The Vulnerability of the Power Grid Structure: A System Analysis Based on Complex Network Theory

Banghua Xie, Xiaoge Tian, Liulin Kong* and Weiming Chen

Faculty of Engineering, China University of Geosciences, Wuhan 430074, China; xiebanghua@cug.edu.cn (B.X.); xiaoge@cug.edu.cn (X.T.); chenweiming@cug.edu.cn (W.C.)
* Correspondence: kongliulin@cug.edu.cn

Abstract: The safety and reliability of the power grid are related to national power security, economic development and people’s daily life. The occurrence of extreme weather changes the external environment greatly. Including generators and transmission lines, many power grid units cannot resist such a huge attack and get damaged easily, which forces units to quit from the power grid running system for a while. Furthermore, if the number of influenced units is high enough, the whole power system will be destroyed by cascading failure caused by extreme weather. Aiming at dealing with the cascading failure emergencies, this paper is trying to improve the traditional power structural vulnerability model so that it can be used to discuss extreme weather and propose a theoretical topological model to help scholars measure the damage caused by extreme cases. Based on previous research in this field, this paper utilizes complex network knowledge to build the power grid topology model. Then, considering extreme cases and the three attack modes simulation process, this paper makes use of the characteristic parameters of the power grid topology model and designs an algorithm, according to the realistic situation of the propagation mechanism of cascading failure of the power grid model as well as extreme weather research. Finally, taking IEEE-30 and IEEE-118 node bus system as examples, which shows that the structural vulnerability method proposed in this paper can properly address the mechanism of unbalanced load of cascading failure of power grid units under extreme conditions and can provide theoretical reference for preventing and reducing the impact of extreme cases on power grid which improves the reliability of the power grid.

Keywords: extreme weather; cascading failure; structural vulnerability; complex network; attack modes

1. Introduction

Recently, global climate change brings new challenges to the power grid design [1]. Determining how best to address the impact brought by climate change is a problem. The literature [2] reviews methods used to model the extreme weather impact. In China, typhoons threaten the southern power system’s stability. Literature [3] summarizes and analyzes the wind accidents of the transmission line. As an emerging concept, [4] resilience is used to measure whether the power grid can be resilient to high-impact and low-probability events.

To be concrete, the state of power grid system and the reliability level of power grid are different under different situations [5], especially under extreme cases. To explore the way of quantifying impact of extreme weather, literature [6] proposes a quantitative reliability index to address the probability and result of power failures. Extreme weather can make the power grid units (including topological nodes and lines) much more unstable in a short time [7], which leads to the failure of individual or local units due to disturbance. As a result, the unit quits from the power grid system, changing the power flow, and then leads to cascade effect, which makes the more power units fail and out of control, leaving the power grid to collapse [8]. Taking power grid faults in central China as an example, in one-year, the number of faults of 500 kV transmission lines have reached 726 for extreme
situations, and the faults of 220 kV transmission lines have reached 3668 [9]. Most of these cascading failures are usually caused by extreme cases. Once a key node or line failed and quit from the network, it would make other related nodes and lines get higher load pressure. The more key nodes or lines quit, the more major bottlenecks are created, which will contribute to the deterioration of electric parts like dielectric materials and operating systems [10]. Jufri, F.H. [11] concludes major power outages worldwide from 2011–2016 and the result showed as Figure 1, which shows that over 20 million people suffered from power outages during those five years and typhoon seems to be one of the most powerful extreme cases that causes severe power outages.

![Pie chart of major power outages under extreme cases from 2011–2016.](image)

Hence, nowadays it is an urgent and important task to do research on analyzing the power grid structural vulnerability under risky circumstances. As one of the most crucial parts that affect the stability of the power grid, power grid vulnerability as a hot topic has widely concerned scholars at home and abroad. Some scholars try to propose methods for improving the resilience and stability of critical electrical power infrastructure to extreme weather [12], while others are trying to find indexes to address the topological vulnerability of the power grid. Particularly, complex network theory has been acknowledged in the wide domain for topological analysis of power systems [13]. Complex network, direct and alternating current power flow are common methods that can be used to model and establish the vulnerability model of the power grid. Literature [14] proposes a new vulnerability index which is weighted line betweenness to find critical lines in the power grid. Also, literature [15] proposes a new parameter named new-ability to evaluate the vulnerability of the power grid. Literature [16] does a survey to trace the evolution in the field where properties of different power grids are studied by using complex network analysis. Literature [17] reviews the latest and relevant papers that have studied robustness by using complex network theory, finding that few of papers focus on strategies to improve robustness. The research on vulnerability index is quite mature, such as load loss and transmission efficiency. The methods used for studying the power grid vulnerability can be classified as deterministic and uncertainty methods [18,19]. The deterministic methods are mainly based on operating state, while the uncertain methods refer to risk possibility assessment. Quantifying the impact of the weather is a difficult task due to its high stochasticity. Hence, a few literatures try to analyze the vulnerability under some attack modes.

Although the application of CN theory in the power system vulnerability assessment has drawn broad interest in recent years, challenges remain. Some literatures still focus on how to address the vulnerability or try to propose methods help improve the vulnerability
of infrastructures of the power grid but do not consider structural vulnerability. Some try to analyze the structural vulnerability of the power grid by utilizing some simulation methods such as attack modes but do not consider the extreme cases. Some literatures consider the extreme cases and vulnerability of the power grid but they do not consider the simulation methods to test vulnerability such as attack modes.

Thus, this paper considers the structural vulnerability of the power grid as well as extreme weather. Finally, this paper uses simulation methods to test and analyze the results. Compared with previously mentioned literatures, this paper not only focuses on vulnerability but also utilizes simulation methods of three special attack modes and extreme conditions. It provides a systematic view of how to analyze and test the vulnerability of the power grid under an extreme weather. Our research methods are as follows.

First, this paper establishes the whole power grid in a macro complex network perspective and improves the topological model by making it into a directed weighted topology model by classifying the node sources and weighting line reactance.

Also, characteristics and necessity of power grid vulnerability are obtained through several attack modes of power grid cascading failure, which is an effective way to quantify results. Based on this, this paper constructs the vulnerability model of power grid structure under extreme circumstances by using the theory of cascading failures.

Finally, extreme conditions are considered for analyzing structural vulnerability. The structural vulnerability model of the topology power grid is studied by utilizing the IEEE 118 bus node system. Results show that there is a significant relation between the structural vulnerability and extreme cases, proving our structural vulnerability model is useful and can be an example for the large-scale power grid. Figure 2 shows the structural organization of this paper:

![Structure flowchart of this paper.](image)

### 2. Related Works

Vulnerability analysis mainly is studied by using below main methodologies [20]. First, define the structural, logical and functional relations among all units with the power grid. Second, try to quantify the performance of indicators. Third, studying system results under different accidental cases. Literatures aiming at vulnerability can be classified into two types [21]: 1. Analytical articles 2. Simulation articles. However, not all scholars can access a titanic amount of data from the real power grid. Hence, the simulation method is becoming more and more popular. Simulation methods can also be performed in two ways: Complex network and Direct current power flow. Ouyang, M. [22] compares three kinds of power grid models including topological model, betweenness based model and direct current power flow model in a vulnerability view to find that topological model and
betweenness based model sometimes perform better when it comes to a certain marginal value. Methods in complex network can be divided into two major approaches: basic complex network models with few electrical elements and improved models with some features like betweenness added to the complex network [23]. This paper is proposing a power grid model considering network theory and typical research methods based on complex systems including cascade model, OPA model, branch process model, etc. [24]. Carreras, B. and Cao, Y. [25,26] analyze the power-law relationship between large-scale blackout and frequency in the American power system, proving it is a mathematical feature of self-organized criticality. Dwivedi A [27] proposes a max-flow-based complex network approach to analyze the vulnerability of power grid. Ren Z [28] counts relationship data between regional environment and line failure rate and uses the least square method to fit to obtain the grid unit failure rate. Besides, many literatures find that the power grid system obeys the small-world model and reveal that the influence of a few nodes and lines will cause great harm to the whole situation [29,30], which indicates the severe results that can be met by the power grid topological structure when it comes to some severe attack. Besides, there are many literatures concentrate on studying the algorithms that improve the complex network efficiency in the network theory [31–33]. Although these articles have studied systematically the complex network theory applications on the power grid, few of them pay much attention to analyzing the harsh outcomes met by the power grid.

Most above literatures contribute more to the basic topological research method in establishing model, while other literatures focus on cascading failures which cause many blackouts accidents all around the world and find they can cause severe reduction in network stability as well as reliability [34,35]. Catastrophic outages caused by cascading power grid failures until now still lead to extremely serious effects. To prevent the power grid from cascading failures, analyzing, and measuring attacks that cause these problems is becoming an urgent topic. Liu, B. [36] utilizes complex network to analyze the vulnerability of key nodes of power grid and build a cascading failure model based on ac power flow model and network topology model, proving cascading failure can cause severe reduce in network stability and reliability. Li, K. and Liu, K. [37] first investigate the robustness of the Chinese power grid under different attack and defense effects and quantify two approaches to avoid this including improving load capacity and protecting critical edges. Wang, J.W. and Rong, L.L. [38] propose two attack strategies and quantified the results that indicate characteristics of a breakdown edge have an important impact on the effects of intentional attacks. Ding, M. [39] analyzes the influence of the overall structure of the power grid on the cascading failures of the power grid from the topology structure of the power grid, and points out that the higher number and degree of nodes will improve the connectivity of the power grid, but at the same time, the severity of the failures will be greater when the power grid is deliberately attacked. Power grid faults will affect the vulnerability of the power system, so it is necessary in order to analyze and evaluate its uncertainty and fault vulnerability, and consider the attacks suffered by the power grid [40,41]. Similar articles all contribute to propose new methods to protect the power grid network from cascading failures. However, few of them consider the possible concrete background of these attack conditions which makes the simulation or analysis lack of some credibility.

In the view of the recoverability of the power grid system, some researchers focus on the measures to improve the flexibility of the power grid, including the preparation strategies before extreme situations and a series of operation strategies that can be adopted in some disasters [42–47]. Some researchers seek to propose various graded response mechanisms and recovery decision-making mechanisms after disasters [48–51]. While others focus on the research of power grid transmission framework topology such as power grid topology reconfiguration and dynamic topological analysis [52,53].

Hence, despite the fact that the above research method considers the failure rate of power grid units in extreme cases, it does not take into account the different action characteristics and effects of different extreme cases on the power grid. Using the constant
failure rate model cannot reflect the randomness and characteristics of weather and cannot be well applied to unusual weather conditions and weather superposition.

3. Background Knowledge

Watts and Strogatz first introduce the small-world model, namely WS small-world model [54,55], and reveal that the small-world model exists in many common networks. Research shows that the power grid system also generally follows the small-world network model [56,57]. Their model is shown in Figure 3, where $p$ refers to the possibility of randomness.

![Figure 3. WS small world network model structure.](image)

The above small-world network mainly introduces a small number of remote connections to the network through the process of edge reconnection, which makes the small-world network have the small characteristic path length of a random network. Therefore, once a small fault occurs in the power system, it may lead to a wide range of cascading failure, which may lead to the collapse of the power grid.

The large-scale interconnection of power grid makes it complicated to describe the dynamic situation of the power system. In addition, if local units are unable to exit the power grid due to low functional vulnerability, it is more likely to lead to continuous chain failure, resulting in large-scale power outages and heavy losses. To study the vulnerability of the power grid from a macro perspective, the first goal is to transform the case power grid structure into a topological model based on graph theory.

Then, when modeling according to the structure and characteristics of different types of power grid units, the power grid units are divided into two categories, which are represented by nodes and edges, respectively, which form a topological model without direction and weight. There are $k$ edges numbered from 1 to $k$. Each edge can be labeled with $i,j$, which means the start node is node $i$ and the end node is node $j$. We define an undirected unweighted graph called $V = A, B$ like Figure 4, in which $A$ and $B$ are respectively defined as column matrix and n-order symmetric correlation matrices to represent, respectively, all nodes and the connection relationship between nodes. The element in the $i$th row and the $j$th column in the matrices $B$ is the connectivity coefficient $b_{ij}$, while $a_{ij}$ represents the $i$th node in $n$ node. Therefore, the number of network edges $k$ is equal to the number of elements when $b_{ij} = 1 (1 \leq i, j \leq n)$. Also, if there is a node then $a_{i'} = 1$ else the $a_{i'} = 0 (1 \leq i' \leq n)$. Or if there is a connection between $i$ and $j$ then $b_{ij} = 1$ else $b_{ij} = 0$.

\[
A = (a_1, a_2 \cdots a_n), \quad (1)
\]

\[
B = \begin{pmatrix}
    b_{11} & b_{12} & \cdots & b_{1n} \\
    b_{21} & b_{22} & \cdots & b_{2n} \\
    \vdots & \vdots & \ddots & \vdots \\
    b_{n1} & b_{n2} & \cdots & b_{nn}
\end{pmatrix}, \quad (2)
\]
Energy flow can be in both directions along the edges of the network, and the weight of each edge is 1. When there is a parallel connection, because the number of multipath edges is the same and the multipath weight is the same, the minimum path cannot be determined, which has a great influence on the analysis of network parameters. So, in this paper, the undirected and unweighted model is changed into a directed and weighted one.

Energy can only be transferred from the node with higher electrical potential to the node with lower electrical potential, transforming the undirected topological model into the directed topological model. In this paper, grid nodes consist of three types as in Figure 5, which can quite match the reality. When the output power of nodes is greater than the load power, the nodes are the source nodes. When the output power of a node is lower than the load power, the node is a sink node. Additional nodes are contact nodes.

As shown in Figure 5, if node $v$ belongs to the source node, then the path only leaves from this node. This is because the source node is the starting node of the shortest path, and the number of shortest paths leaving the node is less than the number of shortest paths leaving the node. On the contrary, if node $v$ belongs to a sink node, the number of shortest paths entering the node is greater than the number of shortest paths leaving the node. In this case, this paper introduces a virtual node to transform node $v$ into a link node.

The reactance value $x_{ij}$ is taken as the edge weight $w_{ij}$, and the reactance is similar to the effect of resistance on DC current. When the reactance value of the line is larger, the transmitted power is smaller, which makes the unweighted topology model be converted into the weighted topology model. Redefine an $N$-order weight matrix $W$ to represent the connection relationship between nodes under weighting. The element in row $i$ and column $j$ of matrix $W$ is $w_{ij}$:

$$W = \begin{pmatrix}
  w_{11} & w_{12} & \cdots & w_{1n} \\
  w_{21} & w_{22} & \cdots & w_{2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  w_{n1} & w_{n2} & \cdots & w_{nn}
\end{pmatrix},$$

(3)

And

$$w_{ij} = \begin{cases}
  0, & i = j \\
  x_{ij}, & i \neq j \text{ and there is a connecting edge between } i \text{ and } j \\
  \infty, & i \neq j \text{ and there is no connecting edge between } i \text{ and } j
\end{cases}$$

(4)
Distance $DIS_{ij}$ between node $i$ and node $j$ is the sum of the edge reactance included in the shortest path. Distance $DIS_{ik}$ between node $i$ and $k$ is obtained as Figure 6.

![Figure 6. Weight calculation.](image)

The average path length $AL$ of the network is defined as the average distance between any two nodes.

$$DIS_{ik} = w_{ij} + w_{jk}, \quad (5)$$

$$\frac{1}{2}n(n-1)AL = \sum_{i \neq j} DIS_{ij}, \quad (6)$$

Two types of betweenness are divided into node betweenness $BT_v$ and edge betweenness $BT_e$. Edge betweenness $BT_e$ is the proportion of weighted shortest paths passing through an edge in the network to all weighted shortest paths in the network. Node betweenness $BT_v$ is the proportion of weighted shortest paths passing through a node in the network to all weighted shortest paths in the network, where $\delta_{ij}$ refers to the number of shortest paths between node $i$ and node $j$. $\delta_{ij_v}$ and $\delta_{ij_e}$ are the number of shortest paths between node $i$ and node $j$ containing node $v$ or edge $e$, respectively.

$$BT_v = \frac{\sum_{i \neq v \neq j} \delta_{ij_v}}{\sum_{i \neq j} \delta_{ij}}, \quad (7)$$

$$BT_e = \frac{\sum_{i \neq j} \delta_{ij_e}}{\sum_{i \neq j} \delta_{ij}}, \quad (8)$$

The betweenness $BT_G$ of source node $v$ is as following, and $n_L$ is the number of sink nodes.

$$BT_G = BT_v + \frac{1}{2}n_L, \quad (9)$$

The betweenness $BT_L$ of sink node $v$ is as following and $n_G$ is the number of source nodes.

$$BT_L = BT_v + \frac{1}{2}n_G, \quad (10)$$

In the reactance weighted network, the node degree $k_i$ remains unchanged, which is defined as the number of edges connected to this node. The average degree $AVED$ of a network is the average degree of all node degree $k_i$.

$$AVED = \frac{1}{n} \sum k_i \quad (11)$$

The flow chart of power grid topology model is presented in Figure 7. It shows the process of power grid topology characteristic parameters and model modeling analysis as follows:
Cascade failures refer to the fact that some units of the power grid exit the power grid due to slight disturbance, and the cascade effect causes the unbalanced load of other units in the neighborhood to cause faults, which eventually leads to the occurrence of large-scale power outages and makes the power grid collapse. The cascading failure process can be divided into three stages: initial stage, expansion stage, and collapse stage [58] in Figure 8:

1. **Initial stage**: due to external disturbance in extreme cases, individual disturbed units fail due to limited capacity. In the initial stage of the accident, the whole power grid is less affected at this stage. If the accident is found in time and the corresponding preventive measures are taken, the further deterioration of the accident can be controlled in time;

2. **Expansion stage**: in the initial stage, the fault continues to spread and expand, which leads to the change of unit load related to the unit logic of the initial fault under the action of system structural vulnerability, so that it is easy for the fault to exit the operation system. The expansion stage of accident expansion is formed by concluding which time the fault range of the power grid is expanded. However, it is still a partially controllable stage.

3. **Collapse stage**: when the faults continue to spread and expand in the expansion stage, the loads caused by many local unit faults will accumulate further, which makes the overall load distribution and initial distribution of the system change rapidly. Due to the influence of the power grid, larger-scale faults will eventually lead to the cracking of the power grid system and even the whole power grid.
4.1. Evaluation Index of Power Grid Structural Vulnerability

The structural vulnerability of the power grid system is defined as the difficulty degree that individual units or subsystems in power grid system are disturbed and exit from operation, which makes the units or subsystems in the neighborhood exit one after another by a chain effect. Finally, it leads to the collapse and paralysis of the power grid system. In order to quantify the change degree of power grid transmission capacity before and after-failure due to vulnerability of power grid units, this paper defines the index of the power grid structural vulnerability as load loss percentage and network transmission efficiency, which are described as follows:

4.1.1. Percentage of Load Loss

When the grid nodes are overloaded or run out of the grid due to the disturbance of the external environment, the load transmitted by the whole grid will change accordingly. \( L_j \) and \( L_k \) represent the load of \( jth \) and \( kth \) nodes. The percentage of load loss \( \eta_L \) is defined as the ratio of the load of all normal operation sink nodes \( L_j \) in the current power grid to the load of all nodes \( L_k \) in the power grid in the initial state, which is expressed in a percentage system. \( G_1 \) is the set of all failed transmission nodes. \( G_0 \) is the set of all normal working nodes.

\[
\eta_L = \frac{\sum_{j \in G_1} L_j}{\sum_{k \in G_0} L_k} \times 100\% \tag{12}
\]

4.1.2. Network Transmission Efficiency

For the undirected powerless network topology model, the network transmission efficiency \( E \) is defined as the average of the reciprocal distance \( DIS_{ij} \) between the network nodes of all node pairs in the power grid, i.e.,:

\[
E = \frac{1}{\frac{1}{2}n(n-1)} \sum_{i \neq j} \frac{1}{DIS_{ij}} \tag{13}
\]
In this paper, the line reactance value is used as the weight of the edge, and the shortest transmission path of the node is the current transmission path. Using the line reactance value $w_{ij}$ instead of the network node distance $d_{ij}$ can better reflect the actual operation state of the power grid, so the network transmission efficiency $E$ is overloaded as follows:

$$E = \frac{1}{2n(n-1)} \sum_{i \neq j} \frac{1}{w_{ij}}$$  \quad (14)

Assuming there is no direct connection between node pair $i$ and $j$, it is known from the previous chapter that $w_{ij} \to \infty$ at this time and then $1/w_{ij} \to 0$.

The network transmission efficiency decline percentage $\eta_E$ is defined as the ratio between the current network transmission efficiency $E$ and the initial network transmission efficiency $E_0$, which is expressed in percentage, namely:

$$\eta_E = \frac{E}{E_0} \times 100\%$$  \quad (15)

4.2. Vulnerability of Power Grid Structure

Due to the restriction of economic factors, the load capacity of the power grid unit is limited. The load on the line is the energy flowing through the line. Energy flowing through nodes can be split into inflow energy and outflow energy. Inflow energy is divided into generator input energy $L_G$ and input energy $L_{in}$, and outflow energy is node load energy $L_i$ and output energy $L_{out}$, as shown in Figure 9. The load of the node is all the energy flowing into or out of the node, i.e., The inflow load will always be equal to the outflow load according to basic Kirchhoff’s law of electrical circuits:

$$L_i = L_G + L_{in} = L_L + L_{out}$$  \quad (16)

![Figure 9. Schematic diagram of energy flowing through nodes.](image)

In the grid cascading failure model, the load of each unit under the initial grid topology is taken as the reference load, and the rated standard load capacity $S_{Ratedi}$ and the limited load capacity $S_{Limiti}$ are defined as follows:

$$S_{Ratedi} = a_0 \cdot L_{i0}$$  \quad (17)

$$S_{Limiti} = a_1 \cdot L_{i0}$$  \quad (18)

$L_{i0}$ is the load of each unit under the initial power grid structure. $a_0$ is the rated load capacity coefficient. $a_1$ is the ultimate load capacity coefficient, which is taken as 1.1 and 1.2, respectively, in this paper.

The variation of external environmental factors and the fault of adjacent lines will make the load level of the line change [59]. Load specified capacity and load limit capacity are used to measure the impact of load on vulnerability, which cannot reflect the vulnerability level of power grid lines and systems in the short term in the future. Therefore, this paper improves the calculation method of unit failure rate of the line. Considering the functional relationship between the unit failure rate of the line and the load level, this paper divides

$$\sum_{i,j \in s} \frac{1}{\text{Distance}(i,j)}$$
the influence of the load on the failure rate into three piecewise functions and puts forward an improved cascading failure model of the power grid in extreme cases, which is described as follows [59]:

\[
\lambda_i(t) = \begin{cases} 
\lambda_{io}, & 0 < L_i \leq S_{Ratedi} \\
(S_{Ratedi} - L_i)^n + c, & S_{Ratedi} < L_i < S_{Limiti} \\
\infty, & L_i \geq S_{Limiti}
\end{cases}
\] (19)

\(L_i\) is the load value of line unit \(I\) under the current operating condition. \(S_{Ratedi}\) is rated load capacity. \(S_{Limiti}\) is the limit load capacity. \(k, c, n\) are shape coefficient, position parameter and change coefficient, respectively. According to reference [59], the values of these three factors are \(0.1\lambda_{io}, 0, \) and \(1\), respectively.

When the load \(L_i\) of power grid unit is less than the rated load capacity \(S_{Ratedi}\), the failure rate of power grid lines is little affected by the load, which is the same as the original failure rate \(\lambda_{io}\) in the current state. When the power grid line unit exceeds the rated load capacity \(S_{Ratedi}\) but does not exceed the limit load capacity \(S_{Limiti}\), the line unit is in an overload state. When the adjacent lines quit operation, the system load will be redistributed, which will increase the transmission burden of other line units and increase the failure rate of line units. When the line load is closer to the limit load capacity \(S_{Limiti}\), it is easier to receive external disturbances and cause faults. When the load \(L_i\) of power grid unit exceeds the limit load capacity \(S_{Limiti}\), the protection device cuts off the line.

When a grid unit is removed, the load of the unit will be distributed to other adjacent units according to the following equations. Based on the Kirchhoff’s laws using the node voltage method, the above DC resistive networks is established, in which the \(w_{ij}\) refers to the component of the matrix mentioned before. The power flow of DC resistive networks can be obtained as follows:

\[
\begin{pmatrix}
L_1 \\
\vdots \\
L_k \\
\vdots \\
L_n
\end{pmatrix} = \begin{pmatrix}
w_{11} & \cdots & w_{1k} & \cdots & w_{1n} \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
w_{k1} & \cdots & w_{kk} & \cdots & w_{kn} \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
w_{n1} & \cdots & w_{nk} & \cdots & w_{nn}
\end{pmatrix} \begin{pmatrix}
L_{out1} \\
\vdots \\
L_{outk} \\
\vdots \\
L_{outn}
\end{pmatrix}
\] (20)

\[
L_k = L_{outk} \sum_{m=1}^{n} W_{km} L_{outm}
\] (21)

4.3. Extreme Weather Background

In this paper, the research of extreme weather is more about gale and icing weather which is common all over the world [60]. There are many literatures that focus on how to analyze extreme weather and its effects. Literature [61] proposes a circular geometrical model to address the wind and ice effects for their attributes. As a common phenomenon, ice will come with gusts, tornadoes, hurricanes, etc. Usually, icy weather and windy weather weaken the power grid in different ways. The main factor of icy weather that influences the power grid is ice coating the power wires, and that of windy weather is strong wind that can do damage to all wires and towers. Ice coating will result in the cross section of wires increasing and will affect the ice load. A heavy ice or snow event will collapse the high voltage power tower. Hence, in this paper, extreme cases will be set as wind and ice conditions and we build the extreme weather model:

\[
EW(\text{wire}_{xi}, \text{wire}_{yi}) = Ae^{\left(-\frac{1}{2}\left(\frac{(\text{wire}_{xi} - EW_{xi})^2}{\varrho} + \frac{(\text{wire}_{yi} - EW_{yi})^2}{\varrho}\right)\right)}
\] (22)

In the above (22), \(A\) denotes the extent of the extreme weather and \((\text{wire}_{xi}, \text{wire}_{yi})\) and \((EW_{xi}, EW_{yi})\), separately, represent the position of line/wire and extreme weather middle location. \(r\) is the radius of the extreme affecting range and \(\varrho\) is a coefficient. Since the
extreme weather have already been classified two major types in this paper that will be studied, their power load model will also depend on both the extreme weather as well as their models. According to the literatures discussed before, here models can be built as follows:

\[
L_I = \int_0^t A_1 e^{-\frac{1}{2}l\left(\frac{\partial y_{EI}(t)}{\partial t} + \frac{\partial y_{EW}(t)}{\partial t}\right)^2} dt
\]

\[
L_W = W(t) \left( A_{W1} e^{-\frac{1}{2}\left(\frac{\partial y_{EI}(t)}{\partial t} + \frac{\partial y_{EW}(t)}{\partial t}\right)^2} - A_{W2} e^{-\frac{1}{2}\left(\frac{\partial y_{EI}(t)}{\partial t} + \frac{\partial y_{EW}(t)}{\partial t}\right)^2}\right).
\]

The above Equations, \(L_I\) and \(L_W\) are load under icing and wind weather. (23) is in the form of integral for ice coating is constantly increasing. And in the next equation, \(W(t)\) indicates the effects brought by wind angle for that only when the wind direction and the wires direction is at right angles the wires will suffer the whole effects. Otherwise, the wind can be treated as vector and be decomposed into two vectors, which includes a parallel one and a vector just at the right angles with the wire direction. This paper sets \(\lambda_I(t) = g_1(L_I(t))\), \(\lambda_W(t) = g_2(L_W(t))\), where \(\lambda_I\) means the failure rate of ice load and \(\lambda_W\) means the failure rate of wind load. \(g_1\) and \(g_2\) are used to express the two different failure rate function. Here comes a question: what about the regions that both suffer from ice and wind. \(a_I\) and \(a_W\) are the coefficients of the two weathers. Literature [61] suggest a coefficient that allows the two failure rates can add up to a new failure rate if there are two extreme conditions:

\[
\lambda = a_I \lambda_I + a_W \lambda_W(t)
\]

In extreme cases, when any unit of the power grid quits operation due to its own factors or disturbed faults, the load of the power grid unit is redistributed. When the load of adjacent units or small-scale subsystems exceeds the limit load, the fault occurs and is removed, which propagates repeatedly, resulting in cascading failure of the power grid.

### 4.4. Vulnerability Analysis Process of Power Grid Structure

In extreme cases, when any unit of the power grid quits operation due to its own factors or disturbed faults, the load of the power grid unit is redistributed. When the load of adjacent units or small-scale subsystems exceeds the limit load, the fault occurs and is removed, which propagates repeatedly, resulting in cascading failure of the power grid.

In order to discuss the vulnerability of small-world characteristics of power grid to power grid structure, this paper designs different attack strategies to attack power grid in extreme cases, so as to determine the impact of cascading failures on power grid structure vulnerability and find out the weak units or subsystems that have the greatest impact on the power grid.

This paper improves the attack mode of algorithm and divides it into the following three types for simulation:

1. **Line random attack**: randomly attack a normal operation line according to the weight of line reliability and time is used to weigh the vulnerability of power grid function. This paper set the reliability as a time-based integration where \(\lambda_i\) is unit failure rate:

\[
F_i(t) = e^{\int_0^t \lambda_i dt}
\]

2. **Line betweenness attack**: attack the line with the largest specified betweenness in turn.

3. **Linear function vulnerability attack**: attack the line with the highest specified vulnerability in turn. The vulnerability is calculated by using load of loss. The vulnerability is calculated by using betweenness times weight the vulnerability of power grid:

\[
F_v(t) = BT_e(1 - e^{\int_0^t \lambda_i dt}),
\]
The process of vulnerability analysis of power grid structure in this paper. All the following steps of the analysis algorithms are established by using anaconda python 3 IDE. Steps are as follows and are shown in the Figure 10:

Step 1: Data initialization.
Input data from IEEE-30 and IEEE-118. At the same time, the extreme weather condition will also be included. Finally, set the number of the total loop.

Step 2: Choose an attack mode.
Enter the loop, and select the attack objects (the line with the highest vulnerability, the line with the highest intermediate number and the line with random attack) and exit the loop after attacks of settled number.

Step 3: Cascading failures.
Transfer the load of the line according to (21). According to the power dispatch after the load transferring, remove the nodes and related lines if the redistributed load exceeds the capacity of this node or line. From the first node and related lines to traverse to the last node and related lines to check whether the load of nodes and relative lines exceeds the capacity of nodes and lines. Set these nodes and lines as broken and remove them.

Step 4: Calculation.
After removing broken nodes and lines, it is necessary to recalculate the between-ness of remained nodes so that vulnerability parameters can be obtained later. Calculate the failure rate of load exceeding rated capacity but not exceeding limited capacity according to (19). Calculate the percentage of load loss and the variation ratio of network transmission efficiency according to (12)–(15).

Figure 10. Flow chart of vulnerability analysis of power grid structure.

In this paper, the index of structural vulnerability of the power grid with cascading failure is analyzed and reviewed. The percentage of load loss and network transmission efficiency are selected as indicators of structural vulnerability. The mechanism of cascading failure of the power grid under unbalanced load is explored. The connection between the unit load and power grid vulnerability in extreme cases is combined and the load distribution scheme under unbalanced load vulnerability is constructed. Simulation methods of deliberate attack and random attack are designed. In the fourth chapter, an example will
be utilized to verify the rationality of the model constructed in this chapter and carry out risk assessment.

5. Example Analysis

In this paper, the IEEE-30 bus system and IEEE-118 bus system are taken as examples to analyze. The structural vulnerability of the power grid is calculated. Vulnerability of unbalanced power grid load in extreme cases is analyzed. Compared with IEEE-30, IEEE-118 represents a portion of the American Electric Power System (in the Midwestern US) as of December, 1962. It was entered in IEEE Common Data Format and PECO PSAP Format by Rich Christie at the University of Washington in 1993. The IEEE 30 Bus Test Case represents a portion of the American Electric Power System (in the Midwestern US) as of December, 1961. A hardcopy data was provided by Iraj Dabbaghi of AEP and entered in IEEE Common Data Format by Rich Christie at the University of Washington in August 1993. In this paper, the data of IEEE-30 and IEEE-118 is from “Ali R. Al-Roomi (2015). Power Flow Test Systems Repository (https://al-roomi.org/power-flow (accessed on 11 August 2021)). Halifax, Nova Scotia, Canada: Dalhousie University, Electrical and Computer Engineering.”

5.1. Topology Modeling and Analysis of Power Grid

5.1.1. IEEE 30 Topology Model

Figure 11 is a wiring diagram of IEEE-30 node system, which consists of 30 nodes and 41 lines. According to the node properties mentioned above, the nodes can be divided into 5 source nodes, 19 sink nodes, and 6 contact nodes. Moreover, it is noted that although node 5 is both an engine node and a load node, the load power of node 5 should be greater than its generator input power in Table 1, so node 5 is a sink node. The specific type of each node is shown in Table 2. Label nodes and lines, respectively, and determine coordinate positions, and distinguish them with different colors according to node types.

![IEEE-30 bus system topology model diagram](image)

**Figure 11. IEEE-30 bus system topology model diagram.**
Table 1. IEEE-30 system node type.

| Node Type     | Node Number | Node ID                  |
|---------------|-------------|--------------------------|
| Source node   | 5           | 1, 2, 8, 11, 13          |
| Sink node     | 19          | 3, 4, 5, 7, 10, 12, 14, 15, 16, 17, 18, 19, 20, 21, 23, 24, 28, 29, 30 |
| Link node     | 6           | 6, 9, 22, 25, 26, 27     |

According to the first chapter, the topology model of the power grid is established, and the power grid is transformed into a directed weighted topology model. Figure 11 is a schematic diagram of ice and wind effects range, in which a radius is established with a unit length of their effects.

5.1.2. IEEE 118 Topology Model

Figure 12 is a wiring diagram of IEEE-118 node system. Label nodes and lines and determine positions. Finally, distinguish them with different colors according to node types and get pictures from 12 to 14.

![Figure 12. Standard IEEE118-node system.](image-url)

Figures 13 and 14 are the topological diagrams and abstract topological with coordinates, which consists of 118 nodes and 186 lines. According to the node properties mentioned above, the nodes can be divided into 55 source nodes, 93 sink nodes, and 10 contact nodes. Moreover, there are some generators that do not generate power and they are sink nodes. The specific type of each node is shown in Table 3.
Figure 13. IEEE118-node system.

Figure 14. IEEE-118 bus system topology model diagram.
Table 1. IEEE-118 system node type.

| Node Type   | Node Number | Node ID                                                      |
|-------------|-------------|--------------------------------------------------------------|
| Source node | 15          | 10, 12, 25, 26, 31, 49, 61, 65, 66, 69, 80, 87, 89, 100, 103 |
|             |             | 1, 2, 3, 4, 6, 7, 8, 11, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 27, 28, 29, 32, 33, 34, 35, 36, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 62, 67, 70, 72, 73, 74, 75, 76, 77, 78, 79, 80, 82, 83, 84, 85, 86, 88, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 101, 102, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118 |
| Sink node   | 93          |                                                              |
| Link node   | 10          | 5, 9, 30, 37, 38, 63, 64, 68, 71, 81                         |

5.1.3. Extreme Weather Data

Since the failure rate mentioned before in (25), here it is necessary to define the functional relationships between the ice and wind load and the failure rate connected to that. According to the literature [61], Table 4 is about the failure rate function and have been concluded as follows for the next simulation part.

Table 3. Failure rate function of ice and wind load.

| $L_W$       | $\lambda_W$ (Number/h, 50 km) | $L_I$       | $\lambda_I$ (Number/h, 50 km) |
|-------------|-------------------------------|-------------|-------------------------------|
| $L_W \leq 0.3W$ | $1.2 \times 10^{-5}$         | $L_I \leq 0.3l_I$ | $0$                           |
| $0.9d_W < L_W \leq 1.0d_W$ | $8.0 \times 10^{-4}$         | $0.3d_I < L_I \leq 0.5d_I$ | $4.5 \times 10^{-3}$         |
| $1.0d_W < L_W \leq 1.1d_W$ | $0.048$                       | $0.5d_I < L_I \leq 0.9d_I$ | $0.010$                       |
| $1.1d_W < L_W \leq 1.2d_W$ | $0.060$                       | $0.9d_I < L_I \leq 1.0d_I$ | $0.015$                       |
| $1.2d_W < L_W \leq 1.5d_W$ | $0.028$                       | $1.0d_I < L_I \leq 1.1d_I$ | $0.033$                       |
| $1.5d_W < L_W$ | $0.04$                        | $1.1d_I < L_I \leq 1.2d_I$ | $0.050$                       |
| /             | /                             | $1.2d_I < L_I \leq 1.5d_I$ | $0.071$                       |
| /             | /                             | $1.5d_I < L_I$ | $0.10$                       |

Now that the failure rate has been decided by the mentioned function, it is important to figure out how to conduct the extreme weather coming into the system. According to the first chapter, the topology model of the power grid is established, and the power grid is transformed into a directed weighted topology model. Figure 15 is a schematic diagram of ice and wind effects range, in which a radius is established with a unit length of their effects.

![Figure 15. Ice effects range and Wind effects range.](image)

To make cases much easier to understand, two kinds of extreme cases are drawn in Figure 16. They meet a simple topological network in two different angles and original start sites, which indicates similar sites in IEEE-30 and IEEE-118. In this paper, the direction of wind is 45-degrees and starts to blow in 10 km from (0,0) to the end of the map with radius equal to 200 km in the topological Figure 14. Similarly, the direction of ice is −90-degree and start to blow in 10 km from (10,18) to the end of the map with radius equal to 130 km in the topological Figure 14. By doing this, the influences caused by the two cases can be
obtained easily and clearly. By utilizing (25), this paper considers the coefficients of the two proposed extreme cases at the same time and set the maximum load of ice and wind to 50 and 18.95. The wind and ice will go through the power grid from different angles and started sites to influence the lines that are on their ways. Lines within their ways will suffer from wind and ice according to its position and the distance between the line and the central of the wind or ice. After the wind passing through the lines, the load of wind and ice will gradually decrease as time goes by. In this paper, the data of extreme weather is set as Tables 4 and 5.

![Ice and Wind started sites in the topological model.](image)

**Figure 16.** Ice and Wind started sites in the topological model.

**Table 4.** Load of wind and ice of highest 8 lines in IEEE-30 during this process.

| Number of Lines (Wind) | Load of Wind   | Number of Lines (Ice) | Load of Ice   |
|------------------------|---------------|-----------------------|--------------|
| 22                     | 23.6328903    | 12                    | 65.1723427   |
| 30                     | 22.65910081   | 14                    | 65.1723427   |
| 18                     | 22.65449605   | 28                    | 65.1723422   |
| 20                     | 21.91749813   | 6                     | 65.16670399  |
| 23                     | 18.49225909   | 7                     | 65.16670399  |
| 32                     | 12.28254813   | 10                    | 65.16670399  |
| 24                     | 6.298664683   | 9                     | 65.16577223  |
| 17                     | 1.585745099   | 26                    | 65.16028429  |

**Table 5.** Load of wind and ice of highest 8 lines in IEEE-118 during this process.

| Number of Lines (Wind) | Load of Wind   | Number of Lines (Ice) | Load of Ice   |
|------------------------|---------------|-----------------------|--------------|
| 110                    | 23.61433234   | 46                    | 65.16670399  |
| 114                    | 23.53946714   | 49                    | 65.16670399  |
| 108                    | 23.53265901   | 54                    | 65.1241117   |
| 109                    | 23.53114991   | 108                   | 65.00203936  |
| 115                    | 23.52855244   | 109                   | 65.00203936  |
| 112                    | 23.48828542   | 114                   | 64.96905002  |
| 111                    | 23.35066356   | 110                   | 64.96862148  |
| 113                    | 21.02053777   | 115                   | 64.95683736  |

5.2. Simulation and Analysis of Power Grid Functional Vulnerability

5.2.1. Structural Vulnerability Calculation of Proposed Model without Extreme Weather

According to the definition and algorithm of power grid structural vulnerability in extreme cases in Chapter 3, this section mainly calculates vulnerability attack, dielectric attack, and reliability random attack results. However, at first, here the algorithm does not use the extreme cases as background to get initial version of structural vulnerability results. The results are as Figures 17–20. Figures 17 and 20 shows the power grid of 30 nodes and 118 nodes perform differently. In Figure 17, the percentage of load loss is
pretty high under vulnerability and betweenness attack, while reliability attack seems to hold the weakest attack effect. However, in Figure 19, it is different. Vulnerability and betweenness attack caused load losses to shrink greatly, nearly 60%, while the load loss caused by reliability attack only decreased 30%. However, the resulting variation ratio between Figures 18 and 20 is consistent. Their data indicates the variations ratio of network transmission efficiency grow fast for the first five attacks. Then it tends to slowly increase after the first 5 attacks.

Figure 17. Load loss ratio of IEEE-30 bus system without extreme weather.

Figure 18. Variation ratio of network transmission efficiency of IEEE-30 bus system without extreme weather.
Figure 18. Variation ratio of network transmission efficiency of IEEE-30 bus system without extreme weather.

Figure 19. Load loss ratio of IEEE-118 bus system without extreme weather.

Figure 20. Variation ratio of network transmission efficiency of IEEE-118 bus system without extreme weather.

5.2.2. Structural Vulnerability Calculation of Proposed Model under Extreme Weather

In this part, the extreme cases are considered by using Chapters 3 and 4. Similarly, Figures 21–24 indicate the percentage of load loss and the percentage of network transmission efficiency decline under the three attack modes of IEEE-118 and IEEE-30 cases, respectively, under extreme weather. Compared with the Figures 17–20, Figures 21–24 which consider extreme weather illustrate that with extreme cases, the percentage of load loss and variation ratio of network transmission efficiency perform with higher values which indicate the damage made by extreme cases is also bigger, and the values commonly increased.
Here, this paper proposes rates of indexes in IEEE-118 divided by indexes in IEEE-30 with the number of attacked times from 1 to 10. Thus, it is much easier to see the difference of results between the two examples. The results in Figure 25 show that the percentage of load loss of IEEE-118 is clearly much smaller than the percentage of load loss of IEEE-30, proving that bigger network IEEE-118 usually is more stable and reliable than the IEEE-30. On the contrary, in Figure 26, due to more lines and nodes need to be traverse, the variation ratio of transmission efficiency of IEEE-118 is obviously much higher than the ratio of IEEE-30, which suggests that the transmission efficiency in IEEE-118 is much more unstable. The reason why IEEE-118 is not stable in transmission efficiency is that it holds more nodes and lines. Hence, if a line or node is removed, the influenced nodes and lines are much more than the influenced nodes and lines in IEEE-30.
5.2.3. Structural Vulnerability Result Analysis by Comparing IEEE-30 with IEEE-118

Here, this paper proposes rates of indexes in IEEE-118 divided by indexes in IEEE-30 with the number of attacked times from 1 to 10. Thus, it is much easier to see the difference of results between the two examples. The results in Figure 25 show that the percentage of load loss of IEEE-118 is clearly much smaller than the percentage of load loss of IEEE-30, proving that bigger network IEEE-118 usually is more stable and reliable than the IEEE-30. On the contrary, in Figure 26, due to more lines and nodes need to be traverse, the variation ratio of transmission efficiency of IEEE-118 is obviously much higher than the ratio of IEEE-30, which suggests that the transmission efficiency in IEEE-118 is much more unstable. The reason why IEEE-118 is not stable in transmission efficiency is that it holds more nodes and lines. Hence, if a line or node is removed, the influenced nodes and lines are much more than the influenced nodes and lines in IEEE-30.

Figure 24. Variation ratio of network transmission efficiency of IEEE-118 bus system under extreme weather.

Figure 25. Rate of percentage of load loss under the three set attack modes.
5.2.4. Comparison with Other Literatures

To evaluate the efficiency of this structural vulnerability result, it is an absolute necessity to compare this result with results from the other similar literature. In the case of utilizing the previous result, here this paper draws the diagram of IEEE-30 without extreme weather with the diagram calculated in literature [62]. Since literature [62] only uses centrality-based attacks which are utilized to remove the nodes with the highest centrality score, it is only possible to compare its result with the result of our betweenness attack with or without extreme weather as a condition. In [62], the highest centrality scores are the node with the highest degree, which is similar to betweenness in our paper, but betweenness is much more complicated for considering weighted and directed condition in Section 3. [62] considers the centralized attack modes of IEEE-30. The centralized parameter is related to betweenness and other indexes mentioned in the paper. We decided to compare the centralized attack result with our result of betweenness attack mode and get the results shown in the following diagram. It can be seen in Figure 27 that although the results from the start are different, the two load loss indexes of the two modes are getting closer and closer as the number of attacked nodes rises, proving that the result is reliable and applicable. Since the centralized attack is one improved attack mode based on betweenness in [62], there are relations for their common features. The results of IEEE-30 show close value of load loss, which proves that the betweenness in this paper and in the literature [62] are quite relative and effective. However, there are also differences for the two papers aimed at different topics, indicating that the betweenness has bigger impacts on load loss due to the extreme weather.

Figure 26. Rate of transmission efficiency under the three set attack modes.
Figure 28. Cascading failures as attacks happening.

6. Discussion

The results in IEEE-30 and IEEE-118 present high common features in trending. However, compared with IEEE-30, IEEE-118 is much stronger and more adjustable for holding more nodes and lines to manage. Furthermore, extreme cases cast greater impacts on the IEEE-30 than on IEEE-118. Extreme weather really influences the reliability much more after knowing the load loss after random reliability attacks of two systems. The main reason for this may be that in extreme weather a random attack may just occur in a fragile place, which is just influenced by extreme cases. In the future, the relationships between
extreme cases and random attacks may be the next part to explore. Still, load loss and transmission efficiency really act differently. The next future topic maybe the features in topological structural classifications of parameters.

Furthermore, the extreme weather used in this paper is partly from the cited work. The extreme weather model is not very innovative. In the future, we hope to establish the extreme weather model considering the features of the power grid.

7. Conclusions

Power grid topology modeling based on the complex network can reflect the connection structure of power grid units and better identify the structural vulnerability of different units. The degree of node and the weighted intermediate of nodes and lines are introduced as model characteristic parameters to analyze the topology characteristics of the power grid model more effectively. Based on the structural vulnerability model of cascading failure, we propose indexes to address the vulnerability including percentage of load loss and variation ratio of network transmission efficiency. Also, we propose a structural vulnerability model considering extreme cases and analyze the relationships between power loss and power load capacity. Finally, this paper designs a relative algorithm.

The example in this paper further verifies the necessity of analyzing the vulnerability of the power grid structure under extreme circumstances, and finds out

(1) Variation ratio of network transmission efficiency grows fast at the first 5 removed nodes both in IEEE-30 and IEEE-118. Vulnerability and betweenness attack caused load losses to shrink nearly 50% from IEEE-30 to IEEE-118, while the load loss caused by reliability attack only decreases 10%. It can be seen from Figures 18–26 that the power grid has good robustness against line random attack in extreme cases, and the percentage of load loss and the percentage of network transmission efficiency decline increase slowly in line random attack mode.

(2) The percentage of load loss and variation ratio of network transmission efficiency appear with higher values, considering extreme cases.

(3) Bigger network IEEE-118 usually performs more stably and reliably than the IEEE-30, with regard to load loss. However, the variation ratio of transmission efficiency of IEEE-118 is obviously much higher than the ratio of IEEE-30; the influenced nodes and lines are more in IEEE-118.

This paper analyzes the vulnerability of the power grid from a macroscopic perspective, ignoring the internal physical characteristics of the power grid and the dynamic characteristics of complex power grid systems. In future research, the combination of macro and micro will be considered to better study the influence of grid unit reliability on grid cascading failure.

Author Contributions: Conceptualization, B.X. and W.C.; methodology, X.T. and L.K.; validation, W.C.; formal analysis, B.X.; data curation, L.K.; writing—original draft preparation, X.T.; writing—review and editing, L.K., B.X. and W.C.; visualization, X.T.; supervision, X.T.; project administration, B.X. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The study used the open data.

Conflicts of Interest: The authors declare no conflict of interest.
## Nomenclature

| Symbol | Description                                                                 | SI (\ represents none) |
|--------|------------------------------------------------------------------------------|------------------------|
| $w_{ij}$ | Weight of edge $ij$                                                          | P.U.                   |
| $DIS_{ij}$ | The sum of the edge reactance included in the shortest path from node $i$ to $j$. | P.U.                   |
| $AL$ | Average distance of $DIS_{ij}$                                              | P.U.                   |
| $BT_v$ | Proportion of weighted shortest paths passing through a node in the network to all weighted shortest paths in the network | \                      |
| $BT_e$ | Proportion of weighted shortest paths passing through an edge in the network to all weighted shortest paths in the network | \                      |
| $\delta_{ij}$ | The number of shortest paths between node $i$ and node $j$.              | \                      |
| $\delta_{ij,v}$ | The number of shortest paths between node $i$ and node $j$ containing node $v$. | \                      |
| $\delta_{ij,e}$ | The number of shortest paths between node $i$ and node $j$ containing edge $e$. | \                      |
| $n_L$ | The number of sink nodes                                                    | \                      |
| $n_G$ | The number of source nodes                                                  | \                      |
| $k_i$ | The degree of node $i$                                                      | \                      |
| $AVED$ | The average degree of all node degree                                       | \                      |
| $L_j$ | the load of $j$th node                                                      | MV                    |
| $\eta_L$ | The ratio of the load of all normal operation sink nodes in the current power grid to the load of all nodes in the power grid in the initial state | \                      |
| $E$ | the average of the reciprocal distance between the network nodes of all node pairs in the power grid | \                      |
| $\eta_E$ | The ratio between the current network transmission efficiency $E$ and the initial network transmission efficiency $E_0$ | \                      |
| $L_{in}$ | Input energy                                                                | MV                    |
| $L_{out}$ | Output energy                                                               | MV                    |
| $S_{Rated}$ | Rated load capacity                                                       | MV                    |
| $S_{Limiti}$ | Limited rated load capacity                                                | MV                    |
| $a_0$ | Rated load capacity coefficient                                             | \                      |
| $a_1$ | Limited rated load capacity coefficient                                     | \                      |
| $wire_{xi}$ | Position of x-coordinate of line $i$ in topological graph                   | KM                    |
| $wire_{yi}$ | Position of y-coordinate of line $i$ in topological graph                   | KM                    |
| $EW_x$ | Position of x-coordinate of the extreme case                                | KM                    |
| $EW_y$ | Position of y-coordinate of the extreme case                                | KM                    |
| $r$ | Radius of impact range                                                      | KM                    |
| $\partial$ | Coefficient                                                               | \                      |
| $\lambda_I$ | Failure rate of extreme weather $I$                                         | \                      |
| $a_I$ | Coefficient of weather $I$                                                  | \                      |

## References

1. Kezunovic, M.; Dobson, I.; Dong, Y. Impact of extreme weather on power system blackouts and forced outages: New challenges. In Proceedings of the 7th Balkan Power Conference, Sibenik, Croatia, 10–12 September 2008; pp. 1–5. [CrossRef]
2. Panteli, M.; Mancarella, P. Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies. Electr. Power Syst. Res. 2015, 127, 259–270. [CrossRef]
3. Li, T.; Luo, B.; Liu, L.; Wu, T. Wind accident analysis of transmission line in China Southern Power Grid’s Coastal Regions. In Proceedings of the 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT), Changsha, China, 26–29 November 2015; pp. 1700–1704. [CrossRef]
1. Panteli, M.; Mancarella, P. Modeling and Evaluating the Resilience of Critical Electrical Power Infrastructure to Extreme Weather Events. *IEEE Syst. J.* 2015, 11, 1733–1742. [CrossRef]

2. Cadini, F.; Algardi, G.L.; Zio, E. A modeling and simulation framework for the reliability/availability assessment of a power transmission grid subject to cascading failures under extreme weather conditions. *Appl. Energy* 2017, 185, 267–279. [CrossRef]

3. Liu, Y. Short-term operational reliability evaluation for power systems under extreme weather conditions. In *Proceedings of the 2015 IEEE Eindhoven PowerTech*, Eindhoven, The Netherlands, 29 June–2 July 2015; pp. 1–5. [CrossRef]

4. Anvari, M.; Lohmann, G.M.; Wächter, M.; Milan, P.; Lorenz, E.; Heinemann, D.; Tabar, M.R.R.; Peinke, J. Short term fluctuations of wind and solar power systems. *New J. Phys.* 2016, 18, 063027. [CrossRef]

5. Pahwa, S.; Scoglio, C.M.; Scala, A. Abruptness of Cascade Failures in Power Grids. *Sci. Rep.* 2014, 4, 3694. [CrossRef]

6. Pan, Y.; Hu, Y.; Ruan, J.; Du, Z.; Liu, C.; Du, W. Analysis and Prevention of Main Natural Disasters of 500kV Transmission Lines in Central China Power Grid. *Electr. Power Constr.* 2012, 6, 37–42.

7. Kiel, E.S.; Kjølle, G.H. The impact of protection system failures and weather exposure on power system reliability. In *Proceedings of the International Conference on Environment and Electrical Engineering and 2019 IEEE Industrial and Commercial Power Systems Europe (IEEE/ I&CPES Europe)*, Genova, Italy, 10–14 June 2019; pp. 1–6. [CrossRef]

8. Jufri, F.H.; Widiputra, V.; Jung, J. State-of-the-art review on power grid resilience to extreme weather events: Definitions, frameworks, quantitative assessment methodologies, and enhancement strategies. *Appl. Energy* 2019, 239, 1049–1065. [CrossRef]

9. Matko, M.; Golobić, M.; Kontić, B. Reducing risks to electric power infrastructure due to extreme weather events by means of spatial planning: Case studies from Slovenia. *Utilities Policy* 2017, 44, 12–24. [CrossRef]

10. Albert, R.; Jeong, H.; Barabási, A. Error and attack tolerance of complex networks. *Nature* 2000, 406, 378–382. [CrossRef]

11. Chen, X.; Sun, K.; Cao, Y.; Wang, S. Identification of Vulnerable Lines in Power Grid Based on Complex Network Theory. In *Proceedings of the 2007 IEEE Power Engineering Society General Meeting, Tampa, FL, USA, 23 July 2007*; pp. 1–6. [CrossRef]

12. Arianos, S.; Bompard, E.; Carbone, A.; Xue, F. Power grid vulnerability: A complex network approach. *Chaos: Interdiscip. J. Nonlinear Sci.* 2009, 19, 013119. [CrossRef]

13. Pagani, G.A.; Aiello, M. The Power Grid as a complex network: A survey. *Phys. A Stat. Mech. Its Appl.* 2013, 392, 2688–2700. [CrossRef]

14. Cuadra, L.; Salcedo-Sanz, S.; Del Ser, J.; Jiménez-Fernández, S.; Geem, Z.W.; Cuadra, L.; Salcedo-Sanz, S.; Del Ser, J.; Jiménez-Fernández, S.; Geem, Z.W. A Critical Review of Robustness in Power Grids Using Complex Networks Concepts. *Energies* 2015, 8, 9211–9265. [CrossRef]

15. Li, Q.; Li, H.Q.; Huang, Z.M.; Li, Y.Q. Power system vulnerability assessment based on transient energy hybrid method. *Power Syst. Protect. Control.* 2013, 41, 1–6. [CrossRef]

16. Li, X.; Qi, Z. Impact of cascading failure based on line vulnerability index on power grids. *Energy Syst.* 2021, 1–26. [CrossRef]

17. Abedi, A.; Gaudard, L.; Romerio, F. Review of major approaches to analyze vulnerability in power system. *Reliab. Eng. Syst. Saf.* 2019, 183, 153–172. [CrossRef]

18. Johansson, J.; Hassel, H.; Zio, E. Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. *Reliab. Eng. Syst. Saf.* 2013, 120, 27–38. [CrossRef]

19. Ouyang, M. Comparisons of purely topological model, betweenness based model and direct current power flow model to analyze power grid vulnerability. *Chaos Interdiscip. J. Nonlinear Sci.* 2013, 23, 023114. [CrossRef]

20. Wei, X.; Gao, S.; Huang, T.; Bompard, E.; Pi, R.; Wang, T. Complex Network-Based Cascading Faults Graph for the Analysis of Transmission Network Vulnerability. *IEEE Trans. Ind. Inform.* 2018, 15, 1265–1276. [CrossRef]

21. Wang, W.; Song, Y.; Li, Y.; Jia, Y. Research on Cascading Failures Model of Power Grid Based on Complex Network. In *Proceedings of the 2020 Chinese Control and Decision Conference (CCDC), Hefei, China, 22–24 August 2020*; pp. 1367–1372. [CrossRef]

22. Carreras, B.A.; New, M.; Dobson, I.; Poole, A. Initial evidence for self-organized criticality in electric power blackouts. In *Proceedings of the 33rd Hawaii International Conference on System Sciences, Maui, HI, USA, 7 January 2000*; pp. 102–108. [CrossRef]

23. Cao, Y.; Jiang, Q.; Ding, L. Self-organized criticality phenomenon for power system blackouts. *Power Syst. Technol.* 2005, 15, Available. Available online: https://en.cnki.com.cn/Article_en/CJFDTotal-DWJS20051500.htm (accessed on 11 August 2021).

24. Dwivedi, A.; Yu, X. A Maximum-Flow-Based Complex Network Approach for Power System Vulnerability Analysis. *IEEE Trans. Ind. Inform.* 2011, 9, 81–88. [CrossRef]

25. Ren, Z.; Zhang, J.; Zhang, J. Calculation of failure rate of power equipments based on partial least square method. *Power Syst. Technol.* 2005, 5. Available online: https://en.cnki.com.cn/Article_en/CJFDTotal-DWJS200505002.htm (accessed on 11 August 2021).

26. Kim, C.J.; Obah, O.B. Vulnerability Assessment of Power Grid Using Graph Topological Indices. *Int. J. Emerg. Electr. Power Syst.* 2007, 8. [CrossRef]

27. Zhongwei, M.; Zongxiang, L.; Jingyan, S. Comparison analysis of the small-world topological model of Chinese and American power grids. *Autom. Electr. PowerSyst.* 2004, 15, 004. [CrossRef]

28. Chen, T.; Rong, J.; Yang, J.; Cong, G.; Li, G. Combining public opinion dissemination with polarization process considering individual heterogeneity. *Healthcare* 2021, 9, 176. [CrossRef]
32. Chen, T.; Peng, L.; Yang, J.; Kong, G. Analysis of User Needs on Downloading Behavior of English Vocabulary APPs Based on Data Mining for Online Comments. *Mathematics* 2021, 9, 1341. [CrossRef]

33. Chen, T.; Yin, X.; Peng, L.; Rong, J.; Yang, J.; Kong, G. Monitoring and Recognizing Enterprise Public Opinion from High-Risk Users Based on User Portrait and Random Forest Algorithm. *Axioms* 2021, 10, 106. [CrossRef]

34. Busby, J.W.; Baker, K.; Bazilian, M.D.; Gilbert, A.Q.; Grubert, E.; Rai, V.; Rhodes, J.D.; Shidore, S.; Smith, C.A.; Webber, M.E. Cascading risks: Understanding the 2021 winter blackout in Texas. *Energy Res. Soc. Sci.* 2021, 77, 102106. [CrossRef]

35. Dong, H.; Cui, L. System Reliability Under Cascading Failure Models. *IEEE Trans. Reliab.* 2015, 65, 929–940. [CrossRef]

36. Liu, B.; Li, Z.; Chen, X.; Huang, Y.; Liu, X. Recognition and Vulnerability Analysis of Key Nodes in Power Grid Based on Complex Network Centrality. *IEEE Trans. Circuits Syst. I* Express Briefs 2017, 65, 346–350. [CrossRef]

37. Li, K.; Liu, K.; Wang, M. Robustness of the Chinese power grid to cascading failures under attack and defense strategies. *Int. J. Crit. Infrastruct. Prot.* 2021, 33, 100432. [CrossRef]

38. Wang, J.-W.; Rong, L.-L. Robustness of the western United States power grid under edge attack strategies due to cascading failures. *Saf. Sci.* 2011, 49, 807–812. [CrossRef]

39. Ding, M.; Han, P. Vulnerability assessment to small-world power grid based on weighted topological model. *Chin. Society of Electr. Eng.* 2008, 28, 20. Available online: http://www.researchgate.net/publication/294297239_Vulnerability_assessment_to_small-world_power_grid_based_on_weighted_topological_model?ev=auth_pub (accessed on 11 August 2021).

40. Amriouni, M.H.; Aminifar, F.; Lesani, H. Towards Proactive Scheduling of Microgrids Against Extreme Floods. *IEEE Trans. Smart Grid* 2018, 9, 3900–3902. [CrossRef]

41. Gholami, A.; Aminifar, F. A hierarchical response-based approach to the load restoration problem. *IEEE Trans. Smart Grid* 2017, 8, 1700–1709. [CrossRef]

42. Shao, C.; Shahidehpour, M.; Wang, X.; Wang, X.; Wang, B. Integrated Planning of Electricity and Natural Gas Transportation Systems for Enhancing the Power Grid Resilience. *IEEE Trans. Power Syst.* 2017, 32, 4418–4429. [CrossRef]

43. Wang, Y.; Chen, C.; Wang, J.; Baldick, R. Research on Resilience of Power Systems Under Natural Disasters—A Review. *IEEE Trans. Power Syst.* 2016, 31, 1604–1613. [CrossRef]

44. Qi, N.; Cheng, L.; Jiang, Y.; Luo, J.; Sun, K.; Wang, D.; Wang, W.; Sun, W. Vulnerability Assessment Based on Operational Reliability Weighted and Preventive Planning. In Proceedings of the IEEE Sustainable Power and Energy Conference (iSPEC), Beijing, China, 21–23 November 2019; pp. 1749–1754. [CrossRef]

45. Fang, J.; Su, C.; Chen, Z.; Haishun, S.; Lund, P. Power system structural vulnerability assessment based on an improved maximum flow approach. *IEEE Trans. Smart Grid* 2016, 9, 777–785. [CrossRef]

46. Koc, Y.; Warnier, M.; Kooij, R.; Brazier, F. Structural vulnerability assessment of electric power grids. In Proceedings of the 11th IEEE International Conference on Networking, Sensing and Control, Miami, FL, USA, 7–9 April 2014; pp. 386–391. [CrossRef]

47. Albert, R.; Albert, I.; Nakarado, G.L. Structural vulnerability of the North American power grid. *Phys. Rev. E* 2004, 69, 025103. [CrossRef]

48. Bompard, E.; Pons, E.; Wu, D. Analysis of the structural vulnerability of the interconnected power grid of continental Europe with the Integrated Power System and Unified Power System based on extended topological approach. *Int. Transl. Electr. Energy Syst.* 2013, 23, 620–637. [CrossRef]

49. Bender, J.; Farid, A. Seismic vulnerability of power transformer bushings. *Eng. Struct.* 2018, 162, 1–10. [CrossRef]

50. Chang, L.; Wu, Z. Performance and reliability of electrical power grids under cascading failures. *Int. J. Electr. Power Energy Syst.* 2011, 33, 1410–1419. [CrossRef]

51. Zhang, L.; Lu, J.; Fu, B.-B.; Li, S.-B. A cascading failures model of weighted bus transit route network under route failure perspective considering link prediction effect. *Phys. A Stat. Mech. Its Appl.* 2019, 523, 1315–1330. [CrossRef]

52. Zscheischler, J.; Westra, S.;Hurk, B.J.J.M.V.D.; Seneviratne, S.I.; Ward, P.J.; Pitman, A.; AghaKouchak, A.; Bresch, D.N.; Leonard, M.; Wahl, T.; et al. Future climate risk from compound events. *Nat. Clim. Chang.* 2018, 8, 469–477. [CrossRef]

53. Brenna, M.; Faranda, R.S.; Leva, S. Dynamic analysis of a new network topology for high power grid connected PV systems. In Proceedings of the IEEE PES General Meeting, Minneapolis, MN, USA, 25–29 July 2010; pp. 1–7. [CrossRef]

54. Watts, D.J.; Strogatz, S. Collective dynamics of ‘small-world’ networks. *Nature* 1998, 393, 440–442. [CrossRef]

55. Abbott, S.; Watts, D.J. Small-Worlds: The dynamics of between order and randomness. *Am. Math. Mon.* 2000, 107, 664–668. [CrossRef]

56. Nima, A.; Masoud, E. Improving voltage security assessment and ranking vulnerable buses with consideration of power system limits. *Electr. Power Energy Syst.* 2003, 25, 705–715. [CrossRef]

57. Ubeda, J.; Allan, R. Sequential simulation applied to composite system reliability evaluation. *IEEE Trans. Power Syst.* 1994, 9, 81–86. [CrossRef]

58. Song, J.; Cotilla-Sanchez, E.; Ghanavati, G.; Hines, P.D.H. Dynamic Modeling of Cascading Failure in Power Systems. *IEEE Trans. Power Syst.* 2015, 31, 2085–2095. [CrossRef]

59. Newman, D.E.; Carreras, B.; Lynch, V.; Dobson, I. Exploring Complex Systems Aspects of Blackout Risk and Mitigation. *IEEE Trans. Reliab.* 2011, 60, 134–143. [CrossRef]
60. Alexandersson, H.; Tuomenvirta, H.; Schmith, T.; Iden, K. Trends of storms in NW Europe derived from an updated pressure data set. *Clim. Research* 2000, 14, 71–73. Available online: https://www.int-res.com/abstracts/cr/v14/n1/p71-73/ (accessed on 11 August 2021). [CrossRef]

61. Brostrom, E.; Soder, L. Modeling of Ice Storms for Power Transmission reliability Calculations. In Proceedings of the 15th Power Systems Computation Conference, Liege, Belgium, 22–26 August 2005; Available online: https://www.researchgate.net/publication/228896987_Modelling_of_ice_storms_for_power_transmission_reliability_calculations (accessed on 11 August 2021).

62. Chopade, P.; Bikdash, M. New centrality measures for assessing smart grid vulnerabilities and predicting brownouts and blackouts. *Int. J. Crit. Infrastruct. Prot.* 2016, 12, 29–45. [CrossRef]