Appl. Sci. **2015**, *5*, 622-636; doi:10.3390/app5030622

OPEN ACCESS

applied sciences

ISSN 2076-3417

www.mdpi.com/journal/applsci

Article

Critical Nodes Identification of Power Systems Based on Controllability of Complex Networks

Yu-Shuai Li, Da-Zhong Ma, Hua-Guang Zhang and Qiu-Ye Sun *

Department of Electrical Engineering, Northeastern University, Shenyang 110819, China;
E-Mails: lysise@126.com (Y.-S.L.); madazhong@ise.neu.edu.cn (D.-Z.M.);
zhuanghuaguang@ise.neu.edu.cn (H.-G.Z.)

* Author to whom correspondence should be addressed; E-Mail: sunqiuye@ise.neu.edu.cn;
Tel.: +86-24-8368-3907; Fax: +86-24-8368-9605.

Academic Editors: Minho Shin and Takayoshi Kobayashi

Received: 18 July 2015 / Accepted: 14 September 2015 / Published: 22 September 2015

Abstract: This paper proposes a new method for assessing the vulnerability of power systems based on the controllability theories of complex networks. A novel controllability index is established, taking into consideration the full controllability of the power systems, for identifying critical nodes. The network controllability model is used to calculate the minimum number of driver nodes (N_D), which can solve the computable problems of the controllability of power systems. The proposed approach firstly applies the network controllability theories to research the power systems' vulnerability, which can not only effectively reveal the important nodes but also maintain full control of the power systems. Meanwhile, the method can also overcome the limitation of the hypothesis that the weight of each link or transmission line must be known compared with the existing literature. In addition, the power system is considered as a directed network and the power system model is also redefined. The proposed methodology is then used to identify critical nodes of the IEEE 118 and 300 bus system. The results show that the failure of the critical nodes can clearly increase N_D and lead a significant driver node shift. Thus, the rationality and validity are verified.

Keywords: controllability of networks; power systems; node identification; structural controllability; vulnerability

---

1. Introduction

Over the last decades, a number of power system blackouts caused by natural disasters or human factors have occurred, which led to a series of serious effects on the functionality and reliability of the networks, economic growth, and social stability [1,2]. The failure of a few critical nodes or lines can make the system very vulnerable to attacks, which may be the major reason causing the blackouts [3–6]. Thus, it is very important to identify the critical nodes and lines so that the system reliability and efficiency can be improved by monitoring and protecting them. In the past decades, studying the vulnerability of power systems has been a hot issue and many worthy results have been obtained [3]. Most of them assess the vulnerability of the power system by studying the system stability including transient [7], voltage [8,9], and frequency [10] stability, *etc*.

It is well recognized that the complex network theory is very suitable to solve large-scale practical problems. Based on the graph theory, the subject system can be studied from the point of view of structure and dynamical functions of an array of nodes and lines, in which the degree of dependence on the dimensionality of the system can be obviously reduced. Recent developments in this field have opened up a new way to power system research. In recent years, there has been an increasing interest in the study of assessing the vulnerability of the power system based on the complex network theory [3,11–18]. For example, [13] analyzed the structural vulnerability of the North American power grid and concluded that the nodes with high degree play an important role in power systems. Considering the influence of physical topological structure, the concept of betweenness is proposed to identify important nodes or lines in [14–17]. Additionally, a novel betweenness index was defined in [11], in which the reactance was defined as the weight of the lines. However, it is not necessary that the power only flows through the shortest path in a power system. Then, the idea of using the maximum flow theory to analyze the vulnerability of power systems was first proposed in [18]. Yu *et al.* have defined a centrality index to identify the critical lines in power systems with improved results in [3], which considered the maximum flow from the generator nodes to the load nodes based on the Ford-Fulkerson theorem. It should be noted that, although lots of worthy results have been obtained, there still exist some problems that were not well handled. Firstly, few of the existing literatures take the system's controllability into account. However, if the power systems cannot offer full control over the networks, when several important nodes are in fault, some serious phenomenon may occur, e.g., the phenomenon of voltage collapse, which has been well discussed in [19,20]. Secondly, in order to calculate the indexes such as the betweenness index [17] and the centrality index [3], weight of each link (transmission line) needs to be known. However, for most real networks, the weight of each link is either unknown or known only approximately and time-dependently. These problems are the main motivation of our study.

Network controllability is a vast area of research with a long history [21–28]. The structural controllability was first presented and studied in [26], which proved that a physical system is controllable if the system is structurally controllable. Furthermore, in [29], Liu *et al.* extended the results in [26] and proposed a network controllability model to solve the computable problems of the network controllability. It concluded that the minimum number of driver nodes can be calculated by the maximum matching method which was introduced in [30], and the structural controllability problem can be translated into an equivalent geometrical problem. Therefore, according the

aforementioned discussions, this paper proposed a novel method for assessing the vulnerability of a power system based on structural controllability and the network controllability model. The main contributions of the paper are as follows:

(1) Based on network controllability theories, a novel controllability index is established for assessing the vulnerability of power systems, which can effectively identify the critical nodes from the perspective of network controllability.

(2) In order to maintain full control of the power systems, the network controllability model is used to calculate the minimum number of driver nodes for solving this problem.

(3) The proposed method can overcome the limitation of the hypothesis that the weight of each link or transmission line must be known.

Meanwhile, the simulation results show good performances in identifying the critical nodes in the IEEE 118 and 300 bus systems. Furthermore, the effectiveness is validated.

This paper is organized as follows. In Section 1, the background and fundamentals of the research are discussed. In Section 2, some necessary controllability theories of complex networks are briefly introduced, and a directed power system is defined. In Section 3, the controllability index that used to identify the critical nodes is defined and the identification process is listed. In Section 4, the proposed methodology is applied to identify critical nodes on the IEEE118 and 300 bus systems. Additionally, it also discusses the performances of the system under random and targeted attacks. Lastly, we conclude the paper in Section 5.

2. Modeling Power Network Based on Controllability Theories of Complex Networks

In the following, the necessary concepts of the controllability of complex networks theory are presented. Then, the framework to solve the controllability of complex networks will be given. Finally, the network controllability theories will be appropriate for the power system and a directed power system will be defined based on the controllability theories of complex networks.

2.1. Basic Knowledge

(1) Structural Controllability: Lin's structural controllability theorem has been verified in [26], which indicated that a linear control system is structurally controllable if there are no inaccessible nodes and no dilation, or the system is spanned by cacti. What we focus on is that a physical system can be regarded as controllable if it has structural controllability [26,29]. In other words, the link weights are 1 or other non-zero values that do not affect the structural controllability of the system. Thus, structural controllability can overcome the disadvantage of incomplete weight information.

(2) Calculation of Driver Nodes: According to the minimum input theorem, the structural controllability problem can be translated into the maximum matching in its corresponding digraph. Let N_1 and N_D denote the minimum number of inputs and the minimum number of driver nodes, respectively. M^* is the number of matched nodes, and N is the total number of nodes. Then the minimum input theorem can be mathematically represented as follows [29]:

$$N_1 = N_D = \max\left\{N - \left|M^*\right|, 1\right\} \tag{1}$$

Moreover, the framework to solve the controllability of complex networks is shown in Figure 1. An uncontrollable system can be converted to controllability through adding inputs to the minimum number of driver nodes.

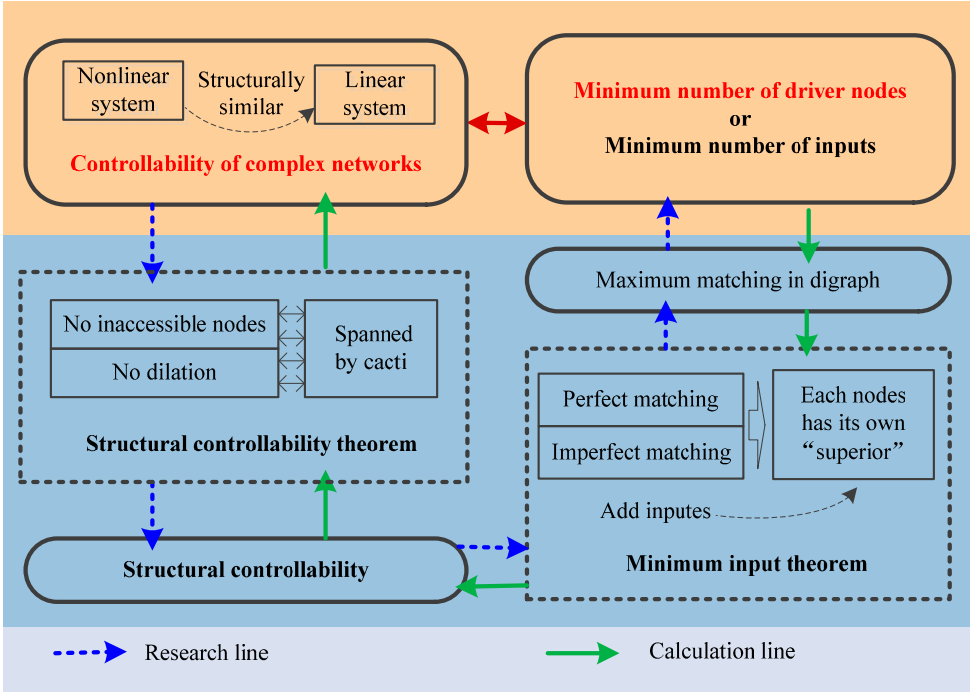


Figure 1. Framework to solve controllability.

2.2. Modeling Power System

According to graph theories, a network is composed with a set of nodes and edges. There are two types of networks containing undirected or directed networks. A network is defined as a directed network if all the connection edges are directed; otherwise, it is undirected. For any directed networks, the information, signal or energy can be transferred from one node to another node via the edges through the network. As far as power systems are connected, the edge weights are usually defined as the reactance so that the shortest path can be translated into the shortest electrical distance, and some other research also used the admittance, which is proportional to the amount of power flowing through any line of the transmission network. However, for most real networks, the weight of each link is either unknown or is known only approximately and time-dependently. According to structural controllability, a system is structurally controllable if it is possible to choose the non-zero weights. Thus, structural controllability supplies a method to overcome inherently incomplete weight information. If a system satisfies Lin's structural controllability theorem, the weights are 1 or non-zero values which do not affect the structural controllability of the system. Thus, in this paper, if there is a directed connection form node i to node j, then the value of e_{ji} is 1, which means the controllability of node i can be affected by node j.

A power system can be seen as a large complex network with a set of nodes and edges. Thus, the controllability just discussed can be appropriate for the power system. For any power system, the generators, loads, and bus bars are modeled as the nodes, and the connecting transmission lines are

modeled as the lines or edges. Based on the power flow in the network, the power system should be modeled as a directed network. Furthermore, according to the Kirchhoff laws, the node-voltage method is a good way to analyze a large power system and is used to calculate the current through the power system. The direction of the power flow can be seen as fixed in any steady state [3]. Therefore, suppose $G = (V,E)$ is a power system with n nodes and k lines where V is the set of nodes and E is the adjacency matrix which define the connectivity of the network. If there is a power flow from node i to node j, the value of e_{ji} is 1; otherwise, e_{ji} will be 0. Then, the obtained adjacency matrix can be used to calculate the controllability of the network.

3. Identification of Critical Nodes base on Controllability Theories of Complex Networks

3.1. Controllability Index

For a power system, let G be a directed network as defined in the previous section with N nodes. Based on the controllability of complex networks, the controllability index can be defined as follows:

$$\lambda_i = \left(N_i^D - N_{orig}^D\right) + \frac{\sum_{j\in\Omega}\left(N_j^D - N_{orig}^D\right)}{K_i} \tag{2}$$

where N^D_{orig} is the minimum number of driver nodes of the original network, N^D_i is the minimum number of driver nodes of the network after the node i is in fault, Ω is adjacency nodes of node i and K_i is the degree of node i, N^D_j is the minimum number of driver nodes of the network after the node j is in fault.

The physical significance of expression (2) is as follows: a node may be considered critical if when it is in fault there needs to be an increase in N_D to maintain full control of the power system, which can be quantified using $N^D_j - N^D_{orig}$. Furthermore, if the small numbers of nodes which are considered of importance in the system fault simultaneously, then it can create two serious problems. One is that the minimum number of driver nodes can rapidly increase, which means the power systems need to increase additional input signals to maintain full control of the power networks. The other one is that the driver nodes' distribution may be changed greatly, which means it leads to a significant driver nodes shift. Thus, the difficulty of fully controlling the power systems will be increased by these two aspects. They may lead to further failures and eventual cascades if the power systems cannot be readjusted in time. Although the power systems can be readjusted, it is very difficult to control the power systems as well. However, the importance of every node is not only related to itself, but also can be related to its adjacency nodes. For example, whether a node is a driver node can be changed if one of its adjacency nodes is in fault. In this paper, the mean value of $N^D_j - N^D_{orig}$ is used to quantify this idea. In addition, K_i can reflect the nodes' structural characteristics of the network.

Equation (2) can be normalized for its relative values by dividing the maximum values. Then the controllability index can be further defined as:

$$\overline{\lambda}_i = \frac{\lambda_i}{\max \lambda} \tag{3}$$

The nodes will be ranked with the controllability index after calculating Equation (3), and the nodes are regarded as critical if they have higher values of the controllability index.

Remark 1: It is well known that the state of power systems can be restricted into a certain range by certain control measures, if it is controllable. Therefore, when faults happen, if a power system is controllable, the state of the power system can be restricted into permitted range by adding external control inputs, so that the blackout risk can be effectively mitigated. Conversely, if a power system is uncontrollable, some serious problems may also happen, e.g., voltage collapse [19,20]. Therefore, whether the power system is controllable or not can have an important influence on the security of the power system. Furthermore, Lin's structural controllability theorem verified that a physical system is controllable if it is structurally controllable [26]. Thus, the concept of structural controllability analysis can also be used to define the security of the power system.

3.2. Identification Process

The controllability index is used to identify the critical nodes, and it is defined in the previous section. In this section, the identification process is shown in Figure 2.

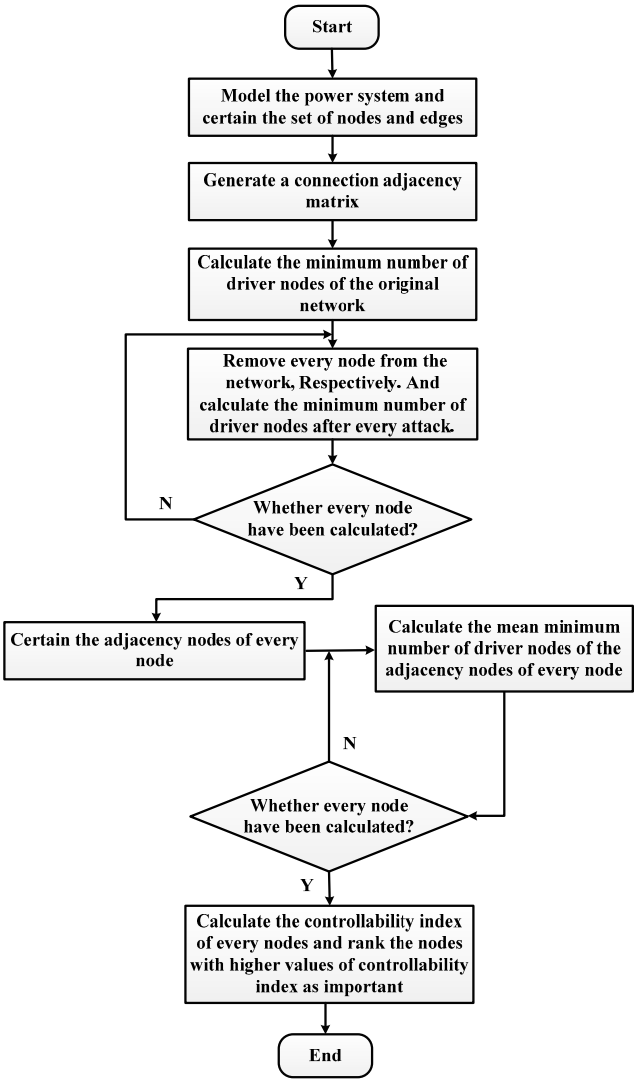


Figure 2. Identification process based on network controllability theory.

4. Simulation Study

In this section, several simulations under different scenarios have been studied to verify the effectiveness of the proposed method, in which the maximum matching and the identification algorithm are programmed through the M-function. The first case is used to show the identification results using the proposed controllability index without any fault or attack. The second and the third cases show the performance of the test system under targeted attacks and random attacks, respectively. In the first three cases, the IEEE 118 bus system as the test system is shown in Figure 3. Then, the proposed method is applied to a larger IEEE 300 bus system to further verify its effectiveness. In the last case, the comparison between the proposed method and some conventional method will be studied. In addition, all the simulation studies are under steady-state conditions.

In practice, there are many types of problems that can lead the power systems to be in fault (e.g., under-voltage, overload, *etc*.). However, in the theory framework of a complex network, when a fault happens to a node, it can be equivalently seen as an invalid node, meaning the node is disconnected from the network [3]. Therefore, in this paper, the nodes will be disconnected from the network if they are in any kind of fault. In addition, all faults in this paper can be considered as a result of the targeted attacks and random attacks, which are two typical types of attack in power systems. The targeted attacks mean that the few critical nodes with higher controllability index values are attacked to failure. On the contrary, random attacks mean that any of the less important nodes with low controllability index values are attacked to failure. During the simulations, a node will be in fault and disconnected from the network if it is subjected to targeted attacks or random attacks.

4.1. Case Study 1: Without Attacks

In this case study, the IEEE 118 bus system is modeled as a directed graph using the earlier methodology. Then, the proposed method is applied to identify the critical nodes in the IEEE 118 bus system. The nodes are ranked based on their controllability indexes and the nodes are regarded as critical if they have higher values of the controllability index. The normalized controllability indexes of critical nodes of the IEEE 118 bus system are plotted in Figure 4. The results are averaged over 100 realizations. In terms of the controllability index, it can be clearly see that some nodes are given higher ranking in this analysis, and they are considered of criticality. From the point of view of controllability, those nodes with higher values of indexes play an important role in maintaining full control of the system. If they are in faults, the whole power system may not be controllable or may need more external inputs to maintain the controllability. Furthermore, the robustness of the network will be test in case study 2 and 3.

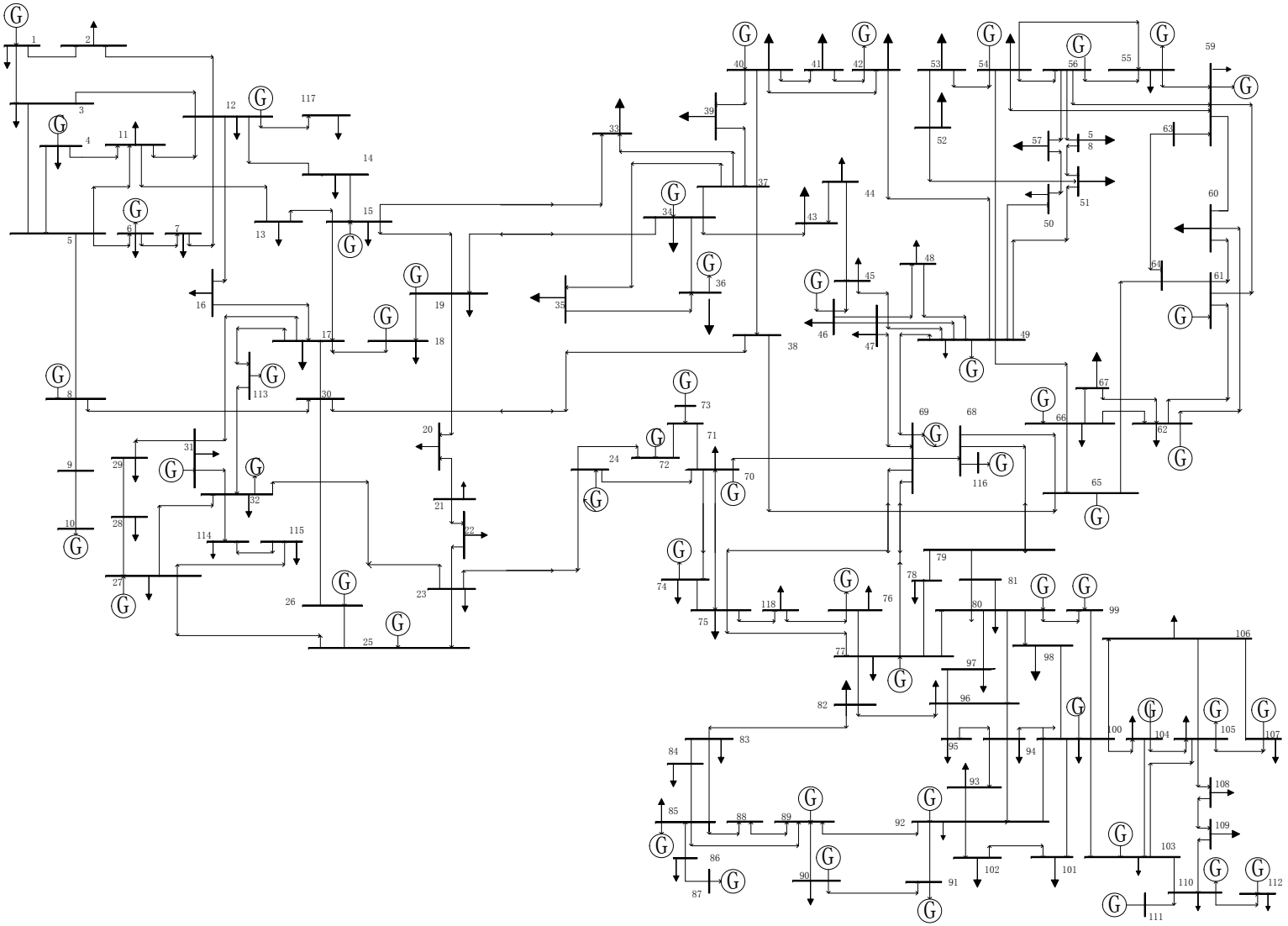


Figure 3. IEEE 118-bus Test system.

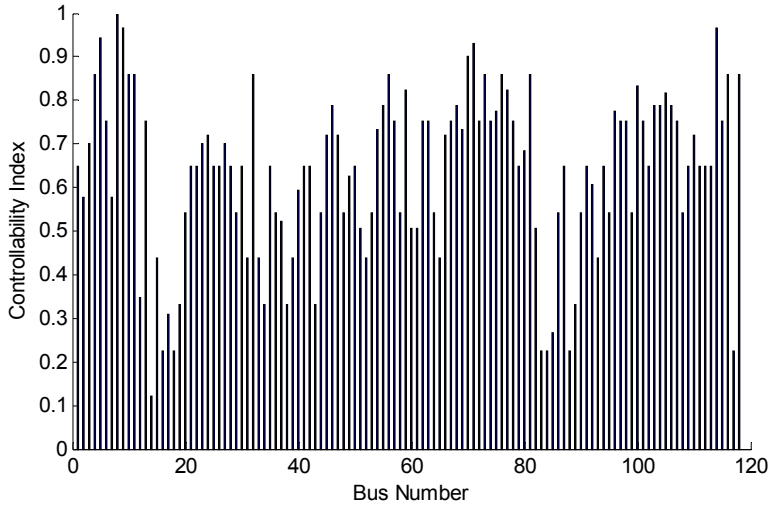


Figure 4. Normalized controllability index.

4.2. Case Study 2: Under Targeted Attacks

In this case study, the focus is on the performance of the proposed method under targeted attacks so that the reliability of the results in case study 1 can be verified. In order to test the robustness of the power system, the analyzed network is subjected to targeted attacks. The set of nodes considered to be critical is disconnected one by one, and the minimum number of driver nodes of the remaining network is calculated after every attack. The results are averaged over 100 realizations and the mean values are plotted in Figure 5. After five such attacks, it can be clearly seen that the minimum number of driver nodes obviously increases as the number of attacks increases, and there needs to be an increase of approximately nine driver nodes to maintain full control of the network, which means that the control robustness of the network is very poor under targeted attacks. Additionally, it shows that the few critical nodes can make the system very vulnerable to attacks in practice. Furthermore, the controllability indexes of the remaining nodes of the IEEE 118 bus system are recalculated after such five targeted attacks. The identification results before and after five targeted attacks are plotted in Figure 6a,b, respectively. It can be observed from Figure 6b that the controllability index distribution is changed clearly, which means there has been a significant driver nodes shift among nodes. In other words, the input should be redesigned so that the analyzed network can be fully controlled. However, it is very difficult or impossible to do that in practice. If the network cannot adjust, it may not offer full control over the network and cannot limit the power system into permitted range. Then, further failures will happen.

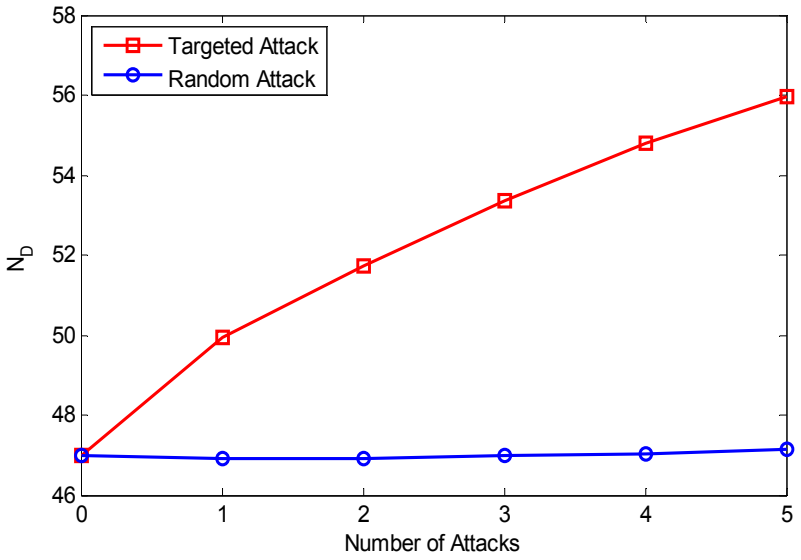
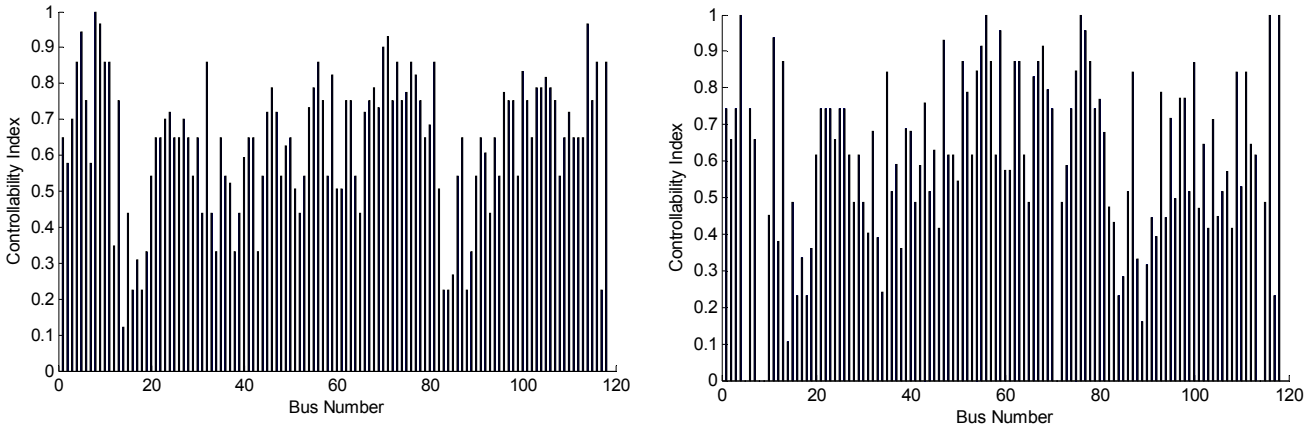


Figure 5. Increase in N_D of the network after attacks.



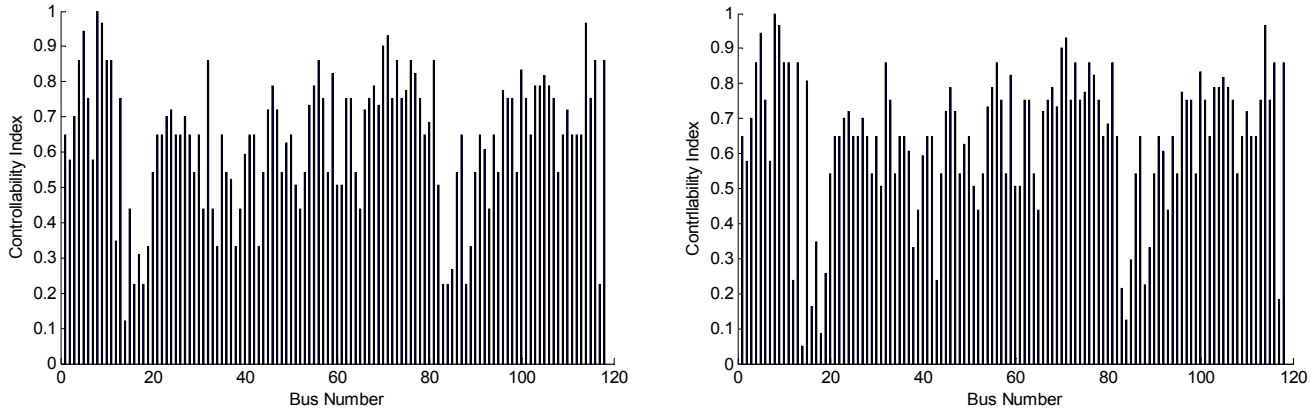
(a) (b)

Figure 6. Effect of targeted attacks on controllability index distribution. (**a**) Original distribution; (**b**) Distribution after five targeted attacks.

4.3. Case Study 3: Under Random Attacks

In this case study, the focus is on the performance of the proposed method under random attacks compared with the results under targeted attacks. The initial conditions are the same as in case study 2. Then, the analyzed network is subjected to random attacks. The nodes with low controllability indexes are disconnected randomly, and the minimum number of driver nodes of the remaining network is also calculated after every attack. The results are averaged over 100 realizations and the mean values are also plotted in Figure 5. It is shown that the minimum number of driver nodes is not clearly changed after five such attacks, which means that the network is very robust in response to random attacks, and the failure of those nodes may not obviously affect the controllability of the system. Furthermore, the identification results before and after five random attacks are plotted in Figure 7a,b. The results show that the controllability index distribution before and after random attacks is very similar, which means the driver nodes distribution is almost not changed. Roughly speaking, the nodes with higher

controllability indexes before attacks still have higher ranking in this analysis.



(a) (b)

Figure 7. Effect of random attacks on controllability index distribution. (**a**) Original distribution; (**b**) Distribution after five random attacks.

4.4. Case Study 4: Implementation on the Tibet Power Grid

In this case study, the IEEE 300 bus system is further considered to show the effectiveness of the proposed critical nodes identification method for a larger power system. The simulation method and process are the same as in case studies 1 to 3, and the simulation results are shown in Figure 8. Figure 8a shows the initial identification results, where some nodes also carriers of higher controllability indexes, which are consider of criticality. Figure 8b shows the minimum number of driver nodes of the remaining network after every targeted and random attack. It can be seen that there needs to be an increase of approximately 12 driver nodes to maintain full control of the network after five targeted attacks. The increased numbers are more than the corresponding results in the IEEE 118 bus system, which means the larger the size of the system, the more difficult it is to maintain full control of the system when the small numbers of critical nodes are absent. Thus, it is more important to identify the critical nodes as the system increases. In addition, there needs to be an increase of approximately 23 driver nodes to maintain full control of the system after 10 targeted attacks. On the contrary, the minimum number of driver nodes is not changed clearly after 10 random attacks. Figure 8c shows the controllability index distribution after 10 targeted attacks, and the identification results are changed clearly compared with the results in Figure 8a. However, the identification results are very similar before and after 10 random attacks, as shown in Figure 8a,d. Therefore, the simulation results mentioned above have once again proven that the system is very robust to random attacks but not targeted attacks, which further verifies the effectiveness of the proposed method.

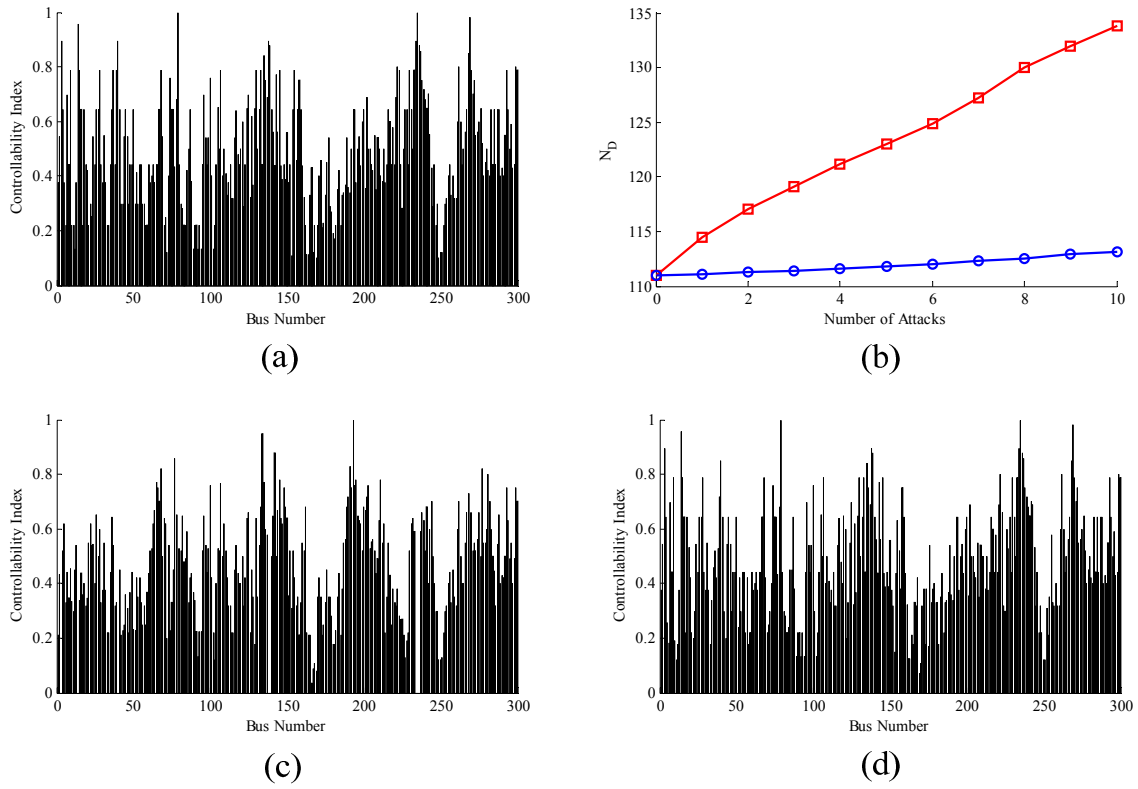


Figure 8. Identification results of the IEEE 300 bus system. (**a**) Initial controllability index distribution; (**b**) Increase in N_D of the network after arracks; (**c**) Controllability index distribution after ten targeted attacks. (**d**) Controllability index distribution after ten random attacks.

4.5. Case Study 5: Comparison with the Conventional Method

In this case study, we focus on analyzing the differences between the proposed method and some conventional methods. It has been previously mentioned that the main vulnerability analysis methods of power systems can be classified as the methods based on system stability and the ones based on complex network theory. The methods based on system stability (e.g., modal analysis based on the Jacobian matrix of the power flow equations, which aims at defining the sensitivity coefficient to assess the stability of the power system and uses the values of sensitivity indexes to identify the critical nodes or bus [8,9]) contain a mass of complex operations which make their analysis a very time-consuming and computation-intensive task. Therefore, it is not very suitable for the vulnerability analysis of large-scale power systems. As an alternative, the methods based on complex network theory have been proposed to assess the vulnerability of power systems in recent decades, which take both the electrical parameters and the topological characteristics of power systems into account in their analysis [18]. This method originated from graph theory and studies the subject systems from the point of view of structure and dynamic function of an array of nodes and lines without heavily relying on the system dimensionality [3], which makes it very suitable for the analysis of large-scale systems. However, as discussed above, most of the existing literature on this issue [3] and [11–18] rigorously requires that the weight of each link must be known and does not consider the system's controllability, which seriously limits its applications in real systems. Compared with the conventional methods

mentioned above, the method in this paper presented a new way to analyze the vulnerability of power systems by considering the system structure controllability, which is suitable to assessing the vulnerability of large-scale power systems as it does not contain complex operations. Moreover, it only requires knowing if there is a direct connection between any two nodes but does not require knowing its accurate connection weight, which can overcome inherently incomplete weight information in real systems.

5. Conclusions

It is important to identify the critical nodes and lines so that the system reliability and efficiency can be improved by monitoring and servicing them, and blackout risk may be better mitigated. This paper proposes a new method to effectively identify the critical nodes in a power network, and the controllability index is defined and used to rank the critical nodes based on the controllability theories of complex networks. This method firstly applies the network controllability theories to research the power system's vulnerability, which fundamentally reveals the important nodes in the power systems and overcomes the limitation of the hypothesis that the weight of each link or transmission line must be known as compared with the present research. The simulation results on the IEEE 118 and 300 bus systems show that the failure of the important nodes can clearly increase the minimum number of driver nodes, meaning there needs to be an increase the number of driver nodes to maintain full control of the network, and leads to a significant driver nodes shift. Thus, its effectiveness is demonstrated through the simulation studies. However, this paper do not consider the time-delays of the networks, which is the future research direction.

Acknowledgments

This work was supported by the Key Foundation of the National Natural Science Foundation of China (61433004), and the Young Foundation of National Natural Science Foundation of China (61203086).

Author Contributions

Y.-S.L. conceived the idea for the manuscript and wrote the manuscript with input from M.-D.Z, H.-G.Z and Q.-Y.S.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Morante, Q.; Ranaldo, N.; Vaccaro, A.; Zimeo, E. Pervasive grid for large-scale power systems contingency analysis. *IEEE Trans. Ind. Inf.* **2006**, *2*, 165–175.
2. Sun, Q.; Han, R.; Zhang, H.; Zhou, J. A Multi-Agent-based consensus Algorithm for distributed coordinated control of distributed generators in the energy internet. *IEEE Trans. Smart Grid* **2015**, doi:1109/TSG.2015.2412779.

3. Dwivedi, A.; Yu, X. A maximum-flow-based complex network approach for power system vulnerability analysis. *IEEE Trans. Ind. Inf.* **2013**, *9*, 81–88.
4. Hussein, M.M.; Senjyu, T.; Orabi, M.; Wahab, M.A.A.; Hamada, M.M. Control of a stand-alone variable speed wind energy supply system. *Appl. Sci.* **2013**, *3*, 437–456.
5. Sun, Q.; Zhou, J.; Guerrero, J.M.; Zhang, H. Hybrid three-phase/single-phase microgrid architecture with power management capabilities. *IEEE Trans. Power Electron.* **2015**, *30*, 5964–5977.
6. Stiel, A.; Skyllas-Kazacos, M. Feasibility study of energy storage systems in wind/diesel applications using the HOMER model. *Appl. Sci.* **2012**, *2*, 726–737.
7. Cai, G.W.; Chan, K.W.; Yuan, W.P.; Mu, G. Identification of the vulnerable transmission segment and cluster of critical machines using line transient potential energy. *Int. J. Electron. Power Energy Syst.* **2007**, *29*, 199–207.
8. Fouad, A.A.; Zhou, Q.; Vittal, V. System vulnerability as a concept to assess power system dynamic security. *IEEE Trans. Power Syst.* **1994**, *9*, 1009–1015.
9. Gao, B.; Morison, G.K.; Kundur, P. Voltage stability evaluation using modal analysis. *IEEE Trans. Power Syst.* **1992**, *7*, 1529–1542.
10. Jung, J.; Liu, C.C. Multi-agent technology for vulnerability assessment and control. In Proceedings of the Power Engineering Society Summer Meeting, 2001, Vancouver, BC, Canada, 15–19 July 2001; pp. 1287–1292.
11. Dwivedi, A.; Yu, X.; Sokolowski, P. Identifying vulnerable lines in a power network using complex network theory. *IEEE Int. Symp. Ind. Electron.* **2009**, 18–23.
12. Nakajima, K.; Yuan, J.; Chen, L.; Sheng, Z. Laser-Driven Very High Energy Electron/Photon Beam Radiation Therapy in Conjunction with a Robotic System. *Appl. Sci.* **2014**, *5*, 1–20.
13. Alhert, R.; Alhert, I.; Nakarado, G.L. Structural vulnerability of the North American power grid. *Phys. Rev. E* **2004**, *69*, 025103–025106.
14. Chen, G.; Dong, Z.Y.; Hill, D.J.; Zhang, G. An improved model for structural vulnerability of analysis of power networks. *Physica A Stat. Mech. Appl.* **2009**, *388*, 4259–4266.
15. Motter, A.E.; Lai, Y-C. Cascade-based attacks on complex networks. *Phys. Rev. E* **2002**, *66*, 1–4.
16. Kinney, R.; Crucitti, P.; Albert, R.; Latora, V. Modeling cascading failures in the North American power grid. *Eur. Phys. J.* **2005**, *46*, 101–107.
17. Freeman, L.C.; Borgatti, S.P.; White, D.R. Centrality in valued graphs: A measure of betweenness based on network flow. *Social Networks* **1991**, *13*, 141–154.
18. Dwivedi, A.; Yu, X.; Sokolowski, P. Analyzing power network vulnerability with maximum flow based centrality approach. In Proceedings of the Industrial Informatics (INDIN), 2010 8th IEEE International Conference on, Osaka, Japan, 13–16 July 2010; pp. 336–341.
19. Hong, M.; Liu, C.C. Complete controllability of a simple, dynamic power system model. *IEEE Trans. Circuits Syst.* **1995**, *42*, 491–494.
20. Hong, M.; Liu, C.C.; Gibescu, M. Complete controllability of an n-bus dynamic power system model. *IEEE Trans. Circuits Syst.* **1999**, *46*, 700–713.
21. Zhang, W.; Wong, S.C.; Tse, C.K.; Chen, Q. Design for efficiency optimization and voltage controllability of series–series compensated inductive power transfer systems. *IEEE Trans. Power Electron.* **2014**, *29*, 191–200.

22. Zhang, H.; Qing, C.; Luo, Y. Neural-network-based constrained optimal control scheme for discrete-time switched nonlinear system using dual heuristic programming. *IEEE Trans. Autom. Sci. Eng.* **2014**, *11*, 839–849.
23. Zhang, H.; Yang, F.; Liu, X.; Zhang, Q. Stability analysis for neural networks with time-varying delay based on quadratic convex combination. *IEEE Trans. Neural Networks Learn. Syst.* **2013**, *24*, 513–521.
24. Zhang, H.; Ma, T.; Huang, G.; Wang, C. Robust Global Exponential Synchronization of Uncertain Chaotic Delayed Neural Networks via Dual-Stage Impulsive Control. *IEEE Trans. Syst. Man Cybern. Part B* **2010**, *40*, 831–844.
25. Zhang, H.; Liu, Z.; Huang, G.; Wang, Z. Novel weighting-delay-based stability criteria for recurrent neural networks with time-varying delay. *IEEE Trans. Neural Networks* **2010**, *21*, 91–106.
26. Lin, C.-T. Structural controllability. *IEEE Trans. Autom. Control* **1974**, *19*, 201–208.
27. Egerstedt, M. Complex networks: Degree of control. *Nature* **2011**, *473*, 158–159.
28. Müller, F.J.; Schuppert, A. Few inputs can reprogram biological networks. *Nature* **2011**, *478*, E4.
29. Liu, Y.Y.; Slotine, J.J.; Barabási, A.L. Controllability of complex networks. *Nature* **2011**, *473*, 167–173.
30. Hopcroft, J.E.; Karp, R.M. A n5/2 algorithm for maximum matchings in bipartite graphs. *SIAM J. Comput.* **1973**, *2*, 225–231.

© 2015 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/).