Vulnerability Analysis for Power Grid Given Renewable Energy Sources Integration

Z. Y. WANG, G. CHEN, Z. Y. DONG, L. Y. ZHANG, D. J. HILL
School of Electrical and Information Engineering, the University of Sydney
Australia

SUMMARY

A power grid is regarded as one of the most critical infrastructures for modern societies, since most of the human activities are highly dependent on the availability of high-quality power supply. Vulnerability of a power system is an essential indication of a grid prone to cascading failures. Undoubtedly, vulnerability analysis plays an important role in the electrical power industry. Therefore, many analytical methods have been proposed for vulnerability assessment. In recent years, the rapid development of complex network theory has provided a new angle on the vulnerability analysis of a power grid. However, current analyses are usually general ones that may ignore the dramatically changes on the penetration level of renewable energy in the grid. Data shows that the capacity of renewable energy generations has increased over 10% each year all over the world. The stability of power grids are greatly impacted by the unpredictable fluctuating characteristics of these renewable resources, which means the networks may be more vulnerable, especially under attacks. In this paper, the complex network model for vulnerability analysis is introduced. Based on the traditional model, an improved vulnerability analysis model given renewable energy integration is proposed. Then, numerical simulations are investigated based on simplified model of the South Eastern (SE) Australia Power System and realistic data of solar and wind output in Australia. The results show the impact of renewable energy sources on power network under different penetration level and load conditions. In addition, some possible recommendations are given for the future research and grid planning.

KEYWORDS

Vulnerability Analysis - Cascading Failure - Renewable Energy - Complex Network
1. Introduction

A power grid is one of the most complicated man-made systems and plays an indispensable role in modern society. However, large scale blackouts all over the world still occur from time to time, in spite of huge investments in power system reliability and security. These blackouts have exposed the potential problems of current mathematical models and analysis methodologies in power systems motivating both academic and industrial societies to seek alternative solutions. In recent years, successful applications of complex networks theory in vulnerability analysis for many natural and artificial networks have attracted the interest of the scientific community to study power grids as complex networks. Actually, a power grid may be described as a complex network like small-world network. This new concept was proposed by Duncan Watts and Steven Strogatz in 1998 [1]. Small-world networks are highly clustered. That is to say, although many nodes that are not neighbours of one another in the network, one can be reached from others by a few steps of paths even if the network size is very large [2]. This means that power networks can maintain a short electrical distance between loads and generators. It may imply that the power transmission capacity of the network would reduce greatly when a failure occurs in these paths [3, 4]. In addition, a power grid has also illustrated the property of scale-free network [5]. It is well known that scale-free networks are robust to random failures but they are vulnerable to targeted attacks. In other words, the removal of a few of important lines and/or nodes would cause cascading failures and severe blackouts.

In the new smart grid framework, more intermittent renewable energy sources, such as wind power, solar power, are connected into the system. The unpredictable fluctuating characteristics of these renewable energy sources must have introduced new security concerns for the stability of power grids. On the other hand, new network expansion also changes the topology of power networks to accommodate these new energy sources. The new network structure with renewable energy sources integration may introduce new vulnerabilities, especially under targeted attacks [6, 7]. Therefore, it is necessary to carry out vulnerability assessment for power grids considering this new situation.

2. The complex network model for vulnerability analysis

According to complex networks theory, a graph can be used to describe the physical connection of a power grid. Based on the topology of a power grid, a graph \( G \) with \( N \) nodes and \( K \) edges can be formed. The Graph \( G \) is denoted by an \( N \times N \) adjacency matrix \( W_{ij} \) describing the physical connections of the network. If there is an edge between nodes \( i \) and \( j \), \( W_{ij} \) is set to 1, otherwise 0. The geodesic path \( d_{ij} \) between two nodes \( i \) and \( j \) is defined as the shortest path between them. The efficiency \( e_{ij} \) between nodes \( i \) and \( j \) is the reciprocal of the geodesic path. This means that the larger the \( d_{ij} \) is, the less efficiently the information can spread between the two nodes. If there is no path between nodes \( i \) and \( j \), \( e_{ij} = 0 \). Once the efficiency is defined, the average efficiency of a network can then be given by

\[
E(G) = \frac{1}{N(N-1)} \sum_{i<j} e_{ij}
\]  

(1)

The \( E(G) \) is usually applied to assess the vulnerability of a network. The index can reveal how the network efficiency changes before and after disturbances. The load at a node \( i \) is defined as the total number of the geodesic paths passing through this node. An important feature of the model is to allocate a given capacity to each node, i.e., the maximum limit of load that a node can bear. The capacity \( C_i \) of a node \( i \) is assumed as directly proportional to the initial load carried by \( i \).

\[
C_i = \alpha L_i(0)
\]  

(2)

where \( \alpha \) is a tolerance parameter. The ref. [8] shows how the damaged efficiency of a power grid changes with different \( \alpha \) under attacks. The \( L_i(0) \) is the initial load handled by node \( i \), and it is also the initial load at iteration step \( t = 0 \). In most complex networks, an initial failure may cause a cascading effect and result in cascading failures. In the complex network model, the removal of a node...

(initial failure), will change the geodesic paths between nodes, then lead to the changes of $L_i$ and $C_i$. This effect would cause some other nodes overloaded and then failed. These new failures would alter the geodesic paths and load of other nodes again. This progress would continue until no overloaded nodes exist. At each iteration step $t$, the following iterative rule is adopted [9,10,11]:

$$
eff_{ij}(t+1) = \begin{cases} 
eff_{ij}(0) \frac{L_i(t)}{C_i} & \text{if } L_i(t) > C_i \\ 
eff_{ij}(0) & \text{if } L_i(t) \leq C_i \end{cases}$$

(3)

where $j$ extends to all nodes that connected to node $i$ directly. At each step $t$, if node $i$ is overloaded, the length of all the edges connected to it is increased. This rule can degrade the transmission capacity of node $i$ and thus decrease the efficiency of whole networks.

3. Vulnerability analysis given renewable energy integration

Renewable energy is generally defined as energy that comes from resources which are naturally replenished, such as sunlight (solar), wind, tides and geothermal heat. In power generation wind power and solar power are more popular. Fig. 1 and Fig. 2 show the practical daily output of photovoltaic (PV) and outputs from three wind farms located in different place in Australia respectively [12]. It is easy to find that the output of PV concentrates during the noon time, and fluctuates during its peak. Apart from that, it is also greatly impacted by weather. The wind power output mainly depends on the location of wind farm. The intermittent and unpredictable characteristics of renewable energy sources should have impact on the vulnerability of power networks.

![Fig. 1 Daily PV output](image1)

![Fig. 2 Daily wind power output](image2)

In order to better make vulnerability analysis, we improve the complex network model in section 2. For distinguishing the nodes that are connected renewable resources from others, a set $\mathcal{R}$ is defined. A node $i \in \{\mathcal{R}\}$ means that the node is connected with a renewable energy generation source. Thus, the efficiency between renewable generator $i$ and node $j$ is defined as $\neff_{ij}$, $i \in \{\mathcal{R}\}$. The efficiency will be affected by the output factor of renewable energy sources from time by time. Then the average efficiency of a network can then be given by

$$E = \frac{1}{N_RN_G} \sum_{i \in \mathcal{R}} \sum_{j \in N_G} \neff_{ij}$$

(4)

At the end of cascading failures, the damaged efficiency $D$ is used to describe the normalized efficiency loss during the cascading failures.

$$D = \frac{E_0 - E_f}{E_0}$$

(5)

where $E_0$ is initial efficiency and $E_f$ is the final efficiency after cascading failures. Therefore, we can assess the vulnerability of a network by observing the $D$ at different iterative step $t$. 

2
4. Simulation and analysis

In order to study the impact of renewable energy sources on network vulnerability, the Simplified Model of the South Eastern (SE) Australia Power System [13] is employed for numerical simulations. The system consists of 14 generating units, 58 load buses and 180 transmission lines. The latest revision of this model was published in 2010 shown in Fig. 3, loosely based on the southern and eastern Australian networks.

The power grid model with renewable energy sources integration is conducted by DIgSILENT. The real power injection vector $P$ represents the amount of traditional generators generation and load at each node under three load operating conditions which shown in Table.1, are obtained from the standard data files of the SE Australia Power System Model [14]. The power outputs of renewable energy generators have been taken the average for each hour, which are obtained from practical Australia WP and PV data files [12, 15].

Table.1 Three normal steady-state operating conditions

<table>
<thead>
<tr>
<th>Load Condition</th>
<th>Light Load</th>
<th>Medium Load</th>
<th>Heavy Load</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Generation MW</td>
<td>15050</td>
<td>19060</td>
<td>23030</td>
</tr>
<tr>
<td>Total Load MW</td>
<td>14810</td>
<td>18600</td>
<td>22300</td>
</tr>
<tr>
<td>Area 4 to Area 2 MW</td>
<td>-200</td>
<td>300</td>
<td>500</td>
</tr>
<tr>
<td>Area 2 to Area 1 MW</td>
<td>470</td>
<td>740</td>
<td>1134</td>
</tr>
<tr>
<td>Area 1 to Area 3 MW</td>
<td>200</td>
<td>-200</td>
<td>1000</td>
</tr>
<tr>
<td>Area 3 to Area 5 MW</td>
<td>200</td>
<td>250</td>
<td>500</td>
</tr>
<tr>
<td>Time in the Day</td>
<td>01:00-08:00</td>
<td>09:00-16:00</td>
<td>17:00-22:00</td>
</tr>
</tbody>
</table>

Fig. 3 Simplified Model of the SE Australia Power System

The numerical simulations have been done for each hour during the day under different penetration levels of renewable energy, 0%, 10%, 20%, 30% and 40%. The Fig.4 and Fig.5 show the damaged efficiency of the power grid under a targeted attack and a random attack given different penetration levels of renewable energy respectively. The random attack curves are gained by averaging 58 individual removals. The targeted attack curves are obtained by removing the highest load bus.
From the simulation outcomes, it can be seen that the curve of damaged efficiency rises with the increase of load condition under both random attack and targeted attack. Obviously, targeted attack can cause more damage to the power grid and more reduction of the efficiency. Again it verifies that power networks have the characteristics of scale-free networks. On the other hand, with the penetration level of renewable energy increases, the damaged efficiency also increases. The actual power outputs from renewable resources are usually intermittent. Particularly PV is not able to generate any energy after sunsets which are more likely to be the peak load period of a day and all the gaps have to be compensated by traditional generators. Thus, the oscillation of power flows in transmission lines would deteriorate with the increase of the penetration level and would be apt to spread cascade failures to larger areas in the power grid. Therefore, it can be seen from Fig.4 and Fig.5 that the maximum damaged efficiency appears at 18:00 in both random and targeted attack scenarios.

Besides, the renewable energy makes different influences in the damaged efficiency of power networks under random and targeted attacks. Fig. 6 shows the varying pattern of random and targeted attacks in the same time points (with the same load condition and output). When the renewable energy is set in low penetration level (10% and 20%), the changes of the performance under random attack is less severe and have long tails. On the contrary, the curves change more dramatically under targeted attacks. It seems that the vulnerability of the grid is more sensitive to the penetration level of renewable energy under targeted attack. Such behaviour can also been disclosed in the 30% line under targeted attacks. Meanwhile, the changes in damaged efficiency become more obvious when the penetration is over 30% under the random attacks. However, when the penetration level comes to 40%, the damaged efficiency under random attack shows significant changes. The curve rises more steeply and draws an exponential tail during peak hours. Based on these results, we may come to the conclusion that the power network may have a threshold on the penetration level of the renewable energy. This threshold is associated with the topology and parameters of the network. If the value of renewable energy connected into the network is over such threshold, the network may be no longer robust to random attacks.
5. Conclusion

In this paper, an improved complex network based vulnerability analysis model considering special characteristics of renewable energy integration have been proposed. Then the simplified model of the South Eastern Australia Power System with practical data is performed to demonstrate how the renewable energy sources impact the vulnerability of the grid. The simulation result shows the changes of vulnerability with different penetration levels under both random attack and targeted attack. From the results, the conclusion can be drawn that the grid would suffer more serious vulnerability under attacks with the growth of renewable energy integration. In other words, the vulnerability of power network deteriorates. Compared with random attacks, the vulnerability is more sensitive to the penetration level of renewable energy under targeted attacks. Also, there is a threshold on the network being robust to random attacks. These new results should be taken into consideration in the future grid design and planning. Particularly, with the high penetration level of renewable energy integrating into a power grid, the topology and the threshold should be considered.

References