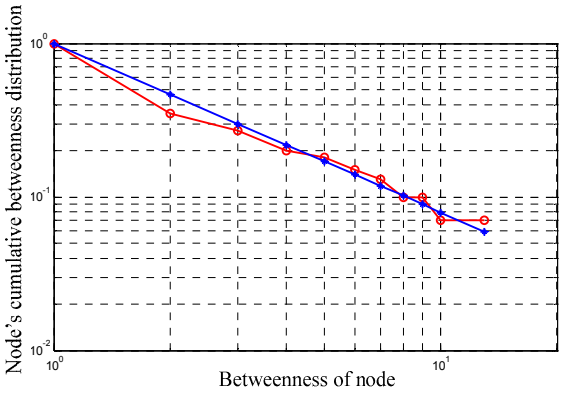


Fig. 3 Node's cumulative betweenness distribution of warship power network

Survivability Evaluation of Warship Power System Based on Complex Network Theory

Evaluation Method. Survivability of a warship power system refers to the ability of the power system to supply the ship after it has gone through the attack or accident. So the survivability index of a warship power system refers to the power supply range and energy which a power system can provide after attack [4] & [5]. This paper adopts the percentage of the load nodes that can be connected to the power supplies after attack.

$$PS = \frac{E}{N} \times 100\% = \frac{\sum_{i=1}^{m} E_i}{N} \times 100\% \tag{1}$$

Where N is the total number of nodes in the grid, m is the number of supply area, and E is the number of nodes that can be connected to the power sources.

Survivability evaluation follows the below steps:

(1) Determine the attack mode.

(2) Calculate the survivability index of a warship power system, depending on the attack mode.

(3) Analyze the impact of the ship power system statistical characteristics on the survivability index.

Attack Mode. Attack mode is classified into two categories: (a) random attack and (b) deliberate attack, according to whether the attack considers the statistical characteristics of the nodes [6]. Random attack determines the attacked node number based on the random number generated by a random function. However, deliberate attack sorts the nodes based on the statistical characteristics of the selected grid nodes and attacks them in turn. It is assumed that the edges connected to a node are broken when the node is under attack.

Comparison of Survivability Index in Different Attack Situations. Whether it is a random attack or a deliberate attack, the destruction on the basic network is to cause mainly the basic network to be disconnected while attack damage to the distribution network is to cause mainly a power failure of some distribution area node. The node - switch matrix method is used to calculate the impact of attack on the basic network

Survivability Evaluation under Random Attack. Ten random attacks hit a 60-node 62-branch ship power system, and it is calculated for the supply performance of the network after the attacks. Assuming that the bow and stern power stations of the basic network are in the parallel operation at the start and one more node is destroyed and its adjacent branches break down after each attack, the attacked node sequence and the power supply performance of the nodes after attack are calculated and listed in Table 1. It is evident from the table that a ring-form basic network is more attack-resistant. Branch 2, 9 and 3 in Table 1, the basic network branches, are disconnected respectively after attack 1, 2 and 4, but the power performance of the network is 100% after strike. The power supply performance of the network declines dramatically after the attacks have struck the

nodes with higher "degree" and "betweenness". The 5th and 8th attacks have randomly hit the nodes with higher "degree" and "betweenness", which causes a sharp decline of power supply performance. There is no effect on the power supply performance when the nodes with degree of 1, i.e. the load nodes, are struck. Moreover, for a small 60-node 62-branch network, the attacked nodes are 16.7% of all and the power-loss percentage of the total nodes is 18.3% after 10 random attacks. Hence the power system has a stronger anti-attack capability against the random attack.

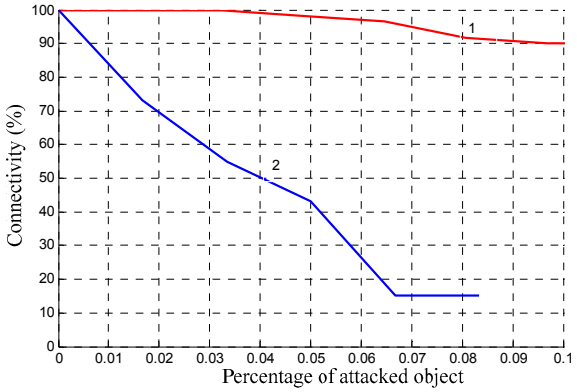
Table 1 Power supply performance after random attack

Attack sequence	Node number	Degree of node	Betweenness of node	Node Property	Power supply performance (%)
1	2	1	13	Power supply	100
2	9	2	1	Power supply	100
3	30	1	1	Load	100
4	3	1	13	Power supply	100
5	10	6	6	Distribution	90
6	43	1	1	Load	90
7	59	1	1	Load	90
8	35	5	4	Distribution	81.7
9	30	1	1	Load	81.7
10	21	1	1	Load	81.7

Survivability Evaluation under Deliberate Attack. A deliberate attack strikes the nodes in sequence: first attack the node with the largest "degree" and "betweenness", and second strike the node with second one and so on. The power supply performance of the nodes after five attacks are calculated and listed in Table 2. The attacks on the nodes with higher "degree" and "betweenness" lead to a sharp drop of the power supply performance, which proves the power network is vulnerable to a deliberate attack. For the small network, the attacked nodes are 8.3% of all but the power-loss percentage of the total nodes is 85% after 5 deliberate attacks. Hence the power system is far less attack-resistant against the deliberate attack.

Table 2 Power supply performance after deliberate attack

Attack sequence	Node number	Degree of node	Betweenness of node	Node Property	Power supply performance (%)
1	5	10	13	Power supply	73.3
2	8	10	9	Power supply	55
3	6	8	7	Power supply	43.3
4	7	7	13	Power supply	15
5	35	6	6	Distribution	15



1 - Power supply performance after random attack
2 - Power supply performance after deliberate attack
Fig.4 Comparison of power supply performance after random attack and deliberate attack

Conclusions

The nodes are often associated with a number of branches so attacks on the nodes are more dangerous. Furthermore, the nodes with higher "degree" and "betweenness", most in the basic network, are the important nodes in the network and the attacks on them will cause a greater damage on the warship power system. A ship power network is more robust to random attacks but less to deliberate attacks.

References

[1] H. Lin: The Research for Survivability of Warship Power System (Harbin Engineering University Press, China 2009), In Chinese.

[2] X. Li, X. Li and G. Chen: Complex Network Theory and Application (Tsinghua University Press, China 2009), In Chinese.

[3] H. Zhang and F. Lu: Proceedings of the CSEE Vol. 34 (2014), p. 613-619, In Chinese.

[4] H. Li, Z. Lu and L. Zhu: Journal of Wuhan University of Technology Vol. 31 (2007), p. 533-536, In Chinese.

[5] T. Jin, B. Luo and X. Chen: Journal of Naval University of Engineering Vol. 18 (2006), p. 37-41, In Chinese.

[6] Z. Lu, Z. Meng and S. Zhou: Proceedings of the 8th International Conference on Probabilistic Methods Applied to Power Systems (2004), p. 635-640.2004.