New Energy Exploitation and Application
http://ojs.ukscip.com/journals/neea

Article

Topological Vulnerability Analysis of the Mexican Power Grid Using Complex Network Theory

Francisco Rivas-Dávalos [1,*], Jorge Sánchez-Jaime [2] and José Horacio Tovar-Hernández [1]

[1] Tecnológico Nacional de México / Instituto Tecnológico de Morelia, Av. Tecnológico 1500, Morelia, Michoacán 58120, México
[2] Tecnológico Nacional de México / Instituto Tecnológico de Toluca, Av Tecnológico 100-s/n, Agrícola, Metepec, 52149, México
[*] Correspondence: francisco.rd@morelia.tecnm.mx; Tel.: +52-4432-85-47-15

Received: 24 April 2024; **Revised**: 10 May 2024; **Accepted**: 15 May 2024; **Published**: 28 May 2024

Abstract: This study presents a pioneering analysis of the network properties within the Mexican power grid (MXPG). The study included the 400 kV and 230 kV grids. Both grids were analysed independently and as a single combined grid. Based on complex network theory, several topological metrics were calculated, and the vulnerability of the power grid to random failures and intentional attacks was investigated. The MXPG displays several features of small-world networks, namely, a large clustering coefficient and a small average shortest path length. The degree distribution reveals exponential behaviour. Additionally, it was found that the power grid is more vulnerable to targeted attacks on nodes with a high degree than to random failures. In general terms, this study illuminates the intricate structure of the Mexican power grid, shedding light on its structural vulnerabilities, crucial for informing future strategies aimed at enhancing its robustness against potential disruptions.

Keywords: complex; network; topology; vulnerability

1. Introduction

In recent years, a theme that has constantly emerged in the analysis and evaluation of network-based critical infrastructure is vulnerability. The analysis of infrastructure vulnerability consists of assessing the physical, operational and geographical characteristics of infrastructure components and their role in the system with which they interact in terms of fragility to disruptive events and the impact of these events on the condition of the infrastructure. Power grids are among the critical infrastructures that are essential for maintaining the functions of other sectors, such as telecommunications, transport and traffic, health, water, and food. For example, the collapse of a power supply during a hurricane can hinder disaster logistics that heavily depend on information and communication technologies. Also, emerging dangers, like deliberate assaults targeting the power grid—ranging from terrorist strikes to cyberattacks—are becoming increasingly prevalent. These novel threats capitalize on the system's vulnerable points, triggering cascading failures and extensive blackouts. When such incidents occur, the afflicted components often pose challenges for swift repairs, potentially causing prolonged disruptions in power supply.

Vulnerability assessment in power systems encompasses structural and operational vulnerability [1]. Structural vulnerability assessment examines how vulnerable points in the system's topology impact its operational state and grid characteristics. Conversely, operational vulnerability assessment focuses on changes in physical or operational attributes and their impact on the system's operational state when vulnerable points

https://doi.org/10.54963/neea.v3i1.260

fail. Hence, physical, operational, and structural characteristics are integrated into power system vulnerability assessment.

Complex networks are the skeletons of complex systems. Understanding the structure of a complex network is pivotal as it largely dictates the properties of the complex system it represents. While knowledge of this structure does not inherently ensure comprehension of system functioning, it is indispensable for advancing such understanding, including its structural vulnerability. Recent studies have delved into analysing the topological properties of real power grids to correlate them with system structural vulnerability. Notably, research grounded in the theory of complex networks has been prominent in this domain. References [2,3] offer comprehensive reviews of literature on power network topology and vulnerability analysis, highlighting numerous works employing purely topological approaches for structural vulnerability analysis in power grids. Herein, we delve into select seminal works to furnish background in the field.

Topology analysis methods include the following metrics: average shortest-path length, network efficiency, clustering coefficient, and the size of the largest component. These topological measures have been used in vulnerability analyses of the following power grids: the European power grid [4], the power grid of the USA [5,6], the IEEE 300-bus power grid [7], the Italian power grid [8], and the Nordic power grid [9]. Additionally, several studies have attempted to characterize network topology by identifying common structures or patterns in different networks. For example, the work in [10,11] suggested that the degree distribution of power grids seems to follow a power law distribution function, which is a characteristic of scale-free networks. However, exponential cumulative degree distribution functions are found in the California power grid [12], the whole US power grid [13], and thirty-three different European transmission power grids [14]. Additionally, small-world networks are found in power grids such as the Shanghai [15], the Italian 380 kV, the French 400 kV, the Spanish 400 kV [4], and the Nordic power grids [9].

The operational vulnerability of the Mexican power grid (MXPG) (see Figure 1) has been extensively assessed; however, there has been a notable absence of topological vulnerability analysis. Mexico's geographical location renders it susceptible to frequent hurricanes, placing it among the top five countries affected by such natural disasters [16]. Consequently, numerous regions within the MXPG experience recurring disturbances and severe disruptions due to these hurricanes. Moreover, Mexico ranks as one of the most seismically active nations globally, with earthquakes frequently impacting its power network. Compounding these challenges is Mexico's status as the second most targeted country in Latin America for cyberattacks, with energy companies bearing the brunt of 32% of these attacks. These direct threats pose significant risks to both the physical and structural integrity of the power network. Given the aforementioned perils faced by the power grid and the dearth of studies addressing its structure, conducting topological analysis and structural vulnerability assessment of the MXPG becomes imperative.

This paper presents the first topology and vulnerability analysis of the MXPG using measures and concepts of complex network theory. Three networks derived from the MXPG are analysed. Two of them correspond to the transmission systems of 400 kV and 230 kV, and the third one is the transmission system with both voltage levels. The topological properties of the three networks are analysed using complex network theory. A vulnerability analysis is performed to determine their tolerance to random failures and intentional attacks on the most connected nodes.

This study presents three primary contributions. Firstly, it conducts the inaugural topological analysis of the 400 kV and 230 kV power networks within the MXPG. This analysis aligns with the prevailing trend of expanding topological evaluations across diverse power systems, as evidenced in literature. Secondly, it unveils the hitherto unknown topological characteristics of the MXPG, augmenting the existing understanding of the system alongside previously documented operational studies. Thirdly, it evaluates the topological vulnerability of the MXPG under scenarios of component failure, whether induced by random occurrences or deliberate attacks.

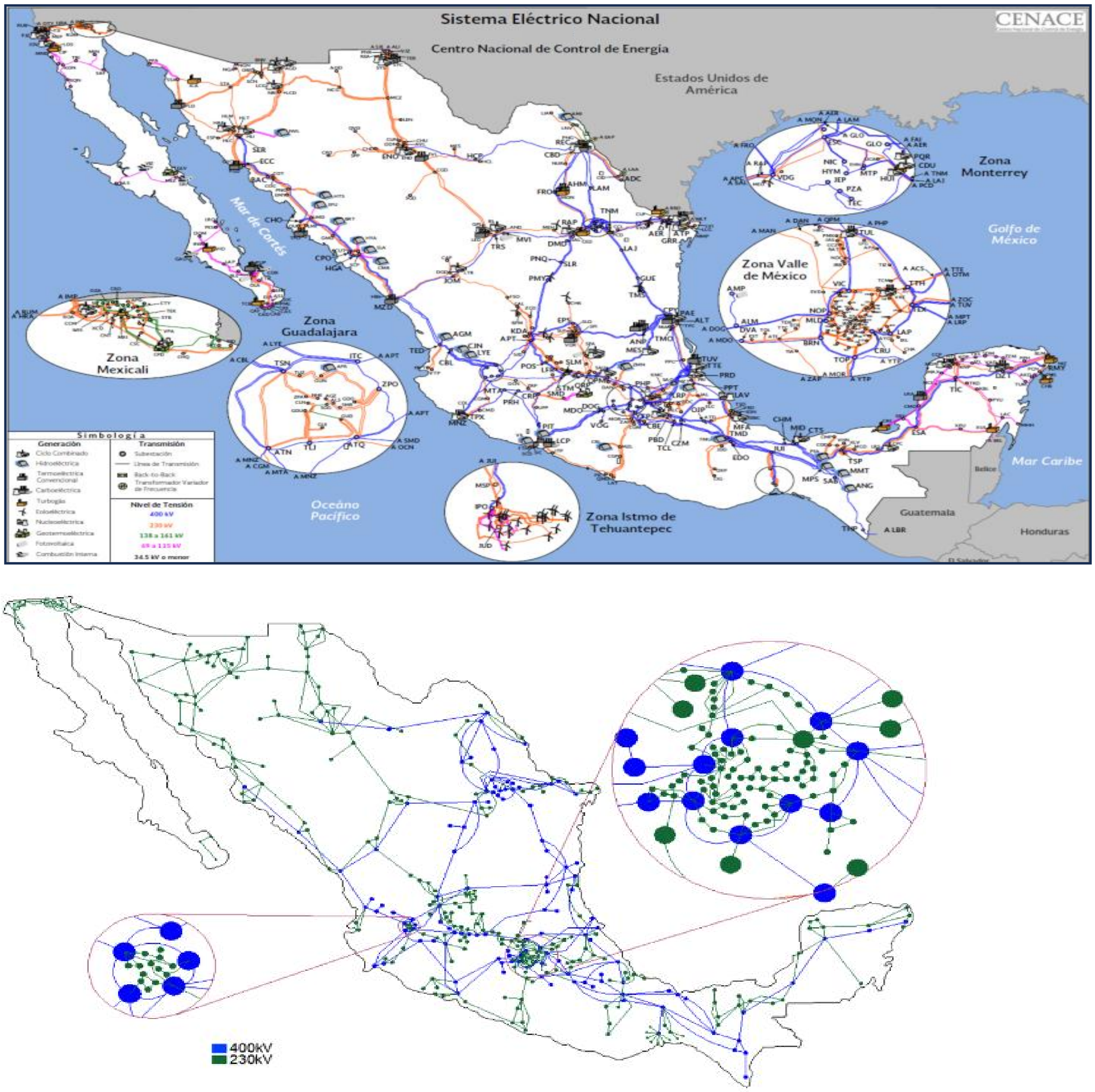


Figure 1. The Mexican power grid. Above, the National Electric System; below, the 400 kV and 230 kV power grids.

2. Complex Network Theory and Representation of Power Grids

2.1. Complex Network Theory

In general, the structure of complex systems can be viewed as complex networks. One of the most characteristic features of complex systems is that some of their properties are not deduced directly from the individual properties of their components. Another characteristic feature of these systems is their networked character, which justifies the use of networks in their representation in a natural way [17]. Modern power systems, also referred to as large-scale power grids, are a typical class of complex systems.

The basic purpose of complex network theory is to describe the form and functionality of real-world complex systems by modelling them as networks and using different measures. Complex network theory methods can be applied to the analysis of power systems for (i) performing preliminary assessments of vulnerabilities by topological and dynamical analysis and (ii) providing elementary information for further detailed analyses of critical areas [18].

The topological structure of electric power grids is an important consideration since it can dramatically influence performance. This is why topological analysis based on complex network theory is quite valuable because it can reveal relevant properties of the structure of a network system by identifying components of structural vulnerability, i.e., network lines and nodes whose failures can induce severe structural damage to the network through the physical disconnection of its parts [18].

2.2. Network Representation of Power Grids

The structure of a power grid is a network in which nodes represent stations (generators, transmission substations, and loads) and links represent the transmission lines between the nodes.

Graph theory provides a natural framework for the mathematical representation of power grids. A network, or graph, is described by $G = (N, M)$, where N is the set of nodes and M is the set of links. Any given network can be uniquely represented by an $N \times N$ adjacency matrix, A. If there exists a link from node i to node j, then element a_{ij} is 1; otherwise, it is 0. Several structural properties of networks are related to adjacency relationships between nodes. By analysing the structure of the network or by assessing the properties of the network when it is changed or degraded due to component failures or deliberate attacks on components, relevant conclusions about the modelling of the power system can be drawn. In this work, six main topological network property metrics are covered.

2.3. Network Topological Metrics

2.3.1. Size

Network size is the most basic metric when describing network structure. The network size is defined by the number of nodes, N, and the total number of links, M.

2.3.2. Node Degree

The node degree (k) is defined as the number of links connected to each node. The idea behind the use of node degree as a network property is that a node is more central or more influential than another node in a network if the degree of the first node is greater than that of the second node.

2.3.3. Degree Distribution

Since the nodes in a given electrical power network do not all have the same degree, the node degree alone is not enough to characterize the network. The degree distribution (that is, the probability that a randomly selected node has exactly k links) provides a better approach for explaining network topology. Several studies have discussed whether the degree distribution in power grids follows a power law or an exponential function. In the power-law degree distribution, the probability of finding a high-degree node is relatively small in comparison with the high probability of finding low-degree nodes (that is, the probability of a node having k links attached to it decays as a negative power of the degree: $p(k) \sim k^{-\alpha}$) [17]. Additionally, these networks are also referred to as 'scale-free' networks since the degree distribution is always characterized by the same scale α, irrespective of sample size. With respect to vulnerability, scale-free methods are robust against random failure but vulnerable to targeted attacks. Exponential-degree distributions are characterized by having a faster decay to zero than power laws, which means that the probability of having nodes with a high degree is slightly greater in scale-free networks [19].

2.3.4. Average Shortest-Path Length

In an undirected network, the shortest path distance l_{ij} is the number of links in the shortest path between nodes i and j. The average shortest-path length (the average of the shortest distance l_{ij} between all pairs of nodes) and network diameter (the maximum shortest path) characterize the distances among nodes globally for a network. The average shortest-path length is calculated with Equation (1):

$$\langle l \rangle = \frac{1}{N(N-1)} \sum\nolimits_{i,j \in N, i \neq j} l_{ij} \tag{1}$$

2.3.5. Clustering Coefficient

The clustering coefficient quantifies the degree to which nodes are clustered in a graph. Suppose a node i is connected to k_i other nodes or neighbours. Then, the clustering coefficient for a given node i is defined with Equation (2):

$$\langle l \rangle = \frac{1}{N(N-1)} \sum\nolimits_{i,j \in N, i \neq j} l_{ij} \tag{2}$$

where M_i and k_i are the number of links connected to node i and the node degree of node i, respectively.

A clustering coefficient equal to 1 indicates that every neighbour of node i is connected to every other neighbour of node i. Correspondingly, for the whole network, the clustering coefficient C is defined as the average of the clustering coefficients of all nodes as shown in Equation (3):

$$C = \frac{1}{N} \sum_{i} C_i \tag{3}$$

Additionally, in this case, the clustering coefficient is 1 only when the network is completely connected (all pairs of nodes are directly connected by a link). In general, the clustering coefficient is always less than one [15].

2.3.6. Global Network Efficiency

Global network efficiency represents the ease with which a graph can transmit information from node i to node j, which depends on its shorter path length. This metric is frequently used to measure the vulnerability of a network when simulating random failures and intentional attacks on critical nodes, and is defined as shown in Equation (4) [20]:

$$E_{global} = \frac{1}{N(N-1)} \sum\nolimits_{i,j \in N.\, i \neq j} \frac{1}{l_{ij}} \tag{4}$$

3. The Studied Networks of the Mexican Power Grid

In this work, three networks from the Mexican power grid were analysed. Two of them correspond to transmission systems of 400 kV (MX400) and 230 kV (MX230), and the third one is a transmission system with both voltage levels (MX400-230).

These networks were obtained by extracting information from the official document National Electrical System Development Program 2017–2031 (PRODESEN, for its acronym in Spanish) [21]. Transmission systems with other voltage levels and three isolated systems located in the peninsula of Baja California were not considered in this work. To analyse these networks, three graphs were generated. The power plants and substation buses (transformers and switching stations) were represented as nodes, and the transmission lines were represented as links. Since the focus of the analysis is on the grid topology, the links and nodes were considered homogeneous, unweighted and undirected (see Figure 2).

For a better illustration of the power networks under study, the green nodes and links form the MX230 network graph, and the blue nodes and links correspond to the MX400 network graph. It can also be seen that there are blue nodes within the MX230 graph, which are the ones that interconnect with the MX400 network graph; in this way, the third graph is formed that corresponds to the MX400-230 network (see Figure 1).

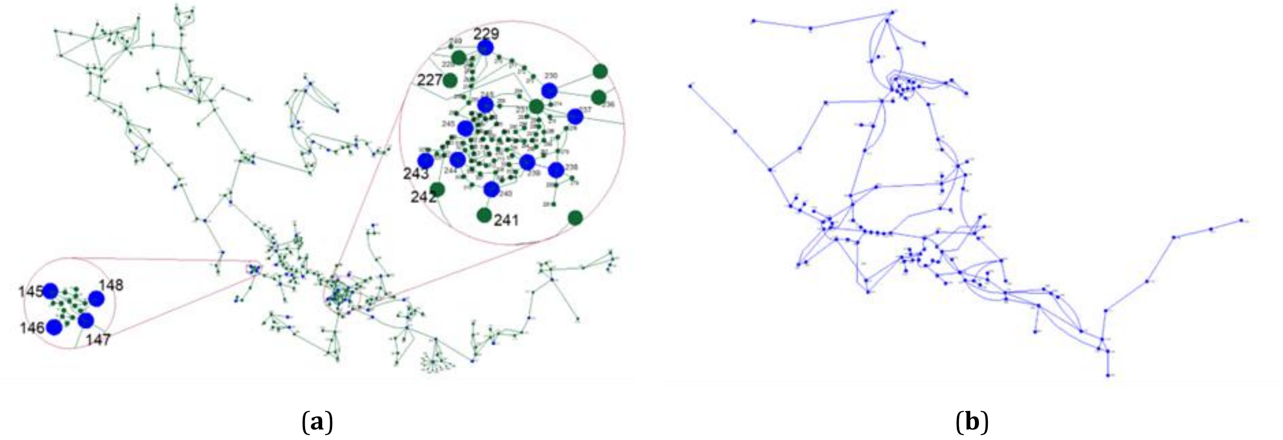


Figure 2. Graph representation of the studied Mexican power networks: (**a**) 230kV; (**b**) 400kV.

4. Topological Properties of the Mexican Power Grid

4.1. Size

The size of the MX400-230 network was compared with the size of the power networks of other countries (see Table 1). The Mexican network is the smallest (N = 429 and M = 612), whereas the largest is the French network. Although the precise factors that determine the number of nodes and lines in the power grid of each country have not been clearly identified, the network size is closely related to electricity consumption.

4.2. Average Node Degree and Degree Distribution

With respect to the values of the average node degree parameter $\langle k \rangle$, it is clear that these values are very similar for all the networks of the different countries in Table 1. This characteristic feature has been found in most power networks worldwide. Table 1 also shows that the 400 kV networks have greater average node degrees than the 230 kV networks. This might be explained by considering that the higher the voltage level is, the greater the network connectivity required since the amount of energy that is transmitted in a power network grows with the voltage level, as mentioned above.

Table 1. Some topological properties of the three MX networks compared to those of some European networks. (N: number of nodes, M: number of lines, $\langle k \rangle$: average node degree, $\langle l \rangle$: average shortest-path length. C: clustering coefficient, d: network diameter).

Country	N	N_{230}	N_{400}	M	M_{230}	M_{400}	$\langle k \rangle$	$\langle k_{230} \rangle$	$\langle k_{400} \rangle$	$\langle l \rangle$	$\langle l_{230} \rangle$	$\langle l_{400} \rangle$	C	C_{230}	C_{400}	d	d_{230}	d_{400}
Mexico	429	367	120	612	468	160	2.85	2.55	2.66	10.62	19.11	8.23	0.179	0.172	0.114	32	50	25
France	1659	1273	386	2160	1479	477	2.59	2.32	2.42	12.17	23.69	8.86	0.071	0.061	0.026	30	54	20
Spain	798	597	201	1115	731	284	2.79	2.45	2.83	10.45	13.90	7.63	0.091	0.103	0.097	24	40	18
Italy	634	372	262	812	437	321	2.53	2.35	2.40	11.98	10.17	9.62	0.046	0.055	0.050	32	30	27
Germany	782	302	480	1090	341	671	2.58	2.12	2.57	12.19	9.58	11.20	0.127	0.119	0.153	29	26	26

The degree distribution of the three MX networks, plotted in Figure 3, peaks at approximately $k = 2$ (most of the nodes have node degree k = 2), but there is a large number of nodes with node degree $k > 2$.

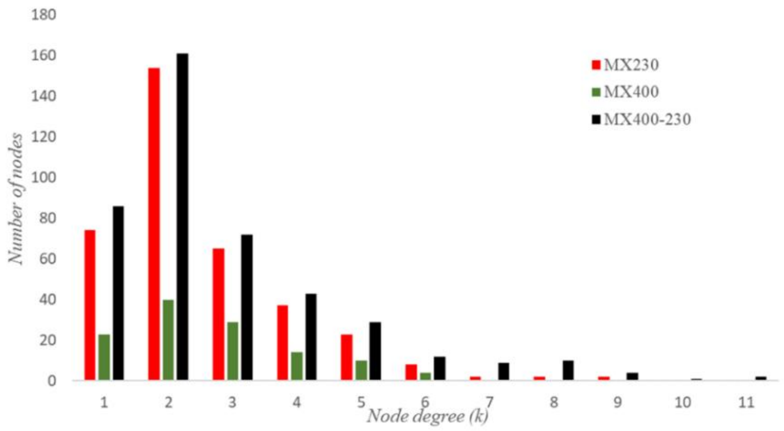


Figure 3. Node degree distribution of the three MX networks.

This implies that a failed substation disconnected from the network can easily be overtaken through other paths in the system. Nodes with $k = 1$ are the boundary substations of the three power transmission networks. Node degree is a measure that has been widely used in studies of different types of complex networks to assess the importance or level of influence of nodes on the performance of a given network. In the particular case of electric power grids, for example, there are studies based on node degree that seek to identify critical nodes that are able to cause the propagation of large-scale cascading failures [22]. Other studies have focused on using this measure to design strategies to restore the power system after a blackout problem [23]. This is why this measure is still used in topology analysis of power systems.

Figure 4 shows the cumulative degree distribution $P(k \geq K)$ of the three MX networks. For each network, the cumulative degree distribution follows an exponential function with (fitting) coefficient of determination R^2 values acceptably large.

According to reference [24], the cumulative degree distributions of the networks shown in Table 1 also follow an exponential function. The β values of these functions range between −0.37 and −0.64. The β value for the MX400-230 network is −0.55, which is within that range. As Figure 4 shows, the smaller the β *is*, the faster the decline; therefore, the probability of finding nodes with a high degree decreases.

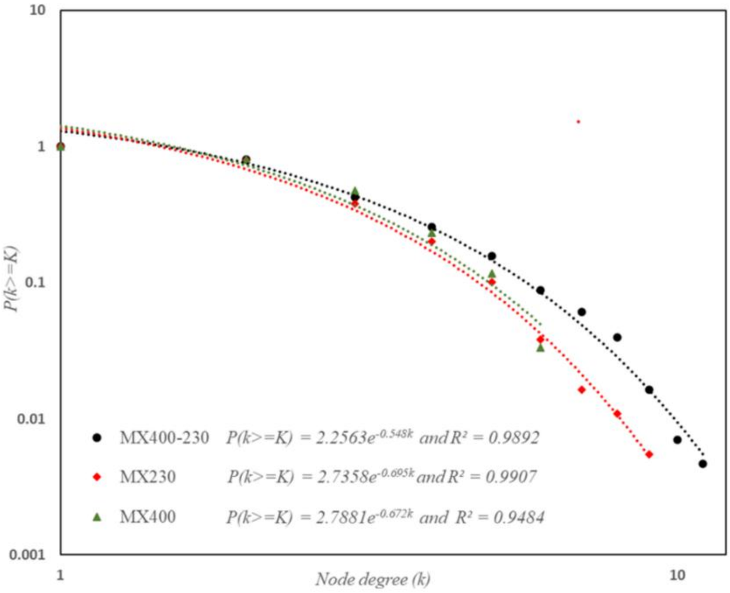


Figure 4. Exponential cumulative degree distribution of the three MX networks.

Additionally, although there is a significant size difference between the MX400 and MX230 networks, their cumulative degree distributions are very close to each other. This implies that there is no mathematical relation between β and network size. Finally, the implication that the cumulative degree distributions of the three MX networks are approximated by exponential functions is that the probability of having high-degree nodes is less than that in a scale-free network.

4.3. Average Shortest Path Length

In the case of network distances among nodes, all the 230 kV networks in Table 1 have greater network diameters and average shortest-path lengths, except for the network of Germany, compared with the 400 kV networks. Generally, in almost any power system construction, 230 kV lines are built to connect distances lower than 400 kV lines. Therefore, the diameter and average shortest path length of the 230 kV networks are larger than those of the 400 kV networks.

In most electric power grids, the distribution of the shortest path lengths follows a quasinormal distribution. However, in some cases, distances spread out to larger values, with a positive skewness [19]. Here, for the case of the MX400–230 network, Figure 5 shows its shortest-path length distribution *P(l)*, which has a tail up to 32, implying that one has to pass at most through 32 nodes for the power to be transmitted from one point to another in the network. This value is the diameter of the network.

Additionally, in Figure 5, the largest portion of the distribution is concentrated around values of 4 and 14, and the distribution peaks at 8, implying that the connectivity of this network is high. Theoretically, for any network, the average shortest-path length is bounded as $1 \leq \langle l \rangle \leq (N+1)/3$, where the lower bound is obtained for the complete network (fully connected network) and the upper bound is reached for the path of N nodes. For the MX400–230 network, an average shortest path length $\langle l \rangle = 10.62$ is found. This clearly reflects that the network has good global connectivity properties. In fact, all networks shown in Table 1 have good global connectivity properties, where the French network has the highest connectivity.

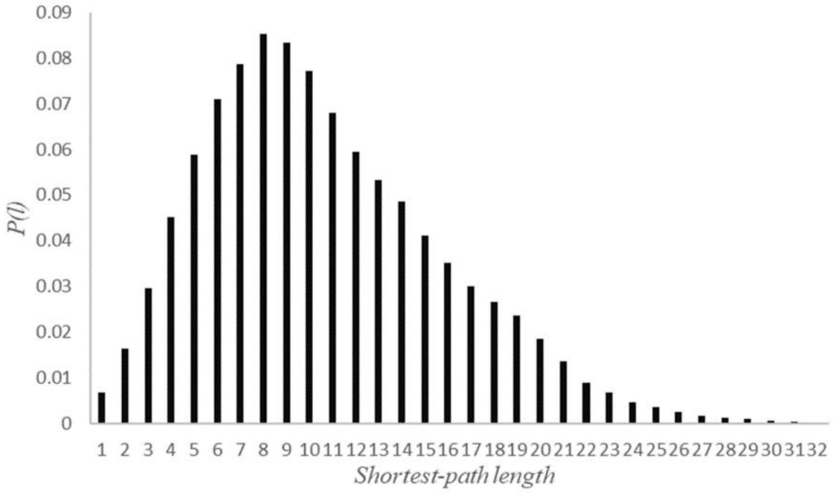


Figure 5. Shortest-path length distribution of the MX400-230 network.

4.4. Clustering Coefficient

Another measure that quantifies the connectivity in a network is the clustering coefficient C. Large values of C are better for the robustness of the connectivity. The disconnection of two parts of the network by node removal can be overcome by simply passing onto adjacent working nodes through short-range neighbouring nodes. In this view, comparing the networks in Table 1, the MX400-230 and MX230 networks had the highest clustering coefficients.

Additionally, for the MX400–230 network, most of the nodes have no links connecting their neighbours (C_i is zero), as shown in Figure 6. Nonetheless, the percentage of nodes with all their neighbours connected (C_i = 1) is above 10%, which can be considered a high value for an electric power grid.

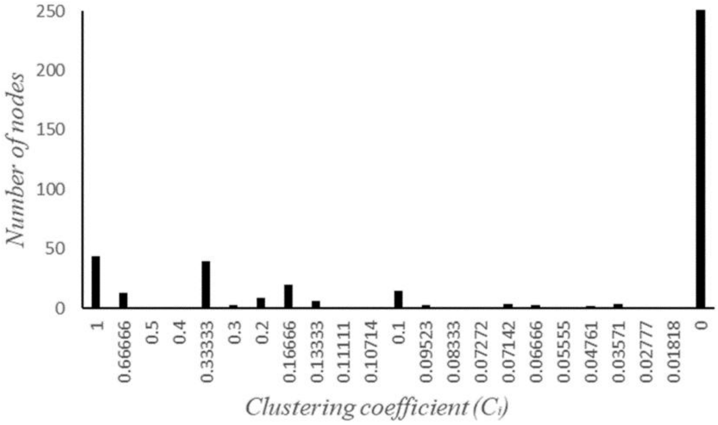


Figure 6. Distribution of the local clustering coefficient values of the MX400-230 network.

4.5. Testing the "Small-Worldness" of the Mexican Power Grid

To fully understand the structure of a power grid, it is essential to have reference network models for comparison. By utilizing random models of the three MX networks, we can analyze the influence of the topological parameters reported in Table 1 on the power grid's structure. Three commonly utilized random network models serve as foundational frameworks for investigating real-world network systems. The first model, known as the Barabási-Albert network [10], embodies a power-law degree distribution and is often referred to as a Scale-Free network. The second model, the Erdős-Rényi random network (ER) [25], is a stochastic network formed by linking nodes with a specified probability p. The third model, the Watts-Strogatz small-world network (WS) [5], fosters connections between any two nodes via paths of relatively short length, scaling logarithmically with network size. Its construction begins with a lattice, followed by stepwise rewiring of links with a probability p.

Given the determination from the preceding Section 4.2 that the Mexican power grid does not conform to a scale-free network structure, this study proceeded to generate ER and WS random networks for comparative analysis (refer to Table 2).

Table 2. Comparison between the three MX network structures and random (ER) and small-world (WS) network models.

Metric	MX230			MX400			MX400-230		
	MX	**ER**	**WS**	**MX**	**ER**	**WS**	**MX**	**ER**	**WS**
N	367	344	367	120	109	120	429	409	429
M	468	474	734	160	158	240	612	617	858
$\langle k \rangle$	2.5504	2.7598	4	2.6667	2.8991	4	2.8531	3.0171	4
k_{max}	9	8	7	6	7	7	11	10	8
$\langle l \rangle$	19.1134	6.3074	5.0939	8.2324	4.881	3.8046	10.6258	5.7815	11.7063
d	50	50	10	25	25	7	32	32	11
C	0.1727	0.0057	0.1502	0.1147	0.0247	0.1179	0.179	0.0052	0.1877

The three MX power networks have clustering coefficients that are significantly larger than the clustering coefficients of the ER networks and very close to those of the WS networks. With respect to the average shortest-path length, the MX400-230 network and its corresponding WS network have very similar metrics, whereas in the MX400 and MX230 networks, their average shortest-path lengths are only somewhat larger than those of the corresponding WS networks. These results lead to the conclusion that the MXPG demonstrates a small-world phenomenon, which is present in the Watts-Strogatz model.

The high clustering that the MXPG structure exhibits provides efficient local distribution with paths that are locally short. Additionally, at the same time, the small average shortest-path length gives shortcuts between the local clusters. All these findings indicate that the small-worldness of the MXPG's structure benefits from a general robustness against attacks: the absence of large hubs that keep the network together improves reliability.

5. Vulnerability Analysis

In this study, the vulnerability of the MXPG under random failures and intentional attacks is analysed by calculating the decrease in global network efficiency. Additionally, critical nodes are identified by measuring the global network efficiency degradation due to the disconnection of one node at a time.

In Table 3, the values of the global network efficiency of the three MX networks are shown, and they are compared with those of several European power networks [4]. According to complex network theory, small-world networks have a high E_{global} corresponding to a low average shortest path length. Therefore, since Mexico's power grid demonstrates the small-world phenomenon, it can be said that these E_{global} values of the three MX networks are high. Figure 7 presents the impact of random failures (randomly removed nodes) and degree-based intentional attacks (large-degree removed nodes) on the global network efficiency of the three MX networks.

Table 3. Comparison between the global network efficiency of the three MX networks with those of some European power networks.

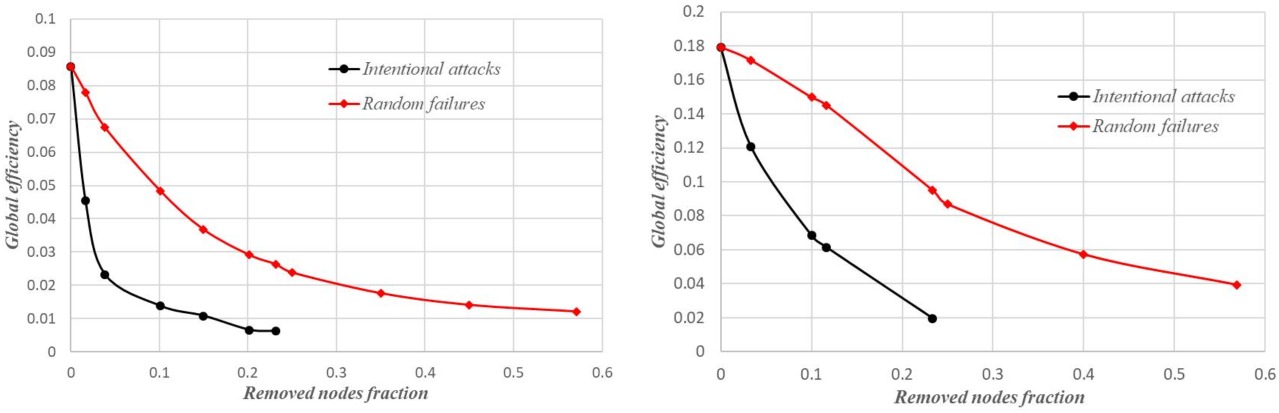
Network	E_{global}
Mexico MX230	0.0858
Mexico MX400	0.1793
Mexico MX400-230	0.1293
France 400kV	0.197
Spain 400kV	0.259
Italy 380kV	0.173
Swiss 220–380kV	0.205

The results indicate that all three networks are more robust against random failures than against intentional attacks. Analysing the MX400-230 network, after 10% of the nodes were randomly removed, the value of E_{global} was 0.115, whereas the global network efficiency reached almost zero for the case of intentional attacks with the same portion of nodes removed. This means that the impact of intentional attacks is more prominent than that of random failures.

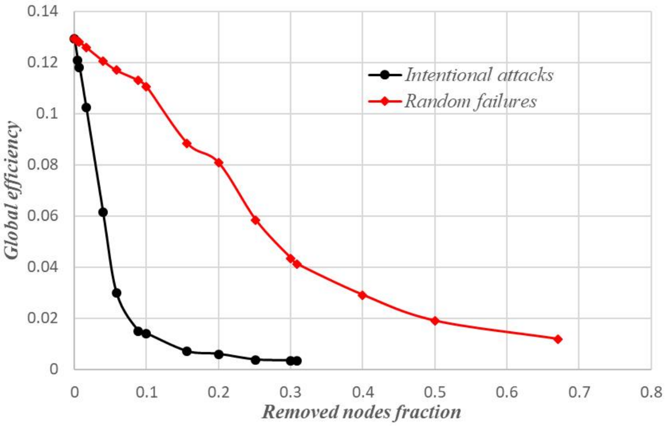
With respect to the identification of critical nodes, in this work, the criticality of a node is determined by estimating its vulnerability in terms of the relative decrease in the global network efficiency caused by its removal [20]. Thus, the vulnerability of a node is obtained with Equation (5):

$$V_i = \frac{\Delta E_{global}}{E_{global}} \tag{5}$$

where ΔE_{global} is the amount of change in global network efficiency when node i is removed from the network and E_{global} corresponds to the original network.



(a) (b)



(**c**)

Figure 7. Impact of random failures and intentional attacks of nodes on the global network efficiency of the three MX networks: (**a**) MX230, (**b**) MX400 and (**c**) MX400-230.

Figures 8 shows the histograms of node vulnerability values for the MX230, MX400 and MX400-230 networks. To explain these histograms, let us take the result of the MX230 network, whose histogram indicates that there are few nodes that cause a substantial change in the global network efficiency. For example, there are three nodes that reach a vulnerability value of 0.26, which means that the network has an efficiency loss of 26% if one of these nodes is removed (see Figure 8a) [21]. On the other hand, there are 77 nodes whose removal would not cause any global network efficiency loss, and even there are 71 nodes whose removal would represent an increase in the global network efficiency of up to 0.001. In these terms, Table 4 shows the most critical nodes for the three MGPGs.

Figure 9 shows the locations of the most critical nodes presented in Table 4. These nodes are identified as load and power substation types.

6. Conclusions

This study marks the first comprehensive unveiling of the network properties inherent to the Mexican power grid. The scale of the MX400-230 network was juxtaposed with analogous networks in other nations, revealing its 429 nodes and 612 connecting links. Notably, the 400 kV network exhibits higher average node degrees compared to their 230 kV counterpart. Analysis of cumulative degree distributions demonstrates their approximation by exponential functions, indicating a lower probability of high-degree nodes relative to scale-free networks. Moreover, the MX400-230 network boasts an average shortest path length of $\langle l \rangle = 10.62$, underscoring its robust global connectivity.

The observed clustering coefficients of the three MX power networks significantly surpass those of Erdős-Rényi networks and closely mirror those of Watts-Strogatz networks. Notably, the MX400-230 network aligns closely with its corresponding Watts-Strogatz counterpart in terms of average shortest-path length, suggestive of a small-world phenomenon akin to the Watts-Strogatz model.

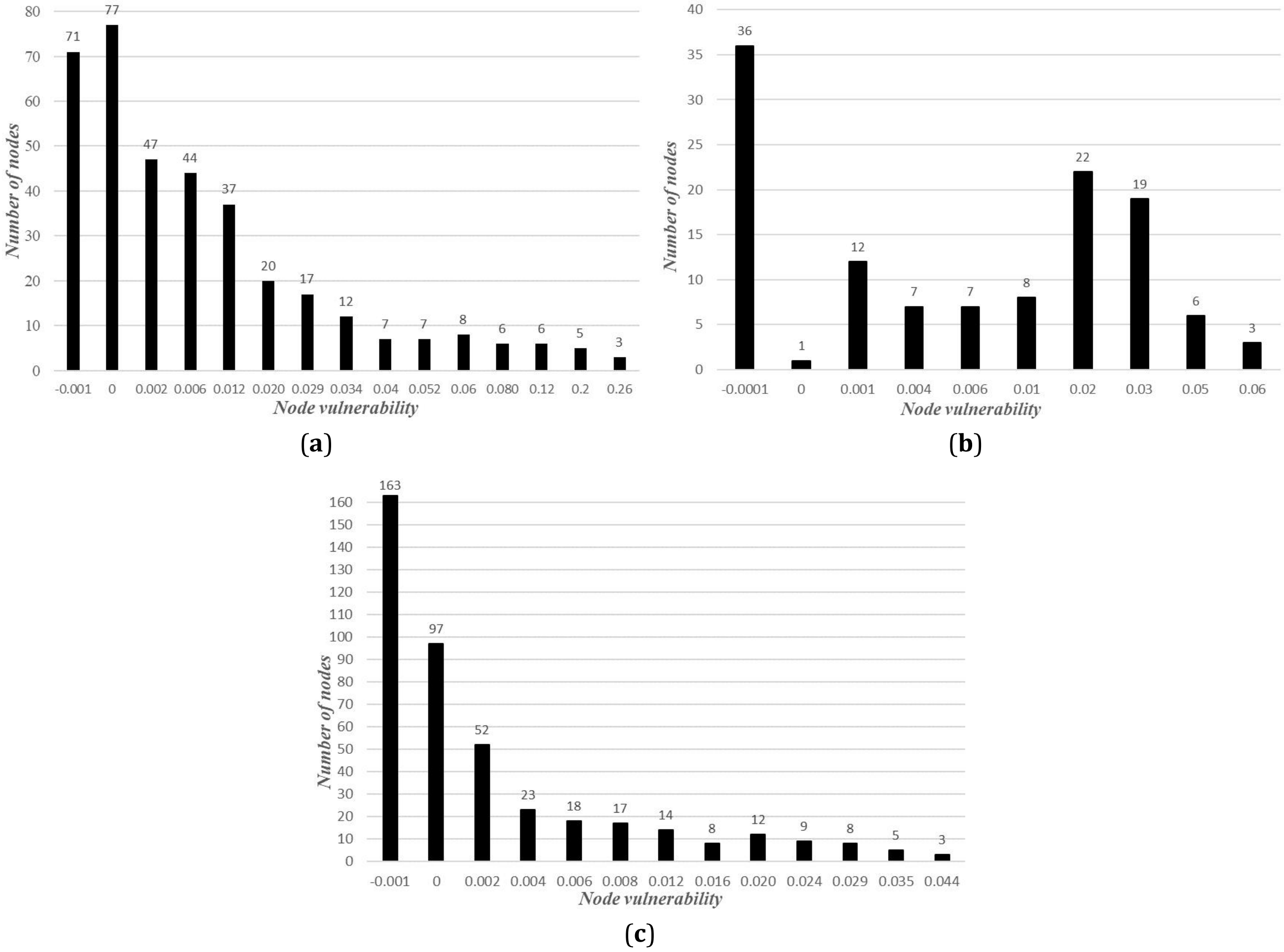


Figure 8. Histograms of node vulnerability defined as the percentage change in the global network efficiency when a node is removed from the network. (**a**) MX230; (**b**) MX400; (**c**) MX400-230.

Table 4. The three most critical nodes for the three MX networks in terms of E_{global} loss by removing them from the network.

Network	Most Vulnerable Nodes (Node Number)	E_{global} Loss in %	k	Node Type
MX230	200	26.0	4	Load
	220	26.1	2	Load
	221	26.6	3	Load
MX400	132	5.64	5	Power substation
	87	5.84	6	Power substation
	96	6.09	5	Load
MX400-230	239	4.1	8	Power substation
	231	4.1	9	Load
	385	4.4	7	Power substation

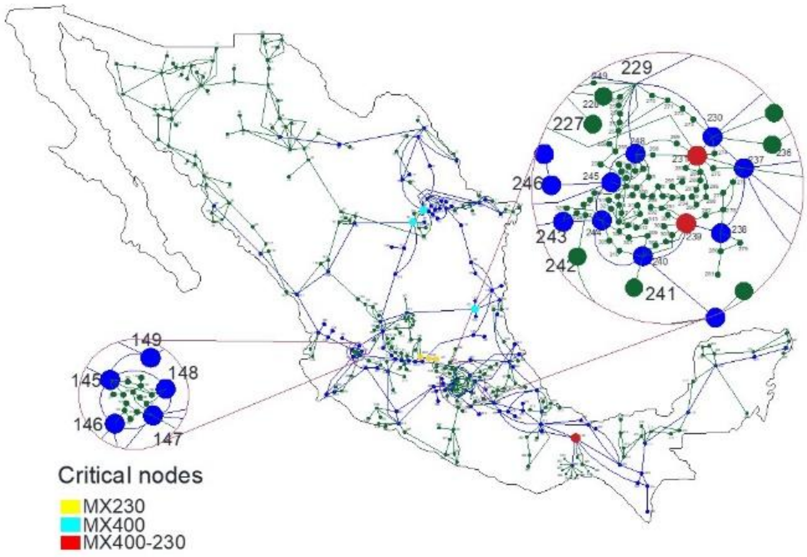


Figure 9. Location of the most critical nodes reported in Table 4.

The pronounced clustering within the MXPG facilitates efficient local distribution while maintaining locally short paths, a characteristic augmented by its small average shortest-path length, fostering shortcuts between local clusters. These attributes collectively underscore the MXPG's small-world structure, which enhances robustness against attacks by eschewing large hubs that traditionally stabilize networks, thus improving overall reliability.

Ultimately, the vulnerability of the MXPG against failures was assessed, revealing a greater susceptibility to intentional attacks than random failures. Notably, in the MX400-230 network, the impact of intentional attacks markedly eclipsed that of random failures, with intentional attacks yielding a near-zero global network efficiency following the removal of 10% of nodes, contrasting with a less severe reduction following random failures.

In summation, this analysis illuminates the intricate structure of the Mexican power grid, shedding light on its structural vulnerabilities, crucial for informing future strategies aimed at enhancing its robustness against potential disruptions.

Author Contributions

Conceptualization, F.R.-D. and J.S.-J.; methodology, F.R.-D. and J.S.-J.; software, J.S.-J.; validation, F.R.-D., J.S.-J. and J.H.T.-H.; formal analysis, F.R.-D. and J.S.-J.; investigation, F.R.-D. and J.S.-J.; writing—original draft preparation, F.R.-D.; writing—review and editing, F.R.-D., J.S.-J. and J.H.T.-H.

All authors have read and agreed to the published version of the manuscript.

Funding

This work received no external funding.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

Simulated data are available upon request.

Acknowledgments

J.S.-J. acknowledges PRODEP for the financial support to study Ph.D.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Abedi, A.; Gaudard, L.; Romerio, F. Review of Major Approaches to Analyse Vulnerability in Power System. *Reliab. Eng. Syst. Saf.* **2019**, *183*, 153–172. [CrossRef]
2. Amani, A.M.; Jalili, M. Power Grids as Complex Networks: Resilience and Reliability Analysis. *IEEE Access* **2021**, *9*, 119010–119031. [CrossRef]
3. Zang, T.; Wang, Z.; Wei, X.; Zhou, Y.; Wu, J.; Zhou, B. Current Status and Perspective of Vulnerability Assessment of Cyber-Physical Power Systems Based on Complex Network Theory. *Energies* **2023**, *16*, 6509. [CrossRef]
4. Rosato, V.; Bologna, S.; Tiriticco, F. Topological Properties of High-Voltage Electrical Transmission Networks. *Electr. Power Syst. Res.* **2007**, *77*, 99–105. [CrossRef]
5. Watts, D.J.; Strogatz, S.H. Collective Dynamics of 'Small-World' Networks. *Nature* **1998**, *393*, 440–442. [CrossRef]
6. Kinney, R.; Crucitti, P.; Albert, R.; Lator, V. Modelling Cascading Failures in the North American Power Grid. *Eur. Phys. J. B* **2005**, *46*, 101–107. [CrossRef]
7. Hines, P.; Cotilla-Sanchez, E.; Blumsack, S. Do Topological Models Provide Good Information about Electricity Infrastructure Vulnerability? *Chaos* **2010**, *20*, 033122. [CrossRef]
8. Crucitti, P.; Latora, V.; Marchiori, M. A Topological Analysis of the Italian Electric Power Grid. *Phys. A* **2004**, *338*, 92–97. [CrossRef]
9. Holmgren, Å.J. Using Graph Models to Analyse the Vulnerability of Electric Power Networks. *Risk Anal.* **2006**, *26*, 955–969. [CrossRef]
10. Barabási, A.L.; Albert, R. Emergence of Scaling in Random Networks. *Science* **1999**, *286*, 509–512. [CrossRef]
11. Wu, D.; Ma, F.; Javadi, M.; Thulasiraman, K.; Bompard, E.; Jiang, J.N. A Study of the Impacts of Flow Direction and Electrical Constraints on Vulnerability Assessment of Power Grid Using Electrical Betweenness Measures. *Phys. A* **2017**, *466*, 295–309. [CrossRef]
12. Amara, L.A.N.; Scala, A.; Barthelemy, M.; Stanley, H.E. Classes of Small-World Networks. *Proc. Natl. Acad. Sci. USA* **2000**, *97*, 11149–11152. [CrossRef]
13. Albert, R.; Albert, I.; Nakarado, G.L. Structural Vulnerability of the North American Power Grid. *Phys. Rev. E* **2004**, *69*, 025103. [CrossRef]
14. Rosas-Casals, M.; Valverde, S.; Solé, R.V. Topological Vulnerability of the European Power Grid Under Errors and Attacks. *Int. J. Bifurc. Chaos* **2007**, *17*, 2465–2475. [CrossRef]
15. Mei, S.; Zhang, X.; Cao, M. *Power Grid Complexity*; Springer: Berlin, Germany, 2011.
16. The Force of Nature in Mexico, as seen from space, 2015. World Space Week 2015 Exhibition. Available online: https://www.unoosa.org/oosa/en/informationfor/articles/the-force-of-nature-in-mexico--as-seen-from-space.html (accessed on 22 February 2024).
17. Estrada, E. Adjacency Relations in Networks. In *The Structure of Complex Networks: Theory and Applications*; Oxford University Press: New York, USA, 2011; Chapter 2, Section 2.2, pp. 27–30.
18. Fang, Y. Critical Infrastructure Protection by Advanced Modelling, Simulation and Optimization for Cascading Failure Mitigation and Resilience. Ph.D. Dissertation, Ecole Centrale Paris, Paris, French, 2 February 2015.
19. Espejo, R.; Lumbrera, S.; Ramos, A. Analysis of Transmission-Power-Grid Topology and Scalability, the European Case Study. *Phys. A* **2018**, *509*, 383–395. [CrossRef]
20. Monfared, M.A.S.; Jalili, M.; Alipour, Z. Topology and Vulnerability of the Iranian Power Grid. *Phys. A* **2014**, *406*, 24–33. [CrossRef]

21. Secretaría de Energía. Programa de Desarrollo del Sistema Eléctrico Nacional 2017–2031 (PRODESEN 2017-2031). Available online: https://base.energia.gob.mx/prodesen/PRODESEN2017/PRODESEN-2017-2031.pdf (accessed on 12 December 2023).
22. Fu, Y.; Ge, M.; Fan, Y.; Sun, X.; Zou, X.; Chen, Z. Identification of Critical Nodes in Power Grid Based on Node Traffic Importance Degree. *Mod. Electr. Power* **2018**, *35*, 1–8.
23. Power System Restoration Using Closeness Centrality and Degree of a Node. In Cigre Egypt 2019, Abbasia, Cairo, Egypt, 6–8 March 2019.
24. Costa, L.D.F.; Oliveira Jr, O.N.; Travieso, G.; Rodrigues, F.A.; Villas Boas, P.R.; Antiqueira, L.; Correa Rocha, L.E. Analysing and Modelling Real-World Phenomena with Complex Networks: A Survey of Applications. *Adv. Phys.* **2011**, *60*, 329–412. [CrossRef]
25. On the Evolution of Random Graphs. Available online: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=420173e087bca0bdb31985e28ff69c60a129c8ef (accessed on 15 February 2024).

Publisher's Note: The views, opinions, and information presented in all publications are the sole responsibility of the respective authors and contributors, and do not necessarily reflect the views of UK Scientific Publishing Limited and/or its editors. UK Scientific Publishing Limited and/or its editors hereby disclaim any liability for any harm or damage to individuals or property arising from the implementation of ideas, methods, instructions, or products mentioned in the content.