Robust Analysis of Grid System Based on Complex Network Attack Mode

Jun Xiang[1](✉), Jiao Zhu[1], Shuyang Guo[1], Yue Chen[2], and Zhizhong Qiao[3]

[1] Hainan Power Grid Co., Ltd., Hainan 570203, China
xiangj@hn.csg.cn
[2] Nari Technology Development Co., Ltd., Nanjing 210033, China
[3] NARI Information and Communication Technology Co., Ltd.,
Nanjing 210033, China

Abstract. With the continuous construction of the grid, its scale is getting larger and larger and the degree of connection is becoming more and more complicated, which means the structure of the grid gradually meets the characteristics of complex networks. Through the modeling of the structure of the grid system and the analysis of complex network theory, different attack modes (i.e., attack strategy of degree node, immediate node, and random node) in the complex network are proposed which are utilized to do the robust analysis of grid system. The IEEE-57 and IEEE-300 node systems are chosen for simulation verification. Based on the results, the connectivity of the system presents different results in different attack modes. Among them, the random attack has the least impact on the system, while the median attack is the most serious. This also corresponds to the definition of the mediator.

Keywords: Robust analysis · Complex network attack mode · Grid system · Simulation verification

1 Introduction

At the end of the 20th century, Watts and Strogatz of Cornell University in the United States published "Collective Dynamics of Small-World' Networks" [1], and the small world network model was first presented to people. There has been a wave of research on complex networks around the world. In 2013, Pagani and Aiello published "The power grid as a complex network: A survey" in "Physica A" [2], which explained that generators and transmission lines can be abstracted into nodes and edges in the network in the power grid. To model, you can use the theory of complex networks to study power networks. So far, researchers in the field of power systems have begun to analyze power systems from the perspective of complex networks [3–6]. Applying the complex network theory, combined with the actuality of the power system, the initial load of the node is defined by the electrical interface, and the cascading failure model is established. The normalized fault scale, average connectivity level and weighted network

X. Sun et al. (Eds.): ICAIS 2019, LNCS 11635, pp. 167–177, 2019.
https://doi.org/10.1007/978-3-030-24268-8_16

efficiency are used to evaluate the evolution of the small world power grid. The change in robustness. The analysis results show that with the increase of network capacity, the robustness of the small world power grid is enhanced, but when the network capacity reaches a certain value, the increased capacity has little impact on the robustness of the small world power grid [7]; with the development of the small world power grid Evolution, the connection between nodes is enhanced, and its overall robustness is also enhanced. Therefore, when planning and designing the power system, the capacity of the power grid should be scientifically and reasonably determined according to the actual situation. It is also possible to refer to the development and evolution mode of the small world power grid to obtain a power grid with strong robustness and low cost. Network robustness refers to the ability of a network to maintain its operation after a node or edge in the network fails due to external interference.

Complex networks are an important method for studying complex systems. The network view of complex systems research has become a new perspective accepted by researchers [8,9]. Compared with other research methods, complex network theory emphasizes the topological characteristics of the system, can properly reflect the dynamic formation process of the network, and reveal some macroscopic properties of the system. These have the robustness and anti-risk ability for analyzing complex networks. Important reference value. Robustness is generally considered to be the robustness of complex systems, and is the key to the survival, maintenance, and continuous service of complex networks in abnormal and dangerous situations. Albert and Barabasi compared the connectivity of ER random graphs and BA scale-free networks to the robustness of node removal in [10].

Two kinds of node removal strategies are studied. One is the random failure strategy, which completely removes some nodes in the network randomly. The second is the deliberate attack strategy, that is, from the removal of the most moderate node in the network, the consciously removes the highest degree in the network. Node. It is the non-uniformity that makes the scale-free network highly vulnerable to deliberate attacks: as long as the consciously removing the nodes with the largest number of values in the network will have a great impact on the connectivity of the entire network [11]. Scientists in different fields have explored this problem and found that robust but fragile is one of the most important and basic features of complex systems [12]. Broder et al. studied the robustness of large-scale WWW sub-networks. Sexual discovery only removes all nodes with degrees greater than 5 to completely destroy the connectivity of the WWW [13]. These studies are qualitative in terms of robustness, and the study of the impact of complex network structures on robustness is not sufficient. Based on the classical node admittance matrix model, this paper classifies nodes, simplifies calculations, and proposes three different attack strategies from the perspective of complex networks. Using static analysis methods, the structural structure is robust from the perspective of grid system. The influence of sex is finally verified by using IEEE-57 system and IEEE-300 system as examples.

The remaining parts of the paper are organized as follows: In Sect. 2, some preliminaries (i.e., the complex network and robustness index of grid system) are introduced. And in Sect. 3, Robust analysis of grid system based on different attack modes (i.e., attack strategy of degree node, immediate node and random node) in complex network is detailedly introduced, which consists of there parts: attack mode, attack simulation process and experiment results. Finally, Sect. 4 is dedicated for conclusion and discussion.

2 Preliminary

2.1 Complex Network and Its Spread and Influence

With the continuous construction of the power grid, the scale of the power grid is getting larger and larger, and the degree of connection is more and more complicated [14]. In recent years, more and more scholars have applied complex network theory to power systems, so that the structure of the power grid gradually meets the characteristics of complex networks and solves a variety of problems. The characteristics of complex networks are often hidden in their statistical properties, and many concepts have been proposed for their statistical properties [15–18]. Because of its many concepts, only three basic concepts used in this article are introduced.

(1) Shortest path length
In the network, the shortest path length $l_{i,j}$ is defined as the number of edges on the shortest path between any two points i and j.

(2) Degrees
In the network, the degree k_i of node i is defined as the number of edges connected to the node. So intuitively, if the degree of a node is greater, then the node is more important in a sense.

(3) Intermediation
In the network, some nodes are not very large, but this node may play a role as a bridge between the two parts of the network, indicating that this node is also very important, so it is defined in all nodes of the network, The number B_i of the shortest path through all the nodes i is the mediator of node i.

Based on the propagation process of the d-dimensional small world network described by the NW network model, Moukarzel studied the propagation equation of the d-dimensional small world network more specifically [19]. The idea is to start from the initial infected node of the network, (1) the virus starts to propagate at constant speed 1; (2) the density of the long-range connection endpoint in the network is ρ; (3) the propagation process is continuous; The probability of encountering a long-range endpoint at the source endpoint is ρ. Then, the average total infection amount $V(t)$ is obtained by the following form and integral equation [20]:

$$V(t) = \Gamma_d \int_0^1 \tau^{d-1} [1 + 2pV(t-\tau)] d\tau \tag{1}$$

After scaling and differentiation, a linear propagation equation of the following form can be obtained [20].

$$\frac{\partial^d V(t)}{\partial t^d} = 1 + V(t) \tag{2}$$

Considering the influence of various nonlinear obstacles in the process of propagation, then, the average total infection amount $V(t)$ is obtained by the following form and integral equation [21]:

$$V(t) = \Gamma_d \int_0^1 \tau^{d-1} \left[1 + \xi^{-d} V(t-\tau) - \mu V^2 (t-\tau)\right] d\tau \tag{3}$$

After the above formula is scaled and differentiated, the following nonlinear equation can be obtained [21]:

$$\frac{\partial^d V(t)}{\partial t^d} = \xi^d + V(t) - \mu \xi^d V^2 (t) \tag{4}$$

Where ξ is the NW length scale and μ is the interaction coefficient. When considering a one-dimensional case, it is inversely proportional to the degree of complexity in a complex network [22], i.e., $\xi \sim 1/k$. The above formula is the expression of the total amount of network propagation $V(t)$ in the small world. In the case of the unbalanced system, the parameters will fluctuate. The physical meaning of such fluctuations is the errors, faults, etc. of complex network nodes and connected edges.

2.2 Robustness Index of Grid System

Robustness refers to the ability of the system to maintain its original performance when the structure or size changes occur in the system [23]. The structural robustness of the grid can be considered as the ability of the grid system to maintain its original power supply function after the structure of the grid changes.

The robustness of complex networks is the key to the survival, maintenance, and continuous service of complex networks in the event of node parameter failure (fluctuations) [24]. A more rigorous definition refers to the characteristics of the control system that maintains relevant performance under certain parameters (such as system structure, size, etc.) [25]. In a complex network, if most nodes in the network are still connected after removing a small number of nodes, then the connectivity of the network is said to be robust to node failures [26].

Artificial giant systems such as power networks and communication networks are increasingly dependent on the daily production and life of human beings. A serious problem is faced: How reliable are these networks? In fact, although hundreds of routers fail on the network every moment, the Internet is rarely affected. The performance of the life system is more robust: although there are thousands of errors in the cells, such as mutations and protein errors, there are very few serious consequences in life, and the source of this toughness mainly comes from within the system. In the network parameters with random fluctuations, there are factors in the system that cause the network structure to abruptly change, and there are also factors (damping) that make the system gradually stabilize before the network disaster.

For real networks, whether it is artificial giant systems such as Internet, telecommunication networks, power networks, large-scale circuits, or natural networks such as various metabolic networks, food chain networks, etc., are open, unbalanced, nonlinear and complex. The system is a typical object of non-balanced statistical physics research. It is in this case that a non-equilibrium network is proposed in correspondence with an equilibrium network. The number of nodes in the system described by the unbalanced network and the connected edges of the nodes are not fixed, but grow with time. The unbalanced complex network model can be constructed in the following ways: (1) the number of network nodes and the connected edges of nodes grow continuously with time; (2) the growth of network nodes and connected edges is in a fixed way: such as connection Preference, etc. [27]; (3) The internal and external network systems have the exchange of basic physical quantities and information; (4) There are fluctuations between nodes and even edges. Compared with the actual network system, the resulting unbalanced complex network model is a better model for describing the real network.

The nonlinear open system described by this unbalanced complex network model differs from traditional statistical methods in that it: (1) treat events occurring in the system as random events; (2) treat the processes occurring as random processes (3) Add some uncertainty directly into the dynamic equations describing the system. This method of studying the statistical properties of a large number of events, directly from the probability characteristics of random events and stochastic processes, is commonly referred to as Stochastic approaches [28].

Therefore, according to the particularity of the grid system, the following two indicators of the robustness of the grid system are defined.

(1) Grid node removal ratio
The grid node removal ratio is defined as: in the grid, the ratio of the number of nodes removed by the grid system to the number of nodes in the grid is:

$$PN = \frac{n_b}{N}, \tag{5}$$

here, N is the total number of nodes in the grid; n_b is the number of grid structures removed due to failure.

(2) Maximum connectivity of the grid system
Maximum connectivity of a power grid system After a fault occurs in a grid, due to the withdrawal of certain components, a connected network may be split into several isolated networks that are connected by itself. Then the maximum connectivity of the grid system is defined as the maximum

connectivity after the fault. The ratio of the number of nodes in the subset to the total number of nodes in the grid:

$$S = \frac{n_r}{N}, \tag{6}$$

here, N is all nodes of the entire network; n_r is the number of nodes in the largest connected subset after the failure.

3 Robust Analysis of Grid System Based on Attack Modes in Complex Network

In the actual power grid, the topology of the original power grid will be changed more or less due to faults and the like. This includes the initial point of failure and the exit of the cascading failure node due to the initial point of failure. This paper focuses on the number of components removed and the impact of the strategy on the robustness of the grid system, i.e., static analysis, without considering the cascading failure response caused by grid nodes or tidal current distribution after removal.

3.1 Attack Mode

In a complex network, the component removal method of the network can be divided into deliberate removal and random removal according to the way it is removed. Removing these nodes does not have a major impact on the connectivity of the entire network. However, it is this non-uniformity that makes scale-free networks highly vulnerable to deliberate attacks: consciously removing the nodes with the fewest values in the network can have a significant impact on the connectivity of the entire network. In the power network studied in this paper, the attack objects of the deliberate and random attacks that simulate the fault are nodes or edges. According to the particularity of the power grid system, the following three attack modes are formulated:

(1) Attack strategy of degree node (degree attack): firstly remove the maximum degree node in the network, then calculate the degree of each node in the new network, and then remove the node, and repeat until the set grid node removal ratio is satisfied.
(2) Attack strategy of intermediate node (median attack): first remove the maximum number of network mediation nodes, then calculate the number of nodes in the new network, and then remove the node, and repeat until the set grid node is removed ratio.
(3) Attack strategy of random node (random attack): randomly remove the number of nodes whose number of grid node removal ratios are set. Due to the contingency of random attacks, repeat the test for 20 times.

3.2 Attack Simulation Process

The robustness analysis of grid system based on static analysis method only considers the influence of grid topology on its own robustness, and does not consider the redistribution of power flow and its chain reaction caused by the removal of components in the grid. So we are studying the impact of different attack modes on the robustness of the grid system in the case of setting different grid node removal ratios. The specific process is as follows:

(1) Initialization: The network topology is generated based on the initial data, and the parameters such as the number and degree of each node of the network are calculated, and the grid node removal ratio of this test is determined.
(2) Node removal is performed according to the selected attack mode until the set value is satisfied.
(3) Generate the final network topology model, calculate the maximum connectivity of the grid system of the model and record the data.
(4) Repeat multiple times, record the maximum connectivity of the final topology under different set values and different attack modes, and plot the curve with the grid removal ratio setting. The flow chart is shown in Fig. 1.

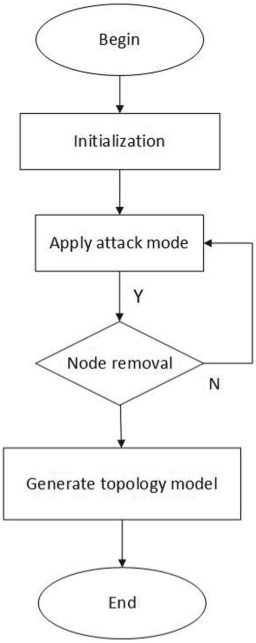

Fig. 1. Process about robust analysis of grid system based on complex network attack mode.

3.3 Experiment

According to the algorithm described above, the IEEE-57 node system and the IEEE-300 node system are selected for simulation verification.

(1) IEEE-300 node system

According to the attack method set in the previous method, the attack is performed in the maximum degree, the maximum number of media, and the random mode. The relationship between the maximum connectivity (S) of the grid system and the grid node removal ratio (PN) is shown in Table 1.

According to the above simulation results, it can be seen that in different attack modes, the connectivity of the system presents different results, in which the random attack has the least impact on the system, while the median attack presents the most serious, which is also the definition of the mediator. Compatible. After the degree attack is 15% set value, the drastic drop of connectivity indicates that when the system node is missing to a certain extent, the quantity changes to the qualitative change.

Table 1. IEEE-300 node system S results in different set PN values and different attack modes.

PN setting value (%)	S (degree attack)	S (median attack)	S (random attack)
0	1.0000	1.0000	1.0000
1	0.8983	0.9831	0.9831
3	0.8559	0.5678	0.9746
5	0.7966	0.3983	0.9407
7	0.6610	0.3051	0.9237
9	0.6356	0.2542	0.9237
11	0.5510	0.1520	0.9019
13	0.5018	0.1500	0.8937
15	0.5000	0.1451	0.8812
17	0.2819	0.1391	0.8647
19	0.2819	0.0951	0.8430

(2) IEEE-57 node system

According to the attack method set in the previous method, the attack is performed in the maximum degree, the maximum number of media, and the random mode. The relationship between the maximum connectivity (S) of the grid system and the grid node removal ratio (PN) is shown in Table 2.

It can be seen that the simulation results are similar to those of the IEEE-300 node system. In different attack modes, the random attack has the least impact

Table 2. IEEE-57 node system S results in different set PN values and different attack modes.

PN setting value (%)	S (degree attack)	S (median attack)	S (random attack)
0	1.0000	1.0000	1.0000
1	0.9845	0.9845	0.9845
3	0.8959	0.9678	0.9546
5	0.8866	0.9583	0.9307
7	0.8410	0.9451	0.9237
9	0.6356	0.9042	0.9137
11	0.5510	0.1520	0.9019
13	0.5018	0.1105	0.8967
15	0.5000	0.0999	0.8895
17	0.2819	0.0971	0.8548
19	0.2819	0.0953	0.8436

and the median attack has the greatest impact. In terms of system collapse, the IEEE-57 node has begun to cause serious system stagnation at the smaller PN setting than the IEEE-300 node, which indicates that the robustness of the system is also related to its own scale.

4 Conclusion

This paper classifies the nodes in the system through power network modeling, and uses the complex network related theory to analyze it statistically and obtain its statistical description index. Different attack models (i.e., attack strategy of degree node, immediate node and random node) based on complex network theory are developed for their networks, and the descriptive indicators of the robustness of the system structure are also defined. Finally, the IEEE-300 and IEEE-57 node systems are attacked according to different modes under different set values, and the conclusion that the system mediation number is larger is more important. At the same time, the conclusion that the system robustness is related to its scale is obtained. Because its complex network characteristics can be considered in future grid design to improve its robustness.

In the next work, we will study the influence parameters of complex network robustness based on complex network propagation and response and derive the interaction coefficients of complex networks, which can be used as a basic parameter to measure the robustness of complex networks.

References

1. Watts, D.J., Strogatz, S.H.: Collective dynamics of small-world networks. Nature **393**, 440–442 (1998)
2. Pagani, G.A., Aiello, M.: The power gridas a complex network: a survey. Phys. A Stat. Mech. Appl. **392**(11), 2688–2700 (2013)
3. Zhang, X., Tse, C.K.: Assessment of robustness of power systems from the perspective of complex networks. In: IEEE International Symposium on Circuits and Systems, pp. 2684–2687 (2015)
4. Zeng, A., Shen, Z., Zhou, J., et al.: The science of science: from the perspective of complex systems. Phys. Rep. **714**, 714–715 (2017)
5. Chen, Z., Wu, J., Xia, Y., et al.: Robustness of interdependent power grids and communication networks: a complex network perspective. IEEE Trans. Circ. Syst. II Express Briefs **65**, 115–119 (2017)
6. Liang, M., Liu, F., Gao, C., et al.: Robustness analysis of the complex network. In: Data Driven Control and Learning Systems, pp. 638–643 (2017)
7. Bhatu, B., Shah, H.Y.: Customized approach to increase capacity and robustness in image steganography. In: International Conference on Inventive Computation Technologies, pp. 1–6 (2017)
8. Nardelli, P.H.J., Cardieri Jr., P., Kretzschmar, W.A., Latva-Aho, K., et al.: Interference networks: a complex system view. Eprint arxiv (2013)
9. Ivanov, I.V.: Epistemology of computational biology and modeling of complex heterogeneous systems (2015)
10. Albert, R., Jeong, H., Barabasi, A.L.: The diameter of the world wide web. Nature **401**(6), 130–131 (1999)
11. Joo, W., Kwak, S., Youm, Y., et al.: Brain functional connectivity difference in the complete network of an entire village: the role of social network size and embeddedness. Sci. Rep. **7**(1), 4465 (2017)
12. Grindrod, P., Stoyanov, Z.V., Smith, G.M., et al.: Primary evolving networks and the comparative analysis of robust and fragile structures. J. Complex Netw. **2**(1), 60–73 (2018)
13. Wang, H., Ding, X., Huang, C., et al.: Adaptive connectivity restoration from node failure(s) in wireless sensor networks. Sensors **16**(10), 1487 (2016)
14. Xia, L.L., Song, B., Jing, Z.J., Song, Y.R., Zhang, L.: Dynamical interaction between information and disease spreading in populations of moving agents. CMC: Comput. Mater. Continua **57**(1), 123–144 (2018)
15. Yao, J., Xiao, P., Zhang, Y., et al.: A mathematical model of algal blooms based on the characteristics of complex networks theory. Ecol. Model. **222**(20), 3727–3733 (2011)
16. Redelico, F.O., Proto, A.N.: Complex networks topology: the statistical self-similarity characteristics of the average overlapping index. In: Proto, A., Squillante, M., Kacprzyk, J. (eds.) Advanced Dynamic Modeling of Economic and Social Systems. SCI, vol. 448, pp. 163–174. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-32903-6_12
17. Lei, M., Xie, B.: Research on the characteristics of complex networks in area joint air defense command information system. In: WIT Transactions on Modelling & Simulation, pp. 593–600 (2014)
18. Jiang, Y.W.: Study on the characteristics of complex networks in network user behavior. J. China Acad. Electron. Inf. Technol. (2017)

19. Moukarzel, C.F.: Spreading and shortest paths in systems with sparse long-range connections. Phys. Rev. E Stat. Phys. Plasmas Fluids Related Interdisc. Top. **60**(6), R6263-6 (1999)
20. Yang, X.S.: Chaos in small-world networks. Phys. Rev. E Stat. Nonlinear Soft Matter Phys. **63**(2), 046206 (2001)
21. Yang, S.K., Chen, C.L., Yau, H.T.: Control of chaos in Lorenz system. Chaos Solitons Fractals **13**(4), 767–780 (2002)
22. Newman, M.E.J., Watts, D.J.: Scaling and percolation in the small-world network model. Phys. Rev. E **60**(6), 7332–7342 (1999)
23. Tanaka, G., Kai, M., Aihara, K.: Dynamical robustness in complex networks: the crucial role of low-degree nodes. Sci. Rep. **2**(1), 232 (2012)
24. Wang, Z.F., Yan, D.Q., Wang, R.D., Xiang, L., Wu, T.T.: Speech resampling detection based on inconsistency of band energy. CMC: Comput. Mater. Continua **56**(2), 247–259 (2018)
25. Abdi, N., Kitous, O., Grib, H., et al.: Evaluation of the robustness of the enzymatic hydrolysis in batch and continuous mode by a central composite design. J. Food Process. Preserv. **42**(1), e13330 (2017)
26. NetAnswer: Robustness of self-consolidating concrete. Materials & Structures
27. Newman, M.E.J.: The structure and function of complex networks. SIAM Rev. **45**(2), 167–256 (2003)
28. Guo, B.H., Cai, S.H., Zhu, J.Q.: Small world network bifurcation driven by non-equilibrium fluctuation. J. Sichuan Normal Univ. (Nat. Sci.) **31**(5), 631–634 (2008)