entropy

MDPI

Article

Analysis of Vulnerability on Weighted Power Networks under Line Breakdowns

Lixin Yang *, Ziyu Gu, Yuanchen Dang and Peiyan He

School of Mathematics & Data Science, Shaanxi University of Science and Technology, Xi'an 710021, China
* Correspondence: yanglixin@sust.edu.cn

Abstract: Vulnerability is a major concern for power networks. Malicious attacks have the potential to trigger cascading failures and large blackouts. The robustness of power networks against line failure has been of interest in the past several years. However, this scenario cannot cover weighted situations in the real world. This paper investigates the vulnerability of weighted power networks. Firstly, we propose a more practical capacity model to investigate the cascading failure of weighted power networks under different attack strategies. Results show that the smaller threshold of the capacity parameter can enhance the vulnerability of weighted power networks. Furthermore, a weighted electrical cyber-physical interdependent network is developed to study the vulnerability and failure dynamics of the entire power network. We perform simulations in the IEEE 118 Bus case to evaluate the vulnerability under various coupling schemes and different attack strategies. Simulation results show that heavier loads increase the likelihood of blackouts and that different coupling strategies play a crucial role in the cascading failure performance.

Keywords: complex network; cascading failure; vulnerability; redistribution rule

Citation: Yang, L.; Gu, Z.; Dang, Y.; He, P. Analysis of Vulnerability on Weighted Power Networks under Line Breakdowns. *Entropy* **2022**, *24*, 1449. https://doi.org/10.3390/e24101449

Academic Editors: Jaroslaw Krzywanski, Yunfei Gao, Marcin Sosnowski, Karolina Grabowska, Dorian Skrobek, Ghulam Moeen Uddin, Anna Kulakowska, Anna Zylka and Bachil El Fil

Received: 13 September 2022
Accepted: 5 October 2022
Published: 11 October 2022

1. Introduction

The electricity supply network is an essential part of the infrastructure of our modern society. A power network is a complex and highly interconnected network, consisting of generators, consumers, substations and transmission lines [1,2]. Furthermore, a power network must maintain its power distribution function even when a few elements are changed. Therefore, the robust operation of physical distribution across a power network is fundament for our daily life. In recent years, due to the environment and the economy, there exists a shift from using central power sources to using small power sources [3–7]. More and more renewable energies are becoming part of the power network in modern society. This leads to many challenges concerning a power system's ability to maintain its function under various conditions.

On the other hand, it has been noticed that transmission lines with large capacities can deliver heavier flows. Each line, however, has a finite capacity. In order for a line to function properly, its flow cannot be more than the capacity at all times. Therefore, when the power network is damaged by various attacks, for instance, the removal of some transmission lines, it may cause huge disturbances and cause a possible blackout [8–12]. Cascading failures in power networks are the main cause of large-scale blackouts, which cause substantial costs. For a power network, the dynamic cascading failure process can be regarded as a sequence of tripping events leading eventually to a power outage spreading over a very large area. Over the past few years, many researchers have investigated load models and analyzed cascading failures by the Kuramoto-like model [13–16]. Furthermore, most of this cascading failure model is related to the analysis of steady states because cascading failures often exhibit dynamical transients. In addition to this, in many real-world networks, there is a weight related to lines and nodes; a network is considered weighted when the larger the weight on a line or node, the harder this line or node is to fail.

Therefore, it is natural that the study of cascading failures in weighted power systems has been a very important topic in power electrical engineering. Wang et al. [17] constructed a cascading failure model with edge overloading for a weighted network and proposed a local weighted flow redistribution rule. Then, in [18], Wu et al. studied cascading failures in the BA network by the load on each node. Recently, S. Muldoon [19] et al. generated weighted small-world networks. In order to capture the relationship between the weighted feature and the cascading failures, this paper intends to put forward a nonlinear weighted flow redistribution rule and construct a cascading failure model.

In earlier work, researchers studied the cascading failures of the single-layer complex network. In [20], the authors proposed three resilience reinforcement strategies based on the nodal capacity redundancy at different structure scales. The performance of the reinforcement strategy had a close correlation with the nodal capacity redundancy. Many approaches analyze the vulnerability of power systems by removing components from the system and evaluate the resultant impact under different removing strategies [21]. Some studies use the Monte Carlo method to simulate all possible contingencies so that the most likely failed components can be identified [22].

However, in many practical situations, interdependent networks are ubiquitous in modern society. With the development of information technologies and power networks, the traditional power network gradually evolved to become cyber-physical interdependent networks [23–27]. More complex coupling formats may increase the vulnerability of the power network. Therefore, it is vital to investigate the cascading failures of interdependent networks. Buldyrev et al. [28] proposed a framework to analyze the robustness of an interdependent network. Later, Dong et al. [29] studied partially interdependent networks. In the previous model, they neglected some concrete engineering characteristics [30–32]. It is more feasible to analyze the structural vulnerability of interdependent power networks when combining the electrical engineering features with the complex network theory. Moreover, we generalize the betweenness concept to construct more practical cyber-physical interdependent networks. Moreover, we combine the proposed model with different coupling strategies to analyze the structural vulnerability under line breakdowns.

In this paper, we study the vulnerability in a weighted power network. In Section 2, we present a nonlinear model to analyze the cascading failure of a weighted power network, including a single-layer network and an interdependent network. Following that, Section 3 investigates the influence of coupling schemes and the mean degree of vulnerability of an interdependent network. Furthermore, the method is illustrated by examples of several power networks. Finally, conclusions and future work are provided in Section 4.

2. Cascading Failure Model for a Weighted Power Network

In this section, we focus on some existing networks to analyze the cascading failure process. The studied network ensembles are the single and interconnected weighted networks.

2.1. Single Weighted Power Network

In general, a power network is summarized as a directed and weighted network. Moreover, there is a weight associated with each link or node, the larger the weight on the link or node, the harder this line or node is to fail. The electrical distance between the generator and consumer is defined as the equivalent impedance, which considers the impedance of the transmission lines between them. Additionally, betweenness centrality is considered as the most representative of the topological properties. However, the pure topological concepts disregard the concrete engineering characteristics of a power network. Therefore, we refine the betweenness as the extended betweenness to construct the power network in this subsection. Based on the above-mentioned betweenness, a new nonlinear model is proposed for studying the vulnerability in the weighted power network with different topologies.

According to the electrical circuit theory, the contribution of the transmission line to the power transmission can be assessed using the power transfer distribution factors (PTDF). PTDF can be denoted by an $N_L \times N_B$ matrix F, where D, G, L denote the set of consumer nodes, generator nodes and transmission lines; $N_L = \dim(L), N_B = \dim(G)$, respectively. The element f_{ej} of the matrix express the change of power on each line e for a unit change of power injected at node i and delivered at the reference node. ${f_e}^{gd}$ represents the change of power on line e that is supplied at generator g and demanded at consumer d, and can be computed as follows:

$$ {f_e}^{gd} = f_{eg} - f_{ed}, e \in L \tag{1} $$

On the other hand, the power transmission line capacity is given by:

$$ C_g^d = \min_{e \in L} ({P_e}^{\max} / |f_e|^{gd}) \tag{2} $$

where ${P_e}^{\max}$ is the transmission limit of line e.

Based on the above specific characteristics of a power network, the extended betweenness of a node can be refined as:

$$ T(w) = \frac{1}{2} \sum_{g \in G} \sum_{d \in D} C_g^d \sum_{e \in L^w} \left| {f_e}^{gd} \right|, w \neq g \neq d \in B \tag{3} $$

where $\sum_{e \in L^w} \left| {f_e}^{gd} \right|$ represents the sum of the PTDFs of all lines connecting a node w when a unit of power supplied at node w and demanded at node d.

It is obvious that the extended betweenness might be close to reality in a power network. Hence, the weight of the nodes in this network depends on their extended betweenness.

First, we assume the node load j for weighted network, and the power distribution model is given by:

$$ L_j = (1 + \gamma) \left(s_i \sum_{j \in \Gamma_i} s_j \right) \tag{4} $$

where $\gamma > 0$ represents the load parameter, s_i denotes the weight of node i and Γ_j is the collection of neighboring nodes. Moreover, each node j has a threshold value, which is defined as:

$$ C_j = L_j + \alpha {L_j}^{\beta} \tag{5} $$

where $\alpha \in [0, 1], \beta \geq 0$ denote capacity parameters.

If a node fails, the neighboring nodes will receive the loads in proportion to its remaining capacity $\pi_j = \frac{C_j - L_j}{\sum_{j \in \Gamma_i} (C_j - L_j)}$, and the received additional load for node j from node i can be described as:

$$ \Delta L_{ij} = L_i \times \pi_{\mathrm{j}} == (1 + \gamma)(s_i \sum_{j \in \Gamma_i} s_j) \times \frac{(s_j \sum_{n \in \Gamma_j} s_n)^{\beta}}{\sum_{j \in \Gamma_i} (s_j \sum_{n \in \Gamma_j} s_n)^{\beta}} \tag{6} $$

when $L_j + \Delta L_{ij} > C_j$, the neighboring node j will also fail, and its load will be further distributed to its neighboring nodes, which may cause the failure of neighboring nodes and form a cascading failure. Only if $L_j + \Delta L_{ij} \leq C_j$, does node j not fail, and thus the cascade failure stop.

Based on the above analysis, it is obvious that the capacity parameters play a central role in the cascading failure of a power network. Thus, we define the threshold value of capacity parameter as α^*, which is the minimum value required to avoid a cascading failure.

That is, all node flows must be less than their threshold for the cascading failure to stop. In order to avoid a cascading failure, the inequality $L_j + \Delta L_{ij} \leq C_j$ must be satisfied.

In what follows, we substitute the load and capacity formula into the inequality:

$$L_j + L_i \times \frac{\alpha {L_j}^{\beta}}{\sum\limits_{j \in \Gamma_i} \alpha {L_j}^{\beta}} \leq L_j + \alpha {L_j}^{\beta} \tag{7}$$

One can thus obtain:

$$\frac{(1+\gamma)(s_i \sum\limits_{j \in \Gamma_i} s_j)(s_j \sum\limits_{n \in \Gamma_j} s_n)^{\beta}}{\sum\limits_{j \in \Gamma_i} (s_j \sum\limits_{n \in \Gamma_j} s_n)^{\beta}} \leq \alpha (1+\gamma)^{\beta} (s_j \sum_{n \in \Gamma_j} s_n)^{\beta} \tag{8}$$

We can further simplify and obtain:

$$\frac{(s_i \sum\limits_{j \in \Gamma_i} s_j)(s_j \sum\limits_{n \in \Gamma_j} s_n)^{\beta-1}}{\sum\limits_{j \in \Gamma_i} (s_j \sum\limits_{n \in \Gamma_j} s_n)^{\beta}} \leq \alpha (1+\gamma)^{\beta-1} (s_j \sum_{n \in \Gamma_j} s_n)^{\beta-1} \tag{9}$$

To explore the relationship between the capacity parameters, we define the conditional probability that the neighboring node of the node with power s' is $P(s'|s_i)$.

According to Bayesian formula, one can get:

$$\sum_{j \in \Gamma_i} s_j = \sum_{s'=s_{\min}}^{s_{\max}} s_i P(s'|s_i) s' \tag{10}$$

Additionally, the conditional probability satisfies the following equation:

$$P(s'|s_i) = s' P(s') / \langle s \rangle \tag{11}$$

Substituting Equations (10) and (11) into (9), we can see that:

$$\frac{s_i {s_j}^{2\beta-2} \langle s \rangle}{\langle s^{2\beta+1} \rangle} \leq \alpha (1+\gamma)^{\beta-1} \times \frac{{s_j}^{2\beta-2} \langle s^2 \rangle^{\beta-1}}{\langle s \rangle^{\beta-1}} \tag{12}$$

Furthermore, Equation (12) can be simplified as:

$$\alpha \geq \frac{s_i \langle s \rangle^{\beta}}{(1+\gamma)^{\beta-1} \langle s^2 \rangle^{\beta-1} \langle s^{2\beta+1} \rangle} \tag{13}$$

Then, the threshold α^* of the capacity parameter α is given by:

$$\alpha^* = \begin{cases} \frac{s_{\max} \langle s \rangle}{\langle s^3 \rangle}, \beta = 1 \\ \frac{s_{\max} \langle s \rangle \langle s^2 \rangle}{(1+\gamma)^{\beta-1} \langle s^{\beta+1} \rangle \langle s^{\beta+2} \rangle}, \beta \neq 1 \end{cases} \tag{14}$$

In order to further analyze the effect of the capacity parameter. We let:

$$Z = \frac{s_{\max} \langle s \rangle \langle s^2 \rangle (1+\gamma)^{1-\beta}}{\langle s^{\beta+1} \rangle \langle s^{\beta+2} \rangle} \tag{15}$$

We take the derivative of function (20) with respect to parameter β:

$$Z'(\beta) = \frac{-N^4 s_{\max}\langle s^2\rangle\langle s\rangle(1+\gamma)^{1-\beta}\ln(1+\gamma)}{\left(\sum_{i=1}^{N} s_i^{2\beta+3}\right)^2} - \frac{N^2(2\beta+3)\sum_{i=1}^{N} s_i^{2\beta+2} s_{\max}\langle s^2\rangle\langle s\rangle(1+\gamma)^{1-\beta}}{\left(\sum_{i=1}^{N} s_i^{2\beta+3}\right)^2} \tag{16}$$

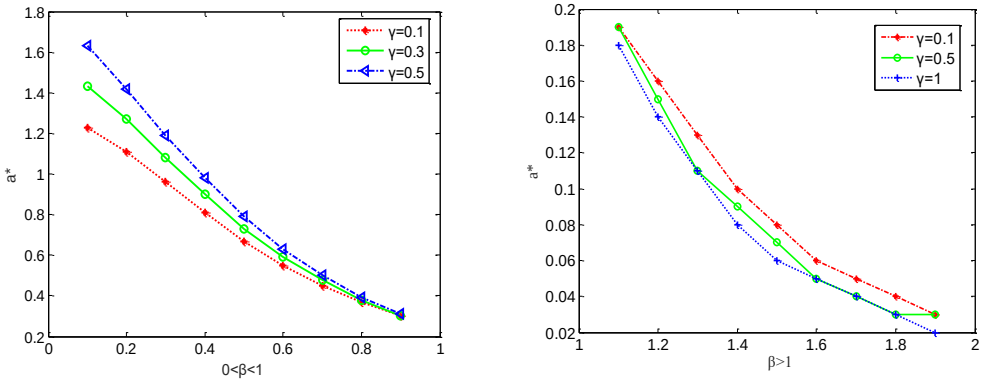
because of $\beta \geq 0$, the inequality $Z'(\beta) < 0$ always holds, and $Z(\beta)$ is a decreasing function.

In addition, we take the derivative of function (16) with respect to parameter γ, one can get:

$$Z'(\gamma) = \frac{s_{\max}\langle s\rangle\langle s^2\rangle}{\langle s^{\beta+2}\rangle\langle s^{\beta+1}\rangle} \times (1-\beta)(1+\gamma)^{-\beta} \tag{17}$$

From Equation (17), one can find that when $\beta > 1$, then function $Z'(\gamma) < 0$. Hence, function $Z(\gamma)$ is a monotone minus function. Interestingly, it is noted that when parameter $\beta > 1$, the higher load γ and the smaller α^*; however, when $0 < \beta < 1$, the smaller load γ, the smaller α^*. That is, a smaller load parameter γ and a larger capacity parameter β enhances the robustness of the network substantially. The following numerical simulations show the validity of theoretical analysis.

Figure 1 illustrates parameters β, γ as a function of the threshold parameter α, and it is found that the lower the value of parameter γ, the stronger the robustness of the weighted power network with parameter $\beta > 1$. Nevertheless, it is observed that parameter α^* increases with the parameter γ when $0 < \beta < 1$. Thus, the simulation results are consistent with the theoretical results.



(**a**) (**b**)

Figure 1. The relationship between threshold α^* and β, γ. (**a**) When parameter $0 < \beta < 1$ (**b**) When parameter $\beta > 1$.

To further understand the different cascade responses in more detail, the relative size of the maximum connected subgraph was used to quantify the robustness of the weighted power network.

$$G = N'/N \tag{18}$$

where N' and N are the number of nodes of the maximum connected sub-network before and after a cascading failure, respectively.

Take the IEEE118 system as an example [33], we investigated the cascading failure process and compared two different attack patterns for a given power network. Before we started the simulations, we supposed that the network was in its stable state. The topology structure of the IEEE system is illustrated in Figure 2.

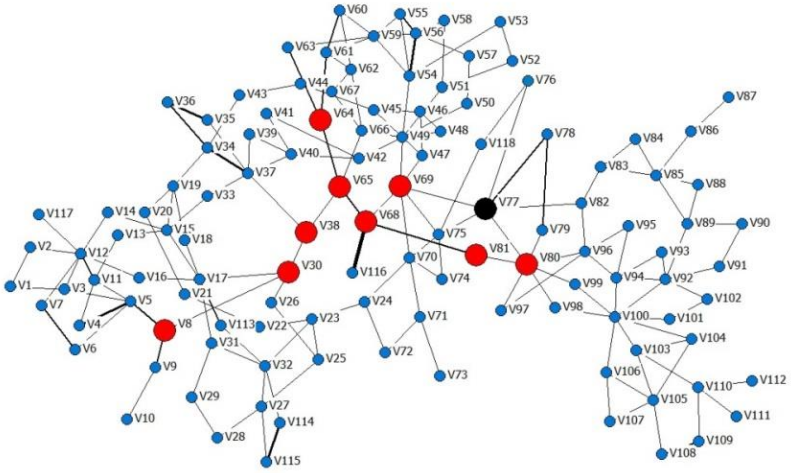


Figure 2. The topology of the weighted IEEE118 system.

We assumed that interdependent relationship and redistribution rules will cause the cascading failure at the same time. The attack on the power network is represented by a random removal of nodes. To explore the effect of a small initial attack on our cascading failure, we calculated S, which represents the number of disabled nodes in the network after the cascading process based on the interdependent relationship and redistribution rules are both over.

Firstly, we initiated the random attack process by removing 10 nodes, we investigated the influence of attack strategies on the cascading failure process. The betweenness value of components was ranked. Vulnerability of power network was analyzed by progressively removing the nodes. More specifically, intentional attack and random attack strategies were considered. In the following simulation, the values of parameter were selected as $\alpha = 0.5$, $\beta = 1$, $\gamma = 0.3$.

From Figure 3, one can observe that the power network had stronger robustness under an intentional attack at the initial time. In contrast, the robustness of the power network was stronger under a random attack than an intentional attack with the evolution of time. For the sake of completeness, we also showed the evolution of the capacity parameter α with different attacks. Thus, we fixed the parameters $\beta = 1$, $\gamma = 0.3$, then adjusted the capacity parameter α to observe the performance of the power network. We simulated cascading failures in the weighted IEEE 118 system using the distribution rule proposed above.

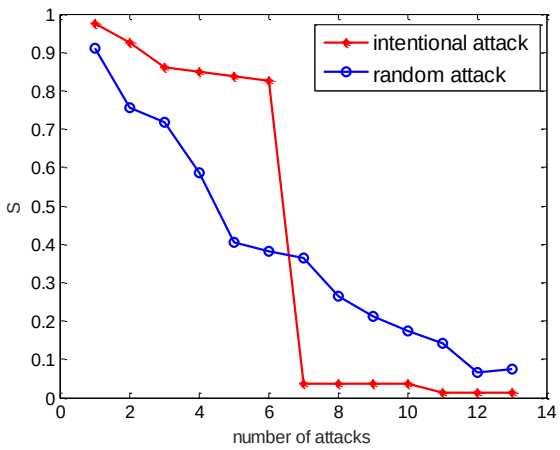
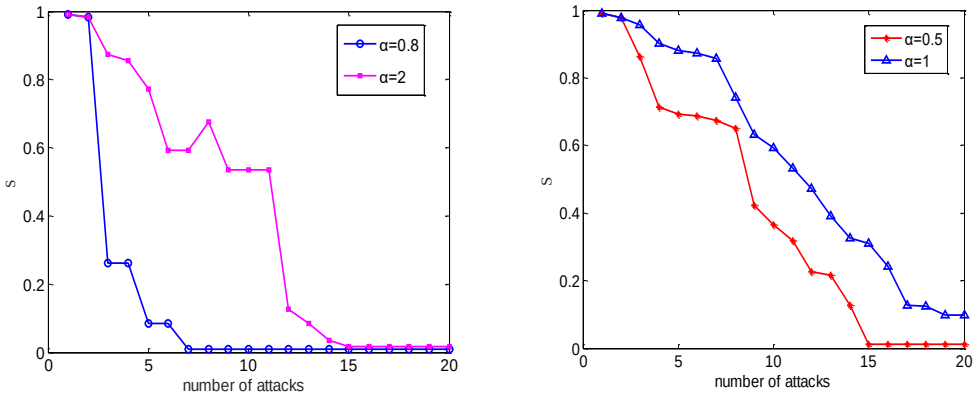


Figure 3. Relative size of the most connected sub-network of the IEEE118 systems under different attack strategies.

From Figure 4, as expected, a larger capacity parameter resulted in fewer node failures, because it makes the overload condition more difficult to be satisfied.



(**a**) (**b**)

Figure 4. The case of a weighted power network under different attack strategies. We averaged over 50 realizations. (**a**) Random attack. (**b**) Intentional attack.

2.2. Multilayer Interdependent Network Model

As is known, interdependent networks are ubiquitous in modern society. With the development of information technologies, the traditional power system has evolved into an electrical cyber-physical power network. In addition, failures in one network may spread to its coupled networks. This section is devoted to the investigation of cascading failures for this kind of interdependent network. Furthermore, interdependence between a power system and its cyber network can enhance the vulnerability of the whole system, so it is vital to analyze the cascading failure of an interdependent network.

According to the above-mentioned topological features, the extended betweenness was applied to IEEE118 system. Then, we constructed an electrical cyber network based on the IEEE118 system. Therefore, the power network and its cyber network can be described as:

$$G = \{V, E, M, W\}, \begin{cases} V = \{V_P, V_C\} \\ E = \{E_P, E_C\} \\ M = \{M_P, M_C, M_{PC}\} \\ W = \{W_P, W_C\} \end{cases} \tag{19}$$

where V, E are the set of nodes and lines, respectively. Additionally, M_P, M_C represent the adjacency matrix of the power network and its cyber network. M_{PC} is the interlayer coupling matrix between two layers. W_C and W_P are the arrangement of weight. In addition, P, C denote the power network and cyber network, respectively.

Specifically, the studied interdependent network can be considered as a partial one-to-one network as depicted in Figure 5, where the lower layer is the power network, the upper layer is its cyber network. Cyber network is in charge of controlling the power network while the power network provides electricity to its cyber network. In addition, the number of nodes in the cyber network is larger than that in the power network because of the existence of autonomous nodes. Hence, it is important to analyze the influence of coupling strategies on the vulnerability of an electrical cyber-physical interdependent network. In what follows, we analyze the performance of interdependent network with two different coupling schemes.

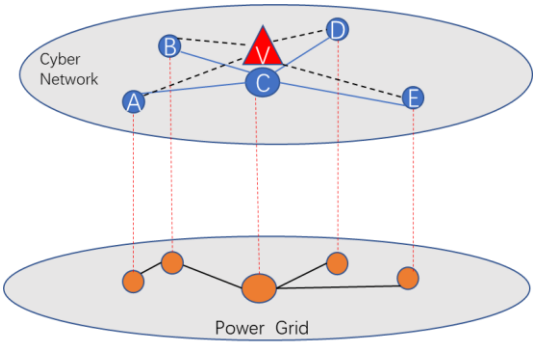


Figure 5. The topology of an electrical cyber-physical interdependent network.

3. Vulnerability Analysis for a Power Network

3.1. The Influence of Coupling Strategy on Vulnerability

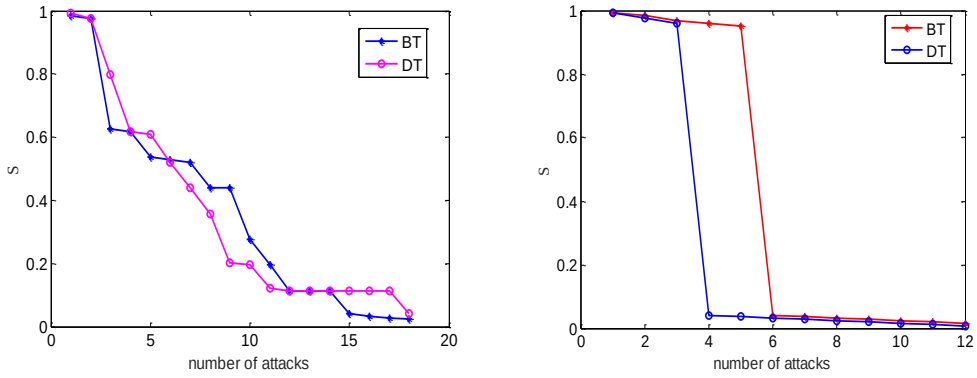
This subsection is devoted to the investigation of vulnerability for the electrical cyber-physical network. Next, to evaluate the vulnerability of a power network under different attacks, we define the normalized avalanche size as:

$$S = \frac{N_C{}' + N_P{}'}{N_C + N_P} \tag{20}$$

where N_C, N_P denote the number of survival nodes in the cyber network and the power network before an attack. $N_C{}'$ and $N_P{}'$ are the number of survival nodes in the cyber network and the power network after an attack. In fact, the degree is equal to the number of connectivity links a node is connected to and plays a crucial role in ensuring connectivity of the networks. We investigate the node failures as a function of the number of attacks. It is well known that the performance of an interdependent network can be influenced by the coupling patterns and attack strategies. The following coupling schemes are considered: (1) betweenness-extended betweenness (BT), and (2) degree-betweenness (DT).

In next step, a scale-free network with a mean degree $\langle K \rangle = 3$ is constructed based on IEEE118 systems, and construct an electrical cyber-physical network via BT and DT coupling schemes. If we neglect autonomous nodes in the cyber network, then each node in a layer mutually depends on only one node in another layer with one-to-one matching. Furthermore, the performance of the interdependent electrical cyber-physical network is shown according to different attacks. Here, we focus on intentional and random attacks.

One can find that inter-coupling strategies can influence the network's performance from Figure 6. There are negligible differences for two coupling strategies under random attacks. Nevertheless, the electrical cyber-physical interdependent network undergoes second-order transition under intentional attacks. At the initial time, the BT-coupling strategy has the stronger robustness than the relationship based on DT-coupling under the same conditions.

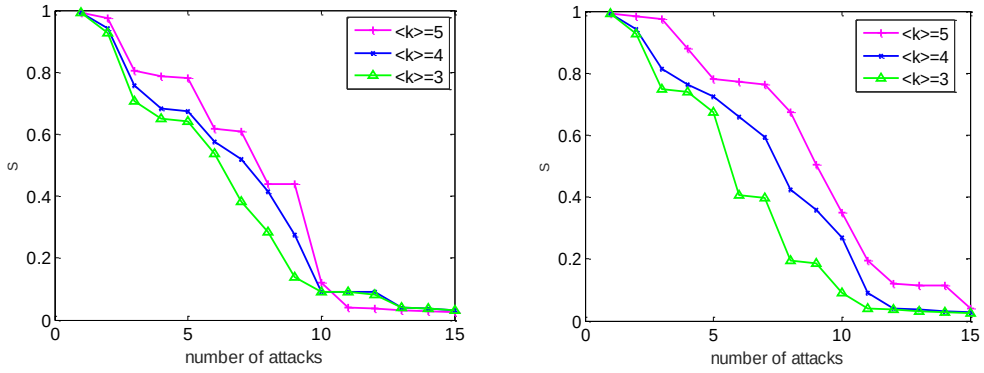


(**a**) (**b**)

Figure 6. The case of the coupled network with partial one-to-one interdependent nodes of the power network and its cyber network with different coupling strategies. The numerical simulations with $N_A = 118, N_B = 136$ and mean degree $\langle k_A \rangle = \langle k_B \rangle$. (**a**) Random attack. (**b**) Intentional attack. We averaged over 30 realizations.

3.2. The Influence of Mean Degree on Vulnerability

On the other hand, if the topology of the weighted power network is selected as the IEEE 118 system; therefore, the topology structure of the power network is fixed. Thus, the topology structure of its cyber network plays a major role in the performance of the interdependent network. Especially, the mean degree of a node plays a crucial role in the cascading failure process. In this subsection, we investigate the role of the mean degree on vulnerability of an electrical cyber-physical interdependent network. Here, the same homogeneous coupling and distribution of generators and consumers was adopted, as in Figure 7.



(**a**) (**b**)

Figure 7. Influence of the average degree on the robustness of an interdependent network. (**a**) Random attack. (**b**) Intentional attack.

Figure 7a depicts the cascading failure process of the cyber network with different mean degrees under random attacks. Figure 7b presents the same case under intentional attacks. In Figure 7b, we can see similar results to Figure 7a, which shows S as a function of the attack strategy. Moreover, Figure 7 reveals that the robustness of the interdependent network is improved with an increase in the average degree of the cyber network. However, at the same time, after some nodes fail, the probability of the cyber sub-network enhances. This leads to the failure of the nodes of the power network, and the collapse of the interdependent network. It is shown that the network's topology plays a significant role in determining the dynamics of cascading failures.

4. Conclusions

In summary, this paper addressed the vulnerability of weighted power networks. We present the extended betweenness to construct a more practical nonlinear model to analyze the cascading failure from edge overloading on weighted networks. Specially, the proposed model takes into consideration the contribution of the transmission line, moreover, the role of the capacity parameter on the cascading failure for a weighted power network. According to the presented weighted power network model, a weighted electrical cyber-physical interdependent network was developed. Furthermore, we analyzed the vulnerability and cascading failure dynamics on the entire interdependent network. Our results show that interdependent networks undergo second-order transition under intentional attacks and the robustness is improved with the increase of the average degree of the cyber network. These results indicate that the significant role of weights and the interdependent relationship in power networks for designing protective strategies against cascading failures.

Vulnerability control and optimization offer new avenues for controlling the dynamic behavior of real-world systems. Additionally, some artificial intelligence approaches can be used to obtain a general strategy for guiding the improvement of cascading failures for multiplex networks, which also deserves more attention in the future.

Author Contributions: Funding acquisition, investigation, software, writing—original draft preparation, L.Y.; writing—review and editing, Z.G.; data curation, formal analysis, writing—original draft preparation, Y.D.; methodology, P.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China (No. 11702195).

Institutional Review Board Statement: Not applicable.

Data Availability Statement: The datasets generated and analyzed during the current study are available from the corresponding author on reasonable request.

Conflicts of Interest: The authors declare no conflict of interests or personal relationships that could appear to influence the work reported in this paper.

References

1. Pagani, G.A.; Aiello, M. The Power Grid as a complex network: A survey. *Phys. A* **2013**, *392*, 2688–2700. [CrossRef]
2. Carareto, R.; Baptista, M.S.; Grebogi, C. Natural synchronization in power-grids with anti-correlated units. *Commun. Nonlinear Sci. Numer. Simul.* **2013**, *18*, 1035–1046. [CrossRef]
3. Peter, J.M.; Jobst, H.; Norbert, M.; Kurths., J. How basin stability complements the linear stability paradigm. *Nat. Phys.* **2013**, *9*, 89–92.
4. Auer, S.; Kleis, K.; Schultz, P.; Kurths, J.; Hellmann, F. The impact of model detail on power grid resilience measures. *Eur. Phys. J. Spéc. Top.* **2016**, *225*, 609–625. [CrossRef]
5. Coletta, T.; Jacquod, P. Linear stability and the Braess paradox in coupled-oscillator networks and electric power grids. *Phys. Rev. E* **2016**, *93*, 032222. [CrossRef] [PubMed]
6. Cohen, R.; Erez, K.; Ben-Avraham, D.; Havlin, S. Resilience of the Internet to intentional breakdowns. *Phys. Rev. Lett.* **2001**, *86*, 4626–4628. [CrossRef] [PubMed]
7. Peng, J.; Kurths, J. Basin stability of the Kuramoto-like model in small networks. *Eur. Phys. J.* **2014**, *223*, 2483–2491.
8. Feld, Y.; Hartmann, K.A. Large-deviations of the basin stability of power grids. *Chaos* **2019**, *29*, 123103. [CrossRef] [PubMed]
9. Che, Y.; Cheng, C. Active learning and relevance vector machine in efficient estimate of basin stability for large-scale dynamic networks. *Chaos* **2021**, *31*, 053129. [CrossRef] [PubMed]
10. Pourbeik, P.; Kundur, P.; Taylor, C. The anatomy of a power grid blackout—Root causes and dynamics of recent major blackouts. *IEEE Power Energy Mag.* **2006**, *4*, 22–29. [CrossRef]
11. Rubido, N.; Grebogi, C.; Baptista, M.S. Structure and function in flow networks. *Eur. Lett.* **2013**, *101*, 68001. [CrossRef]
12. Witthaut, D.; Timme, M. Braess's paradox in oscillator networks, desynchronization and power outage. *New J. Phys.* **2012**, *14*, 083036. [CrossRef]
13. Filatrella, G.; Nielsen, A.H.; Pedersen, N.F. Analysis of a power grid using a Kuramoto-like model. *Eur. Phys. J. B-Condens. Matter Complex Syst.* **2008**, *61*, 485–491. [CrossRef]
14. Manik, D.; Timme, M.; Witthaut, D. Cycle flows and multistability in oscillatory networks. *Chaos* **2017**, *27*, 083123. [CrossRef] [PubMed]

15. Schäfer, B.; Witthaut, D.; Timme, M.; Latora, V. Dynamically induced cascading failures in power grids. *Nat. Commun.* **2018**, *9*, 1975. [CrossRef] [PubMed]
16. Latora, V.; Marchiori, M. Economic small-world behavior in weighted networks. *Eur. Phys. J. B* **2003**, *32*, 249–263. [CrossRef]
17. Wang, F.; Tian, L.; Du, R.; Dong, G. The robustness of interdependent weighted networks. *Phys. A* **2018**, *508*, 675–680. [CrossRef]
18. Wu, Z.-X.; Peng, G.; Wang, W.-X.; Chan, S.; Wong, W.M.E. Cascading failure spreading on weighted heterogeneous networks. *J. Stat. Mech.* **2008**, *2008*, P05013. [CrossRef]
19. Muldoon, S.; Bridgeford, E.W.; Bassett, D.S. Small-World Propensity and Weighted Brain Networks. *Sci. Rep.* **2016**, *6*, 22057. [CrossRef]
20. Li, J.; Wang, Y.; Zhong, J.; Sun, Y.; Guo, Z.; Chen, Z.; Fu, C. Network resilience assessment and reinforcement strategy against cascading failure. *Chaos Solitons Fractals* **2022**, *160*, 112271. [CrossRef]
21. Ma, F.; Liu, F.; Yuen, K.F.; Lai, P.; Sun, Q.; Li, X. Cascading Failures and Vulnerability Evolution in Bus–Metro Complex Bilayer Networks under Rainstorm Weather Conditions. *Int. J. Environ. Res. Public Health* **2019**, *16*, 329. [CrossRef]
22. Cuadra, L.; Salcedo-Sanz, S.; Del Ser, J. A critical review of robustness in power grids using complex networks concepts. *Energies* **2018**, *8*, 9211–9265. [CrossRef]
23. He, W.; Chen, G.; Han, Q.-L.; Du, W.; Cao, J.; Qian, F. Multiagent Systems on Multilayer Networks: Synchronization Analysis and Network Design. *IEEE Trans. Syst. Man Cybern. Syst.* **2017**, *47*, 1655–1667. [CrossRef]
24. Gao, J.; Buldyrev, S.V.; Stanley, H.E.; Havlin, S. Networks formed from interdependent networks. *Nat. Phys.* **2012**, *8*, 40–48. [CrossRef]
25. Zhang, Y.; Arenas, A.; Yağan, O. Cascading failures in interdependent systems under a flow redistribution model. *Phys. Rev. E* **2018**, *97*, 022307. [CrossRef]
26. Shi, L.B.; Zhou, J. Vulnerability Assessment of cyber physical power system based on dynamic attack-defense game model. *Autom. Electr. Power Syst.* **2016**, *40*, 99–105.
27. Buldyrev, S.; Shere, N.W.; Cwilich, G.A. Interdependent networks with identical degrees of mutually dependent nodes. *Phys. Rev. E* **2011**, *83*, 016112. [CrossRef]
28. Pasqualetti, F.; Bicchi, A.; Bullo, F. A graph-theoretical characterization of power network vulnerabilities. In Proceedings of the IEEE 2011 conference on American Control Conference, San Francisco, CA, USA, 29 June 29–1 July 2011; pp. 3918–3923.
29. Dong, G.; Gao, J.; Tian, L.; Du, R.; He, Y. Percolation of partially interdependent networks under targeted attack. *Phys. Rev. E* **2012**, *85*, 016112. [CrossRef]
30. Ji, X.; Wang, B.; Liu, D.; Dong, Z.; Chen, G.; Zhu, Z.; Zhu, X.; Wang, X. Will electrical cyber–physical interdependent networks undergo first-order transition under random attacks? *Phys. A* **2016**, *460*, 235–245. [CrossRef]
31. Dorfler, F.; Chertkov, M.; Bullo, F. Synchronization in complex oscillator networks and smart grids. *Proc. Natl. Acad. Sci. USA* **2013**, *1*, 2005–2010. [CrossRef] [PubMed]
32. Belykh, I.V.; Barrett, B.N.; Vladimir, V.N. Bistability of patterns of synchrony in Kuramoto oscillators with inertia. *Chaos* **2016**, *26*, 094822. [CrossRef] [PubMed]
33. Peyghami, S.; Davari, P.; Fotuhi-Firuzabad, M.; Blaabjerg, F. Standard Test Systems for Modern Power System Analysis: An Overview. *IEEE Ind. Electron. Mag.* **2019**, *13*, 86–105. [CrossRef]