Modelling and vulnerability analysis of cyber-physical power systems based on interdependent networks

Zhang, Haiyan; Peng, Minfang; Guerrero, Josep M.; Gao, Xingle; Liu, Yanchen

Published in:
Energies

DOI (link to publication from Publisher):
10.3390/en12183439

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

energies

MDPI

Article

Modelling and Vulnerability Analysis of Cyber-Physical Power Systems Based on Interdependent Networks

Haiyan Zhang [1], Minfang Peng [1,*], Josep M. Guerrero [2], Xingle Gao [1] and Yanchen Liu [1]

[1] College of Electrical and Information Engineering, Hunan University, Changsha 410082, China
[2] Department of Energy Engineering, Aalborg University, 9220 Aalborg, Denmark
* Correspondence: minfangpeng@hnu.edu.cn; Tel.: +86-1732-528-1129

Received: 7 August 2019; Accepted: 3 September 2019; Published: 6 September 2019

Abstract: The strong coupling between the power grid and communication systems may contribute to failure propagation, which may easily lead to cascading failures or blackouts. In this paper, in order to quantitatively analyse the impact of interdependency on power system vulnerability, we put forward a "degree–electrical degree" independent model of cyber-physical power systems (CPPS), a new type of assortative link, through identifying the important nodes in a power grid based on the proposed index–electrical degree, and coupling them with the nodes in a communication system with a high degree, based on one-to-one correspondence. Using the double-star communication system and the IEEE 118-bus power grid to form an artificial interdependent network, we evaluated and compare the holistic vulnerability of CPPS under random attack and malicious attack, separately based on three kinds of interdependent models: "degree–betweenness", "degree–electrical degree" and "random link". The simulation results demonstrated that different link patterns, coupling degrees and attack types all can influence the vulnerability of CPPS. The CPPS with a "degree–electrical degree" interdependent model proposed in this paper presented a higher robustness in the face of random attack, and moreover performed better than the degree–betweenness interdependent model in the face of malicious attack.

Keywords: cyber-physical power system; interdependent model; cascading failure; vulnerability; link pattern

1. Introduction

With the advent of intelligent power grids, the interaction between communication systems and power grids has increased rapidly, forming complex interconnected networks called cyber-physical power systems (CPPS). Communication systems and power grids work cooperatively to supply service for human beings; they belong to different infrastructures but are representatively interdependent [1,2]. The interdependency between the two heterogeneous networks means that the power grid relies on a communication network for transmitting data and control information; meanwhile, it supplies electricity to the normal running of the communication network [3].

Under some circumstances, composite networks give rise to a security risk far more than single systems, where the strong coupling easily facilitates the propagation of an initial tiny failure, potentially resulting in catastrophic cascading events. For example, such cases were seen in the dramatic large-scale blackout of Italy on 28 September 2003, and the blackout of the Ukrainian power grid in 2016, due to external interference of hackers through the data network. It seems as though CPPS are more vulnerable holistically because of the embedding interactions [4]. While this conclusion may be incomplete and awry for all cases, the impact of interdependency is still not explicitly known and requires further studies.

The communication system and the power grid are completely heterogeneous in nature. The power grid belongs to a time-varying and continuous system, while the communication system is a discrete system. There are obvious differences between them in terms of components, transmission content and working mechanisms [5]. Research on the interaction between the cyber layer and physical layer contributes to reveal the propagation law of cascading fault in CPPS.

Traditional fault analyses are mostly focused on the power system internally. Furthermore, the majority of existing approaches treat the communication network and power grid as two individuals, ignoring the coupling relationship between cyber and physical layers, where they are separated completely and modelled independently.

The seminal contribution is that Buldyrev et al. [6] have developed a framework for understanding the robustness of interactive networks, and have applied this to analyzing cascading failures in a real power network and an internet network. Reference [7] points out that the percolation transition of a randomly coupled network of network (NON)-system is second order. In Reference [8], the authors proposed the concept of inter-similarity between networks and found that the robustness of coupled networks to random attacks could be significantly enhanced by increasing the similarity. Reference [9] proved that the double-star communication networks perform better than the mesh communication networks to prevent cascading failures in CPPS. Jia Guo et al. demonstrated that degree–betweenness interface type is the best in all closeness centrality interface strategies [10]. Reference [11] proposed a Markov-chain framework to capture the interdependence between infrastructure networks and evaluate the impacts of interdependence on recovery capability and system reliability. The authors in [12] put forward a framework to investigate the vulnerability of multi-layer networks and took the Shanghai urban rail transit network as an example to verify it. Recovery interventions are considered for mitigating cascading failures in a real network scenario of CPPS in [13]. In [14], the impacts of flow directions and line limits were analyzed and new electrical betweenness measures are proposed for power grid vulnerability assessment.

On the foundation of the above research, this paper provides a novel interdependent model with the "degree-electrical degree" assortative link pattern. Then, we compared the three types ("degree-electrical degree link", "degree-betwenness link" or "random link") of interdependent models and analyzed the corresponding integral vulnerability of the cyber-physical power system under random or malicious attacks.

The remainder of this paper is organized as follows. Fundamental concepts of the complex network and interdependent network are outlined in Section 2. In Section 3, we describe the interdependent model of CPPS based on the degree–electrical degree link pattern. The propagation process of cascading failures in interdependent networks is introduced in Section 4. In Section 5, we introduce the CPPS vulnerability assessment index. Section 6 shows the case study and simulation results. Finally, the related conclusions are discussed in Section 7.

2. Fundamental Concepts of Complex Network and Interdependent Network

2.1. Fundamental Concepts of Complex Network Theory

A network can be abstracted into a graph $G(V, E)$ by leaving out the intrinsic properties of the components, where $V = \{1, 2, \cdots, N\}$ is a set of nodes and $E = \{e_{ij}\}$ is a set of edges connecting ordered pairs of distinct nodes (i, j). Aside from this, an important notion must be mentioned, this being the adjacency matrix A:

$$\mathrm{A} = \left(a_{ij}\right) \in \mathbb{R}^{N \times N}, \tag{1}$$

where $a_{ij} = \begin{cases} 1 & e_{ij} \in E \\ 0 & otherwise \end{cases}$, which explicitly represents whether there is a link connecting the node pair (i, j) or not.

2.1.1. Random Network

The generation method of random network was proposed by Erdős and Rényi in 1959 [15]. The random edges are rewired with a probability p to connect two chosen nodes. The vital parameter is the connectivity or average degree, which measures the amount of neighbours that one node has in a synthetic random graph.

2.1.2. Average Path Length

The distance between two nodes in a network is quantified by the sum of edges that the shortest path passes through. Moreover, the maximum geodesic distance between any two nodes is called the diameter of the network, denoted as D, that is

$$\mathrm{D} = max_{i,j} d_{ij}. \tag{2}$$

The average path length L, also known as characteristic path length, is referred to as the average distance between any two nodes in the network. The full expression of the average path length is

$$\mathrm{L} = \frac{1}{\frac{1}{2}N(N+1)} \sum_{i \geq j} d_{ij} = \frac{2}{N(N+1)} \sum_{i \geq j} d_{ij}, \tag{3}$$

where N is the amount of nodes.

2.1.3. Clustering Coefficient

The clustering coefficient C , which is introduced to measure the connectivity between two nodes, is defined as proposed by Watts and Strogatz [16]:

$$\mathrm{C} = \langle c \rangle = \frac{1}{N} \sum_{i \in N} c_i, \tag{4}$$

where $c_i = \frac{2e_i}{k_i(k_i-1)} = \frac{\sum_{j,m} a_{ij} a_{jm} a_{mi}}{k_i(k_i-1)}$, which is a local clustering coefficient to show the likelihood of interconnection for two neighbours of the node i [15]. By definition, we could know that $0 \leq c_i \leq 1$ and $0 \leq \mathrm{C} \leq 1$.

2.1.4. Degree and Degree Distribution

The degree d_i of a node i is defined as the sum of other nodes connected with that node. For a directed network, in-degree and out-degree respectively represent the numbers of incoming and outgoing links. Intuitively, the greater the degree is, the more significant the node appears to be. We can use the function $P(d)$ to describe the distribution of nodes' degree and make a plot of the cumulative distribution function, which expresses the probability where the degree of a stochastically selected node happens to be d.

Regular graphs follow a simple degree distribution—delta distribution—since all the nodes shared the same degree. By contrast, random graphs are typically characterized by power-law distribution (namely scale-free distribution). Furthermore, completely random networks approximately show Poisson distribution.

2.1.5. Betweenness

The betweenness is equal to the number of shortest paths through a node or an edge. It is used to identify the critical components of a graph or network. The betweenness of node v is formatted as

$$\mathrm{B}(v) = \sum_i^n \sum_j^n \frac{\sigma_{ij}(v)}{\sigma_{ij}}, \tag{5}$$

where $\sigma_{ij}(v)$ is equivalent to the number of shortest paths between nodes i and j passing through node v, and σ_{ij} is the amount of shortest paths between nodes i and j.

2.1.6. Small-World Effect

The network, which has both short characteristic path length and high clustering coefficient, is labelled as a small-world network by Watts and Strogatz [16]. The small-world effect (six degrees of separation) is generic for many large and sparse real networks, and is reflected in social networks in that two of an individual's friends, unfamiliar with each other, may have mutual acquaintances.

2.1.7. Scale-Free Network

Barthelemy and Amaral conjectured that networks with power-law degree distributions are referred to as scale-free networks, where a fraction of nodes have high connectivity while the majority of nodes have a small node degree [17].

2.2. Introduction of Interdependent Networks

Interdependent networks, namely super-networks, network of networks, or multiple networks, are composed of multiple single-layer networks with different structures or properties [18]. As shown in Figure 1, by taking networks A and B as an example, the dotted lines connecting interdependent nodes between different layers are called connecting edges, and three loopless connection types are shown in Figure 2. Generally, the connection between dependent edges falls into three types: (i) assortative links, (ii) disassortative links and (iii) random links [19]. Assortative links refers to connecting nodes with similar topological characteristics, such as node degree or betweenness, in two networks. Thus, the nodes in network A with higher degrees map the nodes in network B with higher degrees, and vice versa. Disassortative links mean that nodes in network A with higher degrees correspond to the nodes in network B with lower degrees, and vice versa. Random link refers to when the nodes in network A and B are connected randomly.

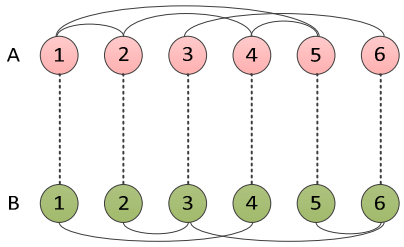

Figure 1. Interdependency diagram.

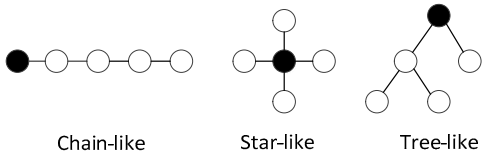

Figure 2. Three types of interdependency.

The CPPS are large-scale composite systems in which the communication network and power grid are continuously interacting through interdependent nodes. Information collecting and monitoring equipment detect and upload the operation data in real-time, including measurement data (e.g., voltage and current of branches or nodes) and the operating state of devices (e.g., information of switches, breakers and transformer taps). The dispatch centre collects measurement information at nodes, monitors the power flow on the transmission line, manages the changes of network topology and then issues control commands [20]. The typical CPPS architecture is shown in Figure 3. Interactive nodes have diverse corresponding relation, for instance, one-to-one, one-to-more, more-to-one and more-to-more.

In order to simplify the calculation, we assume that it is a one-to-one correspondence between power nodes and communication nodes.

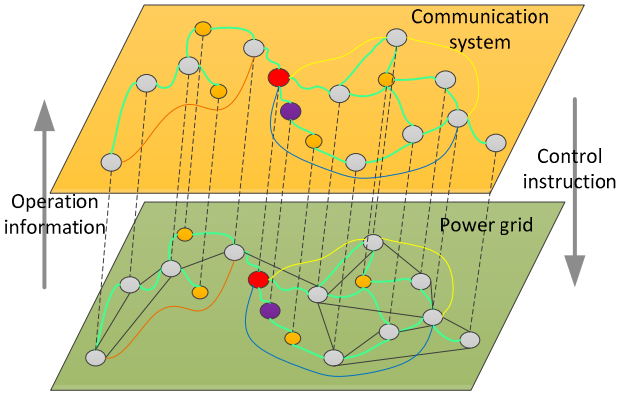

Figure 3. The interdependency between the communication system and power grid.

3. Interdependent Model of Cyber Physical Power System

The topologies of the communication system and power grid were abstracted and expressed as undirected graphs G_C and G_P, respectively. Each layer represented a network with a specific structure and function. $G = (V, E)$, where $V = \{n_i\}$ is the set of nodes in a network, and $E = \{e_{ij}\}$ represents the set of internal edges in each layer.

3.1. The Model of Communication Networks

The cyber layer is a communication network based on Ethernet, where communication facilities, data channels and related algorithms were all represented as normal nodes. Because of transmission characteristics, some special communication nodes were not connected to power nodes, which only connect the inside communication nodes. For the sake of simplicity, we left out this condition in the paper. The connection relation between the communication nodes were expressed by the adjacency matrix, as follows:

$$A_C = (a_{ij})_{N \times N}, \tag{6}$$

where $a_{ij} = 1$ indicates the two nodes C_i and C_j were connected, otherwise $a_{ij} = 0$.

There are two typical structures of the communication network: the double-star network and mesh network. Double-star networks belong to scale-free networks, while mesh networks show small-world properties. The power system is also a small-world network and sensitive to random attacks. It has been demonstrated in the literature [4] that the composite system obtained by coupling two layers of small-world network has a worse robustness under any attacks. Therefore, we only adopted the double-star communication network.

To generate a communication network, the initial node n_0 was specified, and on the base of it we added a new node and m edges in one time step, and connected it to existing nodes according to the probability $p_i = \frac{k_i}{\sum_j k_j}$, where k_i is the degree of the node i and $\sum_j k_j$ is the sum of degree value of all the existing nodes. As the communication network belonged to a scale-free network, we employed the degree value to identify crucial nodes. Then, the control centre (Power Dispatching Centre) [8] always corresponded to the node with highest degree.

3.2. The Model of Power Grids

The relation between load nodes in the power grid can be expressed using the adjacency matrix, as follows:

$$A_P = (a_{ij})_{M \times M}. \tag{7}$$

The power grid is a typical small-world network [9]. Thus, to find out vital nodes, the single index, the degree–betweenness, is questionable. The importance of power nodes depends on (1) node property (2) the location of nodes in the entire topology. Each node does not exist independently but closely relates to its neighbours. Therefore, we introduced the importance evaluation matrix for power nodes:

$$H_I = \begin{bmatrix} S_1 & S_2\frac{\delta_{12}D_2}{\langle k\rangle^2} & \cdots & S_n\frac{\delta_{1n}D_n}{\langle k\rangle^2} \\ S_1\frac{\delta_{21}D_1}{\langle k\rangle^2} & S_2 & \cdots & S_n\frac{\delta_{2n}D_n}{\langle k\rangle^2} \\ \vdots & \vdots & \ddots & \vdots \\ S_1\frac{\delta_{n1}D_1}{\langle k\rangle^2} & S_2\frac{\delta_{n2}D_2}{\langle k\rangle^2} & \cdots & S_n \end{bmatrix}, \tag{8}$$

where n is the total number of network nodes, δ_{ij} represents the corresponding elements in the adjacent matrix, $\langle k\rangle$ represents the average degree, D_i is the degree of node i and $\frac{\delta_{ij}D_j}{\langle k\rangle^2}$ is the distribution parameter of the contribution degree, which denotes that node i distributes its importance to adjacent node j, and self-contribution is 100%.

Referring to the concept of network efficiency in complex network theory, we defined the connectivity efficiency to describe the difficulty of node k for connecting other node i.

$$S_k = \frac{1}{n}\sum\nolimits_{i=1,k\neq i}^{n} d_{ik}, \tag{9}$$

where d_{ik} is measured by the inverse of line impedance of shortest path:

$$d_{ik} = \frac{1}{Z_{ik}}. \tag{10}$$

If two nodes are not directly connected, $Z_{ik} = \infty$, then $d_{ik} = 0$. It shows that the smaller the line impedance value is, the more closely the two nodes are connected.

Therefore, we get the importance evaluation index of the electrical node, called the electrical degree.

$$\mathrm{I}_i = S_i\sum\nolimits_{j=1,j\neq i}^{n} S_j\frac{\delta_{ij}D_j}{\langle k\rangle^2}. \tag{11}$$

This index fuses the topological property and the electrical characteristics of nodes, which was used to evaluate the importance of each node in the power grid.

3.3. Interactive Mechanism and Model between Power Grids and Communications Network

The interdependency between the communication system and power grid is shown as the dotted lines in Figure 2 and represented as $A_{C-P} = \{(\mathrm{n},\mathrm{m})\big|\mathrm{n}\subset V_C, \mathrm{m}\subset V_P\} \subset R^{N\times M}$. The communication layer had N nodes $(C_1, C_2, \cdots, C_N)$ and the power layer had M nodes $(P_1, P_2, \cdots, P_M)$. Then, the overall CPPS can be described as follows:

$$\mathrm{A} = \begin{bmatrix} A_C & A_{C-P} \\ (A_{C-P})^T & A_P \end{bmatrix} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,N} & a_{1,N+1} & \cdots & a_{1,N+M} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{N,1} & \cdots & a_{N,N} & a_{N,N+1} & \cdots & a_{N,N+M} \\ a_{N+1,1} & \cdots & a_{N+1,1} & a_{N+1,N+1} & \cdots & a_{N+1,N+M} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{N+M,1} & \cdots & a_{N+M,N} & a_{N+M,N+1} & \cdots & a_{N+M,N+M} \end{bmatrix}, \tag{12}$$

where, if communication nodes and power nodes exchange energy or information reciprocally, $A_{C-P}(\mathrm{n},\mathrm{m}) = 1$, which means that there is a connecting edge; otherwise, $A_{C-P}(\mathrm{n},\mathrm{m}) = 0$.

In this paper, we advanced an interdependent network model based on assortative coupling, that is, the key nodes in the communication network corresponded to the important nodes in the power grid, called degree–electrical degree coupling. Firstly, in the communication network, all nodes were arranged in descending order of node degree d_C, namely $d_{C1} \geq d_{C2} \geq d_{C3} \geq \cdots \geq d_{CM}$. If two nodes had the same degree, we further compared their betweenness and similarly array in descending order. The higher the degree of nodes, the more crucial the nodes were in the topology. As long as those important nodes survived under attacks, the system could retain normal operation. Secondly, in the power gird, the electrical degree of nodes Ed_C was calculated, which was adopted to arrange the results from large to small, $Ed_{C1} \geq Ed_{C2} \geq Ed_{C3} \geq \cdots \geq Ed_{CM}$. Thirdly, we connected the first M cyber nodes and physical nodes one by one correspondingly to generate the symmetric interdependent network model studied in this paper.

Aside from this, for comparison, we obtained the degree–betweenness interdependent model in the same way. The cyber nodes were sorted by node degree in descending order, and the physical nodes were sorted by betweenness in descending order. Then, some cyber nodes with higher degrees were connected to those physical nodes with higher betweenness. Thus, similarly, we achieved the random interdependent model by coupling the cyber and physical nodes randomly.

4. The Propagation Process of Cascading Failures

In this paper, we supposed that the communication network and power grid had the same law of cascading failures. Once a communication node fails, the coupling power node loses control and quits operation. Afterwards, its coupling communication nodes lose power supply, and even communication interruptions occur. If a power node fails, its adjacent nodes malfunction because of overload. Moreover, the coupling communication nodes are removed from the system because of lacking electricity or incorrect metrical data. At this point, we seek the maximal connected subgraph of the present network structure. If a node does not belong to the maximal connected subgraph, it cannot maintain its function anymore and will also be expired.

We assumed that the node 5 fails because of a random failure or deliberate attack, and the specific fault propagation process of cascading failure is described in Figure 4 [21].

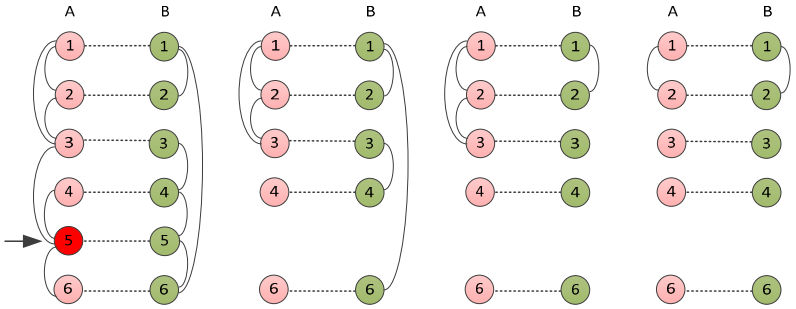

Figure 4. The specific process of cascading failure in a cyber physical power system.

- First stage: in the cyber layer A, node 5 is attacked and fails, and its interconnected edges and interdependent edges are deleted.
- Second stage: in the physical layer B, the node dependent on cyber node 5 fails, and then the directly connected edges are removed.
- Third stage: we seek the maximal connected subgraph of the cyber network A and remove invalid nodes, and meanwhile delete the coupling nodes and relevant edges in the physical layer B.
- Fourth stage: the same as the third stage—the invalid nodes and connected edges in the cyber layer A are removed, and this cycle repeats until there are only the maximal connected subgraph left in network A and B. Then CPPS reaches the final stable state.

5. CPPS Vulnerability Assessment

For interdependent network, the ability to maintain structural and functional integrity under attack is significant. In order to quantitatively analyse the vulnerability of CPPS, we introduced two indices: survival rate of nodes and survival rate of actual load.

5.1. Survival Rate of Node

In this paper, we employed the survival rate of nodes to evaluate the completeness of topological structure after an attack.

$$\mathrm{p} = \frac{N'_C + N'_P}{N_C + N_P}, \tag{13}$$

where N_C and N_P are, respectively, the original number of nodes in communication network and in the power grid. N'_C and N'_P denote the survival nodes after an attack. As can be seen from the formula, before failure $\mathrm{p} = 1$, and the larger the survival rate of nodes is, the less attacks damage the system structure, which indicates that the interdependent network is more robust [22]. When the failure scale 1-p reaches a threshold, the interdependent network will collapse completely.

5.2. Survival Rate of Actual Load

The following constraints must be satisfied during operation.

$$\begin{cases} s.t.F = AP \\ \sum_{i \in V_s} P_{Gi} - \sum_{j \in V_s} P_{Lj} > 0 \\ P_{G_i}^{min} \le P_{G_i} \le P_{G_i}^{max} \\ g_i \in G_i \end{cases}, \tag{14}$$

where the first equation expresses the DC power flow. The second equation shows power flow balance; $\sum_{i \in V_s} P_{Gi}$ is the sum of generator capacity, $\sum_{j \in V_s} P_{Lj}$ represents the set of loads and V_s denotes the power supply areas. The third equation is the constraint of generator output; $P_{G_i}^{min}$ and $P_{G_i}^{max}$ respectively express the minimum and maximum active power of generator i, and the forth equation ensures the connectivity of subgraphs.

Taking the aforementioned constraints into consideration, we can calculate the power flow of the current system composed of surviving nodes after cascading failures to guarantee operation security. If generators or lines overloaded, a series of control measures must be taken, such as load shedding and generator trip. After that, the remaining nodes are the final saved power loads, and then we can calculate the actual load survival rate.

$$\mathrm{L}_P = \frac{\mathrm{L}_R}{\mathrm{L}_O}, \tag{15}$$

where L_O is the total of original power loads, and L_R is the remaining loads after calculating power flow and verification.

The two indexes proposed above are not only suitable for one-to-one link patterns, but are also applicable to one-to-more and more-to-more coupling types in interdependent networks.

6. Case Study and Simulation Results

In this paper, we tested our model on the IEEE 118-bus power system and double-star communication network with the same number of nodes, that is $N_A = N_B = 118$, depicted in Figures 5 and 6, respectively. Generally, the power grid has a tree structure, while the communication network shows a ring structure. Table 1 fully reflects the difference between them in terms of structures and properties. A series of topological characteristics of the two networks [23], such as degree–betweenness, average degree and cluster coefficient, are listed below. We put forward a

new interdependent model with degree–electrical degree assortative link and compared it with the degree–betweenness interdependent model and random link interdependent model. Deliberate attacks, based on node degree and random failures, were adopted to test the vulnerability of the artificial CPPS. The simulation flowchart is shown in Figure 7.

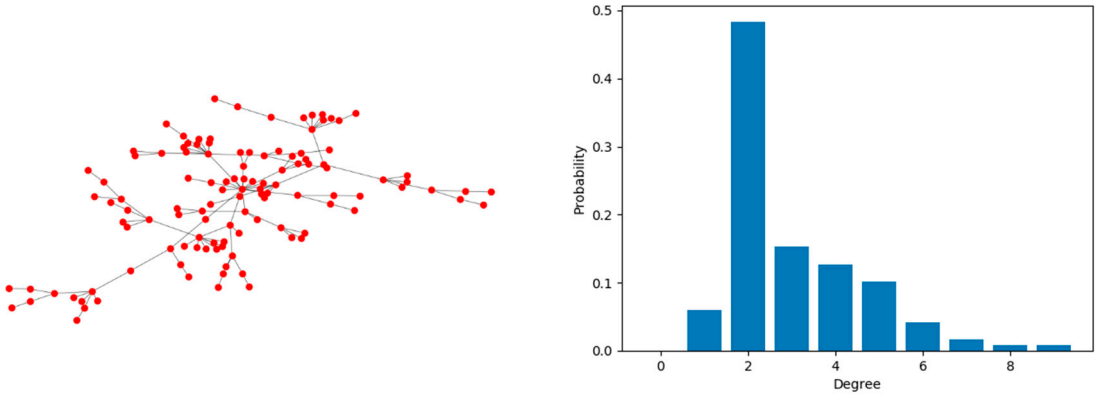

Figure 5. The power grid and its degree distribution.

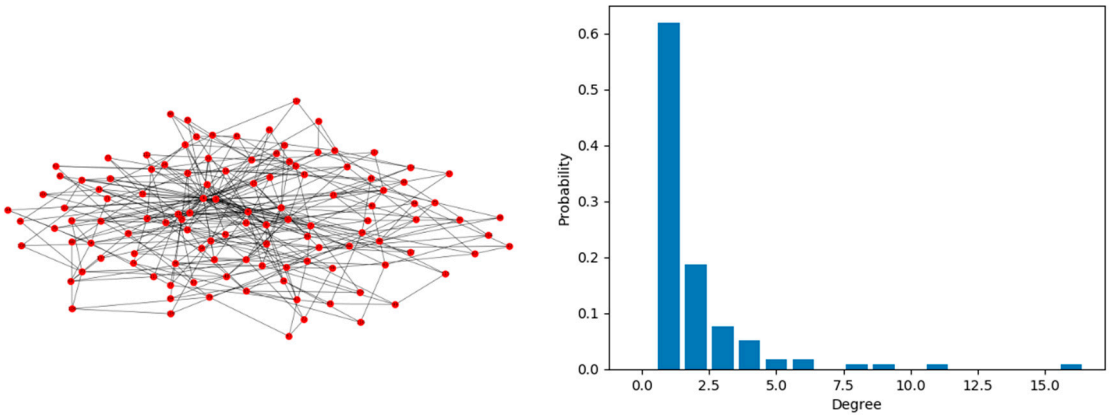

Figure 6. The communication system and its degree distribution.

Table 1. The statistical characteristics of the cyber physical power system.

Network	N	M	$\langle k \rangle$	C	L	D
Communication network	118	137	2.3220	0.0095	4.6083	11
Power grid	118	186	3.1525	0.1628	6.3096	14

In Table 1, N is the number of nodes, M is the number of edges, $\langle k \rangle$ is the average node degree, C denotes the clustering coefficient, L presents the average path length, and D is the network diameter.

6.1. Vulnerability of CPPS under Random Attack

Respectively, we took the three-type coupling modes to build the corresponding interdependent models: the random coupling interdependent model, the degree–betweenness interdependent model and the electrical degree–betweenness interdependent model. Firstly, we studied the vulnerability of CPPS under random attacks with different number of interdependent nodes (30, 60, 90, 118).

When analysing the interaction between the two networks, we took the intermediate connection type and coupling strength into consideration. Figure 8 illustrates how the different coupling strengths and connection types evidently effect the vulnerability of CPPS.

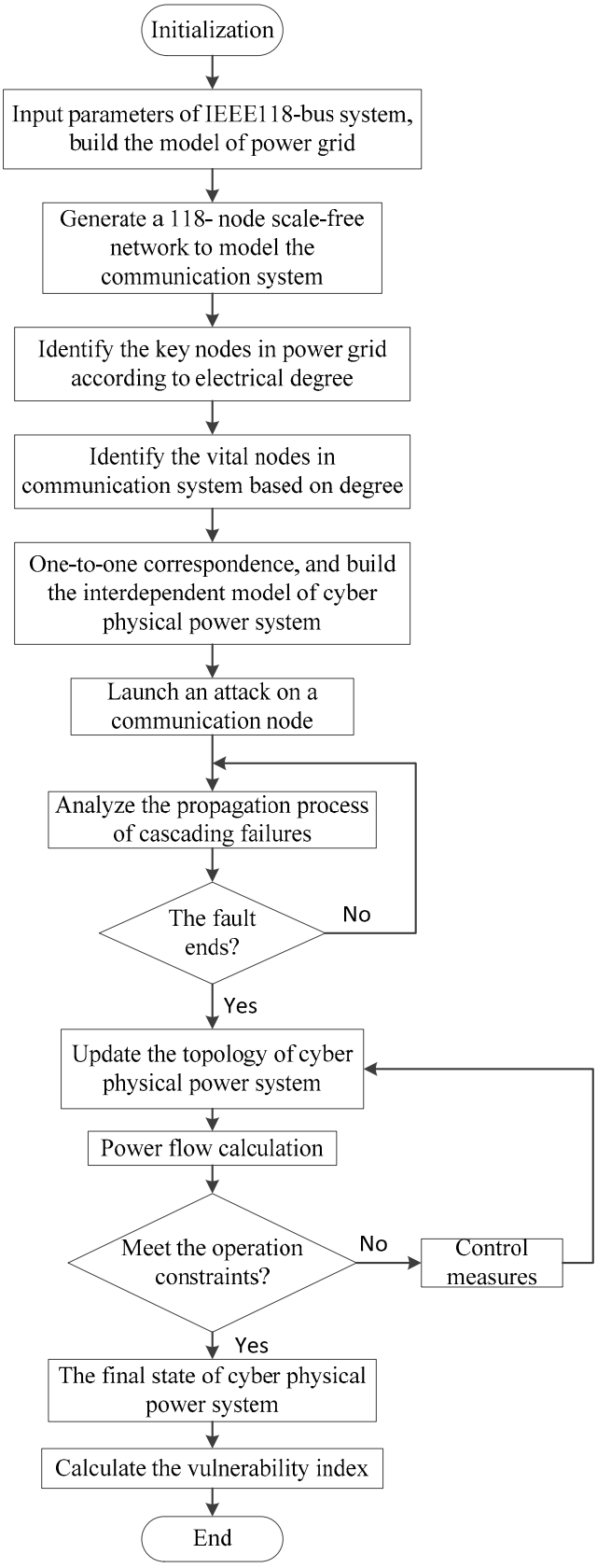

Figure 7. Simulation flowchart.

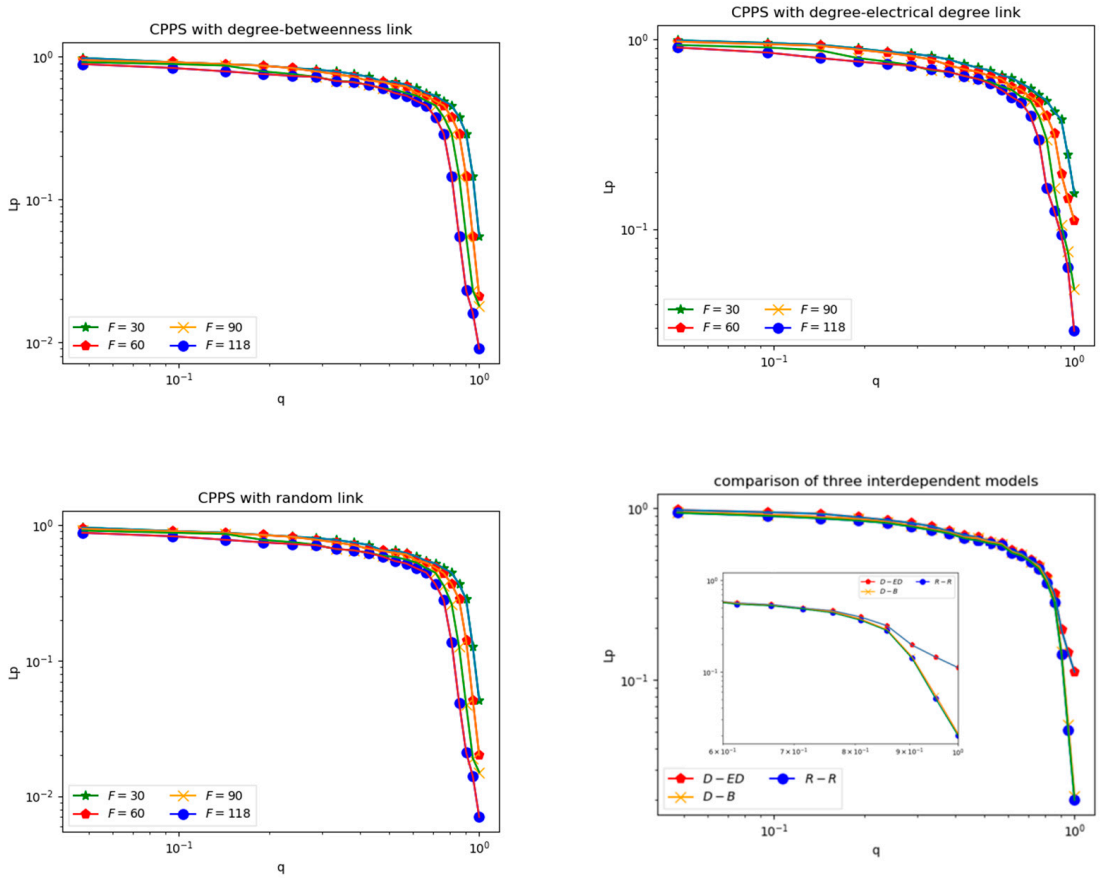

Figure 8. The vulnerability of cyber-physical power systems (CPPS) under random attacks.

After launching a random attack against the communication system, we calculated and compared the actual load survival rate of the cyber physical power system with the "degree–betweenness", "degree–electrical degree" and "random link" coupling modes.

From Figure 8 we know that, under a random attack, the three interdependent models showed similar performance. However, when a large scale attack was launched, the degree-electrical degree interdependent model could effectively reduce the probability of a blackout.

In addition, the figure shows that the resistibility of CPPS under random attack increased with the rise of coupling strength, regardless of what kind of interdependent model was used. Furthermore, the integral CPPS was the most robust with full dependence, i.e., F = 118, which is consistent with the conclusion in [24].

6.2. *Vulnerability of CPPS under Malicious Attack*

As above, comparisons were conducted between the "random link model", "degree–betweenness link model" and "degree–electrical degree link model" under malicious attack. We calculated the vulnerability of the cyber physical power system under different interdependence strengths (30, 60, 90 and 118 strips of links). The simulation results are shown below, divided into four sets.

From Figure 9, we know that, compared with random attacks, the cyber physical power grid is more vulnerable to malicious attacks. In the case of malicious attacks, the cyber physical power system with a random link model is the most robust. The cyber nodes were connected with the power nodes randomly, thus the important nodes in the cyber layer and physical layer will not fail collectively after a malicious attack.

When the number of coupling edges was constant, the degree–electrical degree interdependent model was shown to be more robust than the degree–betweenness interdependent model, which will be useful in guiding the construction of a cyber physical power system.

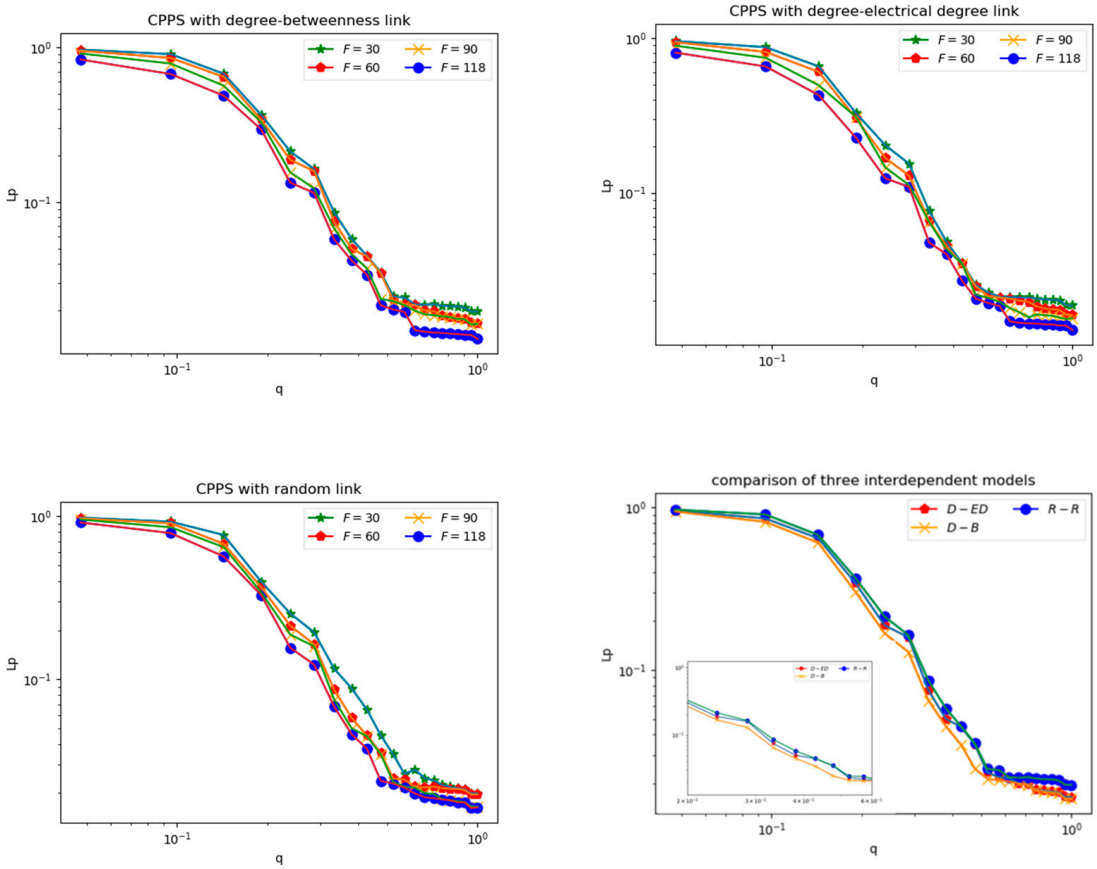

Figure 9. The vulnerability of CPPS under malicious attack.

Moreover, the figure shows that the vulnerability of CPPS under malicious attack increased with the rise of coupling strength. Furthermore, the integral system was the most vulnerable, with the mode of full dependence (i.e., $F = 118$).

7. Conclusions

Comprehensively getting hold of interaction mechanisms and dynamical characteristics of interdependent networks is the basis of cascading failure prevention in cyber physical power systems (CPPS). In this paper, a novel interdependent model of a cyber physical power system based on the degree–electrical degree coupling mode was put forward. As a case study, we took the double-star communication system, a scale-free network, and the IEEE 118-bus power grid, to generate an artificial CPPS. Then, the impacts of different interdependent models, coupling strength and attack types on CPPS vulnerability were analysed.

Through this research, we discovered that, on the premise of one-to-one correspondence, the cyber physical power system was shown to be more vulnerable under a malicious attack than under a random attack. Under a large scale random attack, the degree–electrical degree interdependent model effectively reduced the probability of large-scale blackout. In the case of malicious attack, the cyber physical power system with the random link pattern manifested as the most robust, and the degree–electrical degree interdependent model performed better than the degree–betweenness interdependent model. In addition, whatever the interdependent model, the robustness of the cyber physical power system decreased with the increase of coupling strength between the two layers. These simulation results reflect that the interaction or coupling between the communication system and power grid makes the power gird more vulnerable to some extent.

Moreover, in our opinion, in the future research of modelling and vulnerability analysis of cyber physical power systems, the following factors should be taken into consideration so as to improve the

interdependent model: (1) In practice, the communication nodes and power nodes are not completely one-to-one coupled, and instead may be one-to-more or more-to-more connected. (2) Many vital communication nodes are configured with uninterruptible power supply (UPS) so that a short-time failure of the power gird will not affect the normal operation of the communication network, and thus the corresponding communication nodes may not fail immediately after some power nodes quit. (3) We should premeditate the intervention of multi-scenario requirements and various control measures to prevent cascading failures.

Author Contributions: Formal analysis, X.G. and H.Z.; Methodology, H.Z.; Resources, M.P.; Validation, Y.L.; Visualization, H.Z.; The initial version of the manuscript, H.Z. and J.M.G.; Review and editing, J.M.G.; The final version of the manuscript, H.Z.

Funding: This research was funded by the National Natural Science Foundation of China, grant numbers 61472128 and 61973107.

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

References

1. Otuoze, A.O.; Mustafa, M.W.; Larik, R.M. Smart grids security challenges: Classification by sources of threats. *J. Electr. Syst. Inf. Technol.* **2018**, *5*, 468–483. [CrossRef]
2. Liu, W.; Gong, Q.; Han, H.; Wang, Z.; Wang, L. Reliability Modeling and Evaluation of Active Cyber Physical Distribution System. *IEEE Trans. Power Syst.* **2018**, *33*, 7096–7108. [CrossRef]
3. Kröger, W.; Zio, E. *Vulnerable Systems*; Springer Science & Business Media: London, UK, 2011.
4. Cai, Y.; Cao, Y.; Li, Y.; Huang, T.; Zhou, B. Cascading failure analysis considering interaction between power grids and communication networks. *IEEE Trans. Smart Grid* **2015**, *7*, 530–538. [CrossRef]
5. Zhang, J.; Chu, Z.; Sankar, L.; Kosut, O. Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems? *IEEE Trans. Power Syst.* **2018**, *33*, 4775–4786. [CrossRef]
6. Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **2010**, *464*, 1025–1028. [CrossRef] [PubMed]
7. Parshani, R.; Buldyrev, S.V.; Havlin, S. Interdependent networks: Reducing the coupling strength leads to a change from a first to second order percolation transition. *Phys. Rev. Lett.* **2010**, *105*, 048701. [CrossRef] [PubMed]
8. Chen, Z.; Wu, J.; Xia, Y.; Zhang, X. Robustness of interdependent power grids and communication networks: A complex network perspective. *IEEE Trans. Circuits Syst. II Express Briefs* **2017**, *65*, 115–119. [CrossRef]
9. Cai, Y.; Li, Y.; Cao, Y.; Li, W.; Zeng, X. Modeling and impact analysis of interdependent characteristics on cascading failures in smart grids. *Int. J. Electr. Power Energy Syst.* **2017**, *89*, 106–114. [CrossRef]
10. Guo, J.; Han, Y.; Guo, C.; Lou, F.; Wang, Y. Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties. *Energies* **2017**, *10*, 87. [CrossRef]
11. Rahnamay-Naeini, M.; Hayat, M.M. Cascading failures in interdependent infrastructures: An interdependent Markov-chain approach. *IEEE Trans. Smart Grid* **2016**, *7*, 1997–2006. [CrossRef]
12. Zhang, J.; Song, B.; Zhang, Z.; Liu, H. An approach for modeling vulnerability of the network of networks. *Phys. A Stat. Mech. Its Appl.* **2014**, *412*, 127–136. [CrossRef]
13. Tootaghaj, D.Z.; Bartolini, N.; Khamfroush, H.; He, T.; Chaudhuri, N.R.; La Porta, T. Mitigation and Recovery from Cascading Failures in Interdependent Networks under Uncertainty. *IEEE Trans. Control Netw. Syst.* **2018**, *6*, 501–514. [CrossRef]
14. 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 Stat. Mech. Its Appl.* **2017**, *466*, 295–309. [CrossRef]
15. Erdős, P.; Rényi, A. On the evolution of random graphs. *Publ. Math. Inst. Hung. Acad. Sci.* **1960**, *5*, 17–60.
16. Watts, D.J.; Strogatz, S.H. Collective dynamics of 'small-world' networks. *Nature* **1998**, *393*, 440–442. [CrossRef]
17. Barabási, A.L.; Albert, R. Emergence of scaling in random networks. *Science* **1999**, *286*, 509–512. [CrossRef] [PubMed]

18. Gao, J.; Buldyrev, S.V.; Stanley, H.E.; Havlin, S. Networks formed from interdependent networks. *Nat. Phys.* **2012**, *8*, 40–48. [CrossRef]
19. Rueda, D.F.; Calle, E. Using interdependency matrices to mitigate targeted attacks on interdependent networks: A case study involving a power grid and backbone telecommunications networks. *Int. J. Crit. Infrastruct. Prot.* **2017**, *16*, 3–12. [CrossRef]
20. Wang, H.; Ruan, J.; Zhou, B.; Li, C.; Wu, Q.; Raza, M.Q.; Cao, G. Dynamic Data Injection Attack Detection of Cyber-Physical Power Systems with Uncertainties. *IEEE Trans. Ind. Inform.* **2019**, 1. [CrossRef]
21. Moussa, B.; Akaber, P.; Debbabi, M.; Assi, C. Critical links identification for selective outages in interdependent power-communication networks. *IEEE Trans. Ind. Inform.* **2017**, *14*, 472–483. [CrossRef]
22. Ye, H.; Mou, Q.; Wang, X.; Liu, Y. Eigen-analysis of large delayed cyber-physical power system by time integration-based solution operator discretization methods. *IEEE Trans. Power Syst.* **2018**, *33*, 5968–5978. [CrossRef]
23. Kong, P.Y. Optimal Configuration of Interdependence between Communication Network and Power Grid. *IEEE Trans. Ind. Inform.* **2019**, *15*, 4054–4065. [CrossRef]
24. Wang, J.; Jiang, C.; Qian, J. Robustness of interdependent networks with different link patterns against cascading failures. *Phys. A Stat. Mech. Its Appl.* **2014**, *393*, 535–541. [CrossRef]