electronics

Article

Robustness Assessment of Cyber–Physical System with Different Interdependent Mechanisms

Peixiang Wang, Qianyi Wang, Haicheng Tu * and Yongxiang Xia

School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China
* Correspondence: tuhc@hdu.edu.cn

Abstract: Cyber–physical systems (CPSs) are a new generation of intelligent system that integrate communication, control and computation functions and are widely used in traditional infrastructure networks, such as power network, transportation network and others. In order to ensure the stable operation and improve the robustness of CPSs, the studies of robustness assessment have attracted much attention from academia. However, previous models assume that the failure propagation conforms to a strongly interdependent relationship, and only consider the interaction between nodes, while ignoring the interaction between nodes and links. In this paper, we develop a novel simulation model with the consideration of both the coupling modes and the failure propagation objects. Based on the simulation model, we study how the interdependent mechanisms, failure propagation probability and protection strategies affect the robustness of CPSs. The simulations of our proposed model are demonstrated in a test CPS formed by coupling two classical complex networks. Compared with previous models, our proposed model shows different performances and comprehensively characterizes the interdependent relationship of CPSs. In detail, disassortative coupling shows the worst performance and the CPS becomes more sensitive to failure propagation when Node–Link is selected as the failure propagation object. In addition, compared to the communication network, the power network is more sensitive to failure propagation. Protecting electrical nodes is a more effective way to strengthen the robustness of CPSs when conservation resources are limited. Our work provides useful advice to operators on how to effectively design and protect a CPS.

Keywords: cyber–physical system; cascading failure; robustness; weak interdependent

Citation: Wang, P.; Wang, Q.; Tu, H.; Xia, Y. Robustness Assessment of Cyber–Physical System with Different Interdependent Mechanisms. *Electronics* **2023**, *12*, 1093. https://doi.org/10.3390/electronics12051093

Academic Editors: Keping Yu and Chinmay Chakraborty

Received: 27 January 2023
Revised: 20 February 2023
Accepted: 21 February 2023
Published: 22 February 2023

1. Introduction

Under the Internet of Everything, the safe and stable operation of infrastructure [1–3] is the premise to ensuring social activities and people's daily life activities. For instance, power systems play a crucial role in our daily life. However, with the increasing development of information technology, it is a common practice to combine infrastructures with cyber systems in order to enhance performance. The concept of cyber–physical systems (CPSs) [4–8] has been gradually proposed. Advanced communication and control technologies can make CPSs more efficient and safer, but also increase the risk of external attacks, bringing new challenges for CPSs.

As a typical example of CPSs, the smart grid [9–12] is formed by the coupling of power and communication networks. This coupled system expands in scale and becomes more complex in function. Any sudden change in the network structure can affect its power flow distribution; at the same time, this change can also affect the node or link with the coupled network. Typical cases are the severe blackout caused by physical attacks on 14 August 2003 in America [13] and cyber attacks on 23 December 2015 in Ukraine [14], which eventually led to the failure of the entire system and caused huge economic losses. Therefore, many researchers pay more and more attention to the study of the robustness of CPS and how to comprehensively characterize CPS and analyze the impact of key factors on the robustness of CPS are hot issues in the complex network.

Robustness is usually used to measure a network's ability to maintain its fundamental functions after failures. Research on the robustness of a single network can be divided into topological robustness and functional robustness. Research on topological robustness mainly focuses on analyzing the influence of network structure on system function. The measure on topological robustness is based on network connectivity. This kind of research mainly shows the effect of the connection relationship between nodes on system function, but it can not reflect the power flow distribution of the network itself. Therefore, the research based on functional robustness mainly focuses on the impact of load distribution between nodes on system functions. In the past decade, with the popularization of the concept of CPS, more and more researchers began to focus on the robustness of coupled networks. In 2010, Buldyrew et al. [15] proposed the concept of interdependent networks and presented a general model that assumes the failure of a node in one of the networks results in the failure of the corresponding node in the other network. Since then, a lot of research work based on this model has continued to propose a series of new modeling methods [16–19]. For example, Gao et al. [16] extended the coupling of two networks to multiple networks and proposed a model for the interdependence of multiple networks. In [17], a formal model of object-oriented Petri nets is proposed to improve the reliability of CPS in the dynamic modeling phase. Ref. [18] used random network and IEEE Standard Bus test cases to model CPSs and examine the resilience of these systems under different attack scenarios. Ref. [19] proposed a semantic model for analyzing information flow security in CPSs and thoroughly analyzed the robustness of the semantic model.

In these studies, it is often assumed that the failure of a node in one of the networks will result in the failure of the corresponding node in the other network, due to the strong interdependence between the networks. In actuality, this assumption may not hold in many real-life systems. Taking the smart grid as an example, the failure of an electrical node may not immediately lead to the failure of its counterpart communication node. Instead, the communication nodes are often equipped with the Uninterruptible Power Supply (UPS). If the failure can be found and repaired before UPS is used up, the failure of this node can be avoided. Therefore, Tu et al. [20] proposed a CPS model with weak interdependency between networks. In this model, when a node in one of networks fails, its corresponding node in the other network will also fail; the probability of this happening is dependent on the system configuration. In addition, Jiang et al. [21] proposed a new CPS model that takes into account the real dynamics of both the cyber and physical parts of the system, as well as the asymmetric interdependency between these two parts. The purpose of this model was to accurately depict the asymmetric interdependency between the cyber and physical components of a CPS.

However, the interdependent mechanisms in the above two models [20,21] were still ideal and oversimplified. These models only consider the failure propagation between nodes and do not consider the failure propagation between nodes and links. Taking the smart grid as an example again, when an electrical node fails, its counterpart communication node can still maintain some links to work because of UPS and the remaining links stop working due to the weak interdependency between networks in the smart grid. Similarly, when a communication node fails, some links of its corresponding electrical nodes will be disconnected, but there will still be some links that continue to work. Considering this situation, we will propose a novel model of CPS with the consideration of both the coupling modes and the failure propagation objects. Next, we will apply the proposed model and evaluate the robustness of the CPS that is formed by the interconnection of two classical complex networks. We will show how the model factors affect the robustness of CPS. Therefore, the main contributions of this paper are:

- We consider that the interdependent mechanism is composed of coupling modes and failure propagation objects.
- The failure propagation object in the interdependent mechanism of CPSs can not only be nodes but also links.

- We study how the key factors in the interdependent mechanism affect the robustness of CPSs.
- We investigate which node protection strategy has the most significant improvement in the robustness of CPSs.

The rest of this paper is organized as follows. Section 2 introduces our CPS model which consists of the model of two networks, interdependent mechanisms, a cascading process and metrics of robustness used to measure the performance. In Section 3, we primarily analyze the impact of various model factors, such as the failure propagation object, the coupling modes and protection strategies [22] on the robustness of CPSs. Finally, we discuss the simulation results in Section 4 and summarize the conclusions of this paper in Section 5.

2. The Model

In this paper, we consider that a CPS is composed of a power grid (PG) and communication network (CN) and the interdependent mechanism between them is composed of a failure propagation object and coupling mode. In the following subsection, we will provide a description of the model for each network and introduce the interdependent mechanisms between them. Finally, we will show the whole cascading failure process in CPSs.

2.1. Power Grid Model

The power grid is a type of engineering network. Each transmission line in the power grid has a capacity limit for electrical flow and any sudden change in the network structure can alter the power flow distribution [23,24]. When the power flow distribution has changed, the nodes or links whose current loads exceed their capacities will fail successively and then a series of cascading iterations begin, which is called cascading failure [25–28]. In this paper, we adopt the model proposed by Zhang et al. [29] to track the load distribution in the power grid during cascading failures. As described in the model [29], the power grid is composed of four types of nodes:

(i) The generation node i is the power supply source in a power grid and has a fixed voltage v_i. Thus, the nodal equation for a generation node i is

$$\begin{bmatrix} 0 & \cdots & y_i & \cdots & 0 \end{bmatrix} * V = v_i \tag{1}$$

where $y_i = 1$ and the voltage vector is $V = \begin{bmatrix} \cdots & v_i & \cdots & v_j & \cdots & v_k & \cdots & v_h & \cdots \end{bmatrix}^T$

(ii) The consumer node j dissipates power and at the circuit level, it sinks current I_j, i.e.,

$$\begin{bmatrix} Y_{j1} & \cdots & Y_{jj} & \cdots & Y_{jn} \end{bmatrix} * V = I_j \tag{2}$$

(iii) The distribution node k is a connecting node that nether produces nor consumes power. Thus, we set $I_j = 0$ and the equation is

$$\begin{bmatrix} Y_{k1} & \cdots & Y_{kk} & \cdots & Y_{kn} \end{bmatrix} * V = 0 \tag{3}$$

(iv) The transformer node h connects the high-voltage grids with mid-voltage or low-voltage grids. Therefore, the equation for a transformer node can be expressed as

$$\begin{bmatrix} Y_{h1} & \cdots & Y_{hh} & \cdots & Y_{hn} \end{bmatrix} * V = 0 \tag{4}$$

According to four types of nodes, we can obtain the following power system equation by combining Equations (1)–(4):

$$A * \begin{bmatrix} \cdots & v_i & \cdots & v_j & \cdots & v_h & \cdots \end{bmatrix}^T = \begin{bmatrix} \cdots & v_i & \cdots & I_j & \cdots & 0 & \cdots & 0 & \cdots \end{bmatrix}^T \tag{5}$$

where v_i represents the voltage of node i and $\boldsymbol{A}$ represents the admittance matrix of the power grid.

$$A = \begin{bmatrix} \ddots & & & & \cdots & \cdots & & & & \iddots \\ 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots \\ Y_{j1} & \cdots & Y_{ji} & \cdots & Y_{jj} & \cdots & Y_{jk} & \cdots & Y_{jh} & \cdots \\ Y_{k1} & \cdots & Y_{ki} & \cdots & Y_{kj} & \cdots & Y_{kk} & \cdots & Y_{kh} & \cdots \\ Y_{h1} & \cdots & Y_{hi} & \cdots & Y_{hj} & \cdots & Y_{hk} & \cdots & Y_{hh} & \cdots \\ \iddots & & & & \cdots & \cdots & & & & \ddots \end{bmatrix} \tag{6}$$

where Y_{ij} represents the admittance of a link that connects nodes i and j, $Y_{ii} = -\sum_{j \neq i} Y_{ij}$. If there is no link between nodes i and j, $Y_{ij} = 0$.

Therefore, with the network topology, power consumption and generation information known, the voltage of nodes in the power grid can be determined using Equation (5) and the currents flowing in the transmission lines can be calculated accordingly as

$$I_{ij} = (v_i - v_j) \times Y_{ij} \tag{7}$$

We define the load of node i at time t as its power

$${L_i}^P(t) = v_i \times I_{oi} \tag{8}$$

where I_{oi} represents the total currents flowing out of node i. Moreover, the load of link k at time t is defined as the current through it

$${L_{ij}}^P(t) = I_{ij} \tag{9}$$

The capacity of node i is α_1 times its initial load ${L_i}^P(0)$ and the capacity of every transmission line is α_2 times its initial load $L_{ij}^P(0)$.

$$C_i = {L_i}^P(0) \times \alpha_1 \tag{10}$$

$$C_{ij} = {L_{ij}}^P(0) \times \alpha_2 \tag{11}$$

where α_1 and α_2 are tolerance parameters, which denote the safety margins of the nodes and links in the power grid, respectively.

2.2. Communication Network Model

In this paper, we adopt the data traffic model [30] to model the communication network and the nodes in the communication network are considered as selfish ones [31,32]. In this model, new packets are generated randomly with source and destination nodes selected and then transmitted along the shortest paths. Therefore, the traffic load of node i at time t, denoted by ${L_i}^C(t)$, can be estimated by its current betweenness [33]

$${L_i}^C(t) = \sum_{j,\, k \in \mathcal{N},\, j \neq k \neq i} \frac{n_{jk}^i}{n_{jk}} \tag{12}$$

where $\mathcal{N}$ is the set of nodes in CN, n_{jk} is the total number of shortest paths between nodes j and k, and n_{jk}^i is the number of shortest paths between nodes j and k that pass through node i.

Similar to the power grid, the capacity of node i is β times its initial load ${L_i}^C(0)$

$$C_i = \beta \times {L_i}^C(0) \tag{13}$$

where β is the tolerance parameter in CN; similarly, we set $\beta > 1$.

2.3. Interdependent Mechanism

Different from previous interdependent models, the interdependent mechanisms proposed in this paper include: (i) coupling mode between networks and (ii) failure propagation object. The coupling mode reflects the topological structure of CPS, while the failure propagation object reflects the process of failure propagation, both of which will directly affect the robustness of CPS.

2.3.1. Coupling Mode

In this paper, we consider CPS coupled in three ways as follows:

(i) Assortative coupling (AC)
The nodes in PG and CN are sequentially connected according to the values of capacity in descending order.

(ii) Disassortative coupling (DC)
The nodes in PG and CN are sequentially connected according to the values of capacity in descending order for PG and ascending order for CN.

(iii) Random coupling (RC)
The nodes in PG and CN are randomly connected one by one.

2.3.2. Failure Propagation Object

In previous studies, Node–Node was used as the failure propagation object for the interdependent mechanism of these models, but the case of Node–Link as the failure propagation object was neglected. Therefore, in this paper, we consider that the object of failure propagation in CPS consists of the following two cases:

(i) Node–Node propagation
As shown in Figure 1b, when node A in PG fails and is removed, there is a probability P that its corresponding node in the communication network will also fail. Similarly, when node B in CN fails and is removed, its corresponding node A in PG will be removed with the probability P.

(ii) Node–Link propagation
As shown in Figure 1c, when node A in PG fails and is removed, each link of its counterpart B will be removed with the probability P. Similarly, when node B in CN fails and is removed, each link of its counterpart node A in PG will be removed with the probability P. It is worth emphasizing that when all links of the node fail, the node can be considered as removed.

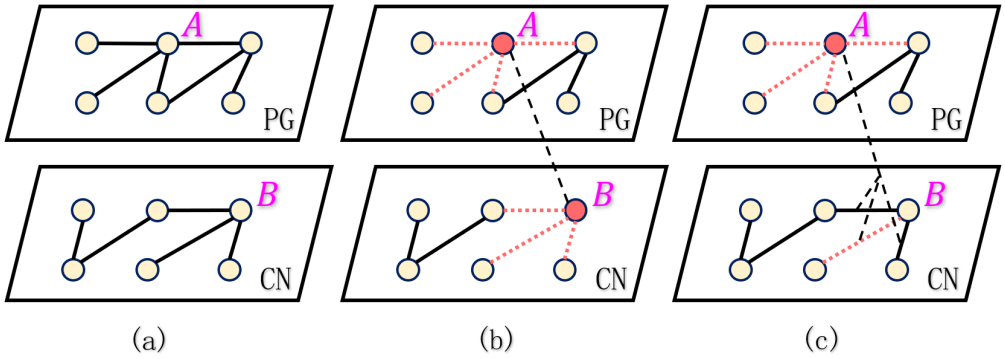

Figure 1. The diagram of failure propagation. Nodes A and B are interdependent. (**a**) Without failure; (**b**) Node–Node failure propagation; (**c**) Node–Link failure propagation.

In combination with different coupling modes and failure propagation objects, there are six interdependent mechanisms proposed in this paper: (Node–Node, AC), (Node–Node, DC), (Node–Node, RC), (Node–Link, AC), (Node–Link, DC) and (Node–Link, RC). Meanwhile, considering that CPS in this paper is not based on the assumption of strong interdependence, the failure in one network will affect the objects (nodes or links) in another network with a certain probability P.

2.4. Cascading Process

In the system, when nodes are removed, whether due to random failure or intentional attacks, the flow distribution is disrupted, causing a redirection of loads throughout the entire network. This can trigger a cascade of overload failures. In this paper, we investigate the cascading failures in the CPS through planting an initial attack. During the cascading failure process, network topology will change constantly, and the network may become fragmented into some disconnected parts. In each part of the power grid, if there are no generators, then all nodes in this part will not have any power supply and are considered unserved, even if they are not overloaded. In the same way, in each part of the communication network, the nodes outside the giant component are also considered as unserved. In addition, if the load on a node surpasses its capacity, the node is considered to fail and will be taken out of the network.

In the CPS model, in addition to node failures caused by the overload and connectivity of the network itself, the failure of a node in one network may result in the failure of its counterpart node in the other network due to the interdependent mechanism. Due to different failure propagation objects, the impact of the failure in one network on the other network is different. The failure node of one network makes the node or links of its counterpart fail in another network with a probability. To accurately reflect the weak interdependence between the two networks, we introduced the failure propagation probability, denoted as P. This probability represents the probability of a failure in one network spreading to the other network. Referring to Figure 2, we provide a detailed description of the simulation process as follows.

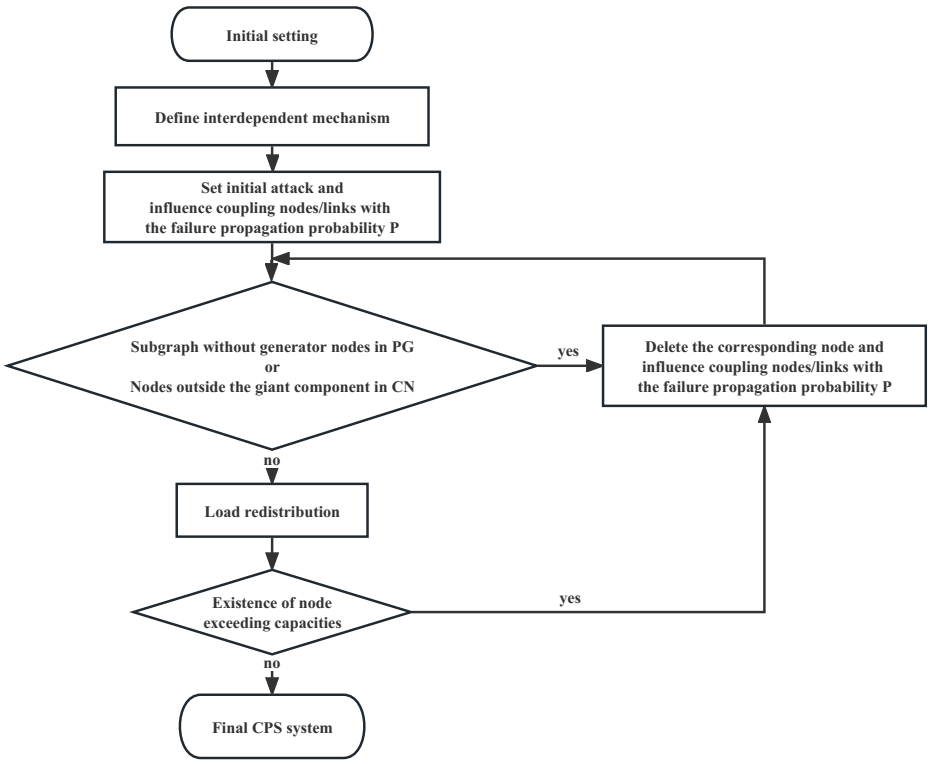

Figure 2. The flowchart of cascading failure process in CPS.

(i) **Initial setting.** At the start of the simulation, we set the parameters in the power grids based on the model described above, including the electrical characteristics (such as voltage) in the power grid. We then calculate the initial load of each node and set its capacity based on that.

(ii) **Interdependent mechanism.** In this paper, the interdependent mechanism of CPS is constructed by coupling mode and failure propagation object. Firstly, each node between two networks will be coupled by a coupling mode, such as assortative, disassortative and random. Then the failure propagation object of the interdependent mechanism in the system will be determined as Node–Node or Node–Link. After the above steps, we have completely established the interdependent mechanism of CPS in this simulation.

(iii) **Initial attack.** In this simulation, we consider an intentional attack scenario. After the initial settings, the node with the highest load in PG and CN are selected as the targets of an intentional attack. These nodes will then be removed from the network.

(iv) **Cascading failure.** Once the initial targets of the attack have been removed, the next step is to detect the connected subgraphs in each network of the CPS. In the PG, any subgraphs that do not contain a generator are considered unserved and then will be removed from the network. For each of these nodes that are removed from the PG, due to the interdependent mechanism, its corresponding node in the CN may be affected. When Node–Node is used as the failure propagation object, its counterpart node in the CN will be removed with the failure propagation probability P; when Node–Link is used as the failure propagation object, all the links of its counterpart node in the CN will be removed with the failure probability P. In the CN, nodes that are not part of the giant component are unserved and taken out of the network. As a result of the interdependent mechanism, the counterpart node in the PG will also be impacted by the removal of these nodes in the CN.

(v) **Load redistribution.** Next, the updated loads in both networks are calculated and any nodes that have become overloaded are removed. The interdependent mechanism between the two networks is considered and the counterpart nodes or links of the removed nodes are checked to see if they have failed, using the failure propagation object and the failure propagation probability.

(vi) If no removal occurred during steps iv or v, then output the final system. Otherwise, go to step iv.

2.5. Robustness Metric

In a network, the relative size of the giant connected component after the cascades is usually used to represent its robustness [34,35]. Similarly, the robustness of the CPS can be defined as the extent of unserved nodes after cascading failures. Therefore, without loss of generality, the percentage of unserved nodes (PUN) is defined as

$$PUN = \frac{N_{unserved}}{N_{total}} \tag{14}$$

where $N_{unserved}$ is the total number of unserved nodes of the CPS after cascading failures. N_{total} is the total number of initial nodes in the CPS.

3. Simulations

As described in Section 2.3, the interdependent mechanism directly affects the robustness of CPS. Therefore, we first focus on the effect of different interdependent mechanisms (including coupling mode and failure propagation object) on the robustness of CPSs. In addition, considering that it is difficult to change the interdependent mechanism of CPSs in reality, we then focus on different strategic node protection for CPSs and find the most effective strategic node protection to improve the robustness of CPSs. In the following simulations, we model the topology of each single network in the CPS using the Barabási–Albert (BA) scale-free network model, which has 118 nodes and 348 links. As described in

Sections 2.1 and 2.2, we consider the electrical model and data traffic model for our model. Specifically, we assume that each generator has a voltage of 1 p.u. and that each consumer node has a current consumption of 1 p.u. We also assume a total of 14 generators and set the admittance of each transmission link to 11 p.u. [36]. To simplify the analysis, we set the tolerance parameters of the power grid model as $\alpha = \alpha_1 = \alpha_2 (\alpha > 1)$.

3.1. The Impact of Interdependent Mechanisms on the Robustness of CPSs

3.1.1. Coupling Mode

The coupling mode is one of the important factors in the interdependent mechanism of CPSs. The change of coupling mode will change the topology of the CPS and then affect the failure propagation process. Thus, it is natural to study how different coupling modes (including assortative, disassortative and random) affect the robustness of CPSs with the failure propagation probability P. Figure 3 shows this relationship for two failure propagation objects: Node–Node propagation (a) and Node–Link propagation (b). As seen in Figure 3, the PUN value has increasing failure propagation probability under any coupling mode. This trend can be easily explained, as a higher failure propagation probability can make the interdependency across networks stronger which means the failure in the network will be more easily propagated to another network and then results in the value of PUN being higher after cascading failure. In addition, take Node–Node propagation as an example (refer to Figure 3a). When the failure propagation probability P is small ($P < 0.2$), the robustness of the CPS under three coupling modes is relatively poor; when P is large, the value of PUN is the largest when the disassortative coupling is chosen in the interdependent mechanism of CPS, which means that the robustness of CPS is the worst when the disassortative coupling is chosen. These results suggest that coupling mode and failure propagation probability all have a great impact on the robustness of CPSs. A CPS has the worst robustness when two networks are disassortatively coupled. At the same time, increasing the failure propagation probability, the interdependency across networks increases. Thus, the value of PUN increases after cascading failures when the failure propagation probability increases and the robustness of the CPS decreases gradually due to the strengthened interdependency across networks.

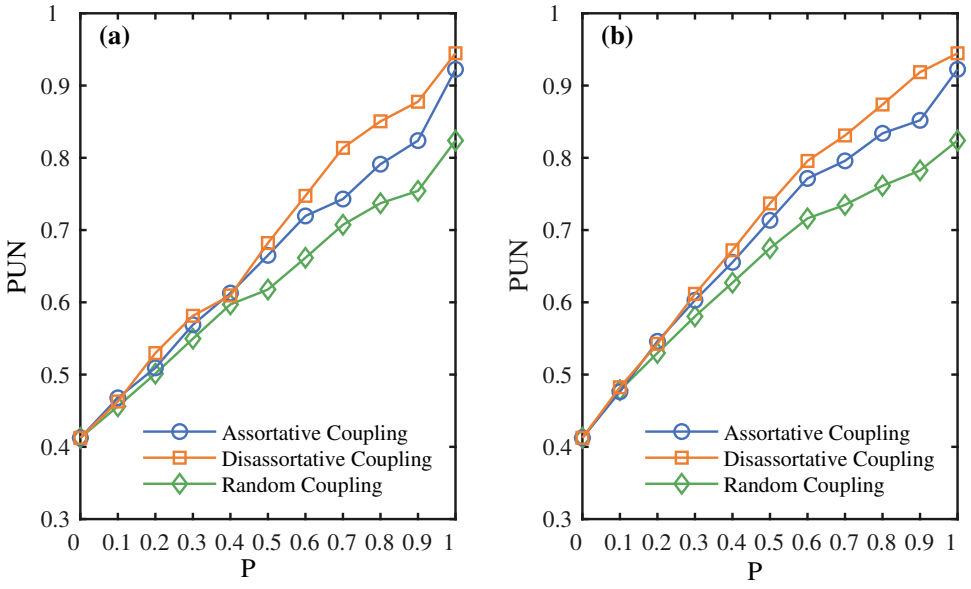

Figure 3. Robustness of CPS changes as a function of failure propagation P under three coupling modes. (**a**) Node–Node propagation; (**b**) Node–Link propagation.

3.1.2. Failure Propagation Object

The interdependent mechanism is not only constructed via coupling mode. Failure propagation object is also an important factor in the interdependent mechanism of CPS. In previous studies, Node–Node has been taken as the failure propagation object in the interdependent mechanism of CPS, while Node–Link as the failure propagation object has been ignored. Based on the proposed interdependent mechanism in our model, we then focus on the impact of failure propagation objects on the robustness of CPS.

Figure 4 gives the impact of failure propagation object and failure propagation probability P on PUN under three coupling modes. Take the assortative coupling as an example (refer to Figure 4a). Primarily, the value of PUN increases as the probability of failure propagation increases under any failure propagation object and we can see a noteworthy phenomenon, that is, that CPS has different sensitivities to the failure propagation objects. Specifically, the corresponding curve of Node–Node is lower than the curve of Node–Link with the same failure propagation probability and coupling mode. This result indicates that choosing Node–Node as the failure propagation object in the interdependent mechanism of CPS can cause a lower value of PUN than choosing Node–Link as the failure propagation object when the same coupling mode is chosen. Combining the actual situation, the result means that choosing Node–Node mode in the interdependent mechanism of CPS has a more positive impact on the robustness of CPS. The reason for this phenomenon is that when Node–Link is the failure propagation object in the interdependent mechanism of CPS, the number of objects affected by the interdependent mechanism significantly increases, which means that under the same failure propagation probability, the number of links affected by the interdependent mechanism is more than for chosen Node–Node mode. Therefore, the strength of the interdependent relationship in CPS is increased, which leads to more serious consequences of cascading failures of the system. In particular, when failure propagation probability P is equal to 1, the values of PUN corresponding to the two failure propagation objects are the same. This is because, whether choosing Node–Node or Node–Link as the failure propagation object, the networks in CPS are strongly interdependent when P = 1, which means that the failure of a node in one network will cause its corresponding node in the other network to fail immediately. Similarly, when failure propagation probability P is equal to 0, there is no interdependency between the two networks in the system and it is only the result of the independent cascading failure process of the two networks. This is why the values of PUN corresponding to the two failure propagation objects is also the same.

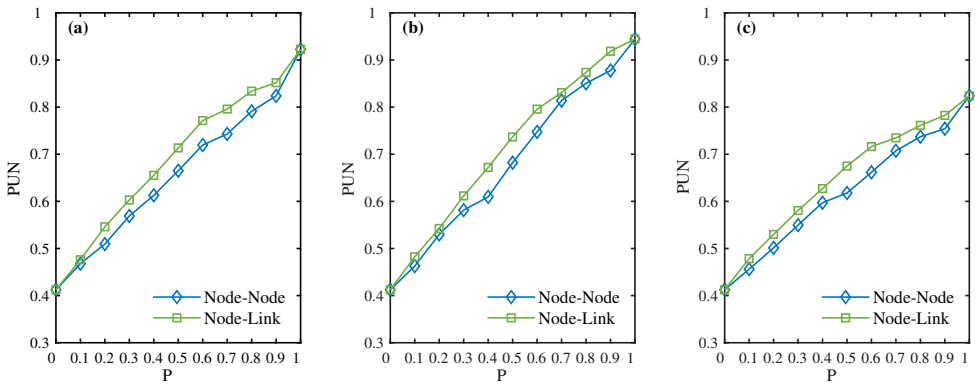

Figure 4. Robustness of CPS changes as a function of failure propagation P under two propagation objects. (**a**) Assortative Coupling; (**b**) Disassortative Coupling; (**c**) Random Coupling.

3.2. The Impact of Protection Strategies on the Robustness of CPS

In Section 3.1, we successfully constructed the interdependent model of CPS proposed in this paper, then studied the impact of the interdependent mechanism (including coupling mode and failure propagation object) on the robustness of CPS by considering the influence

of links and nodes in the networks. However, the interdependent mechanisms in many real-world systems are usually stable, which means that the robustness of these systems cannot be improved by changing the coupling mode or failure propagation object in the interdependent mechanism of the system. For the purpose of reducing the harm caused by the cascading failure of CPS, we often take protection strategies on important nodes to indirectly improve the robustness of CPS and prevent node failure when the interdependent mechanism of the system cannot be changed. Therefore, the protection strategies on important nodes for CPS are particularly important.

Before choosing strategic node protection for CPS, we should firstly determine the interdependent mechanism of CPS. Without loss of generality, we choose random coupling in the interdependent mechanism of the system. Therefore, in this simulation, there are two corresponding interdependent mechanisms for the CPS, (Node–Node, RC) and (Node–Link, RC); we then analyze the robustness of CPS under several strategies for protecting critical nodes. Specifically, we first assess the significance of each node in the network and arrange them in a list in decreasing order of estimated importance. We then use the ranked list of nodes to determine which ones to protect, based on their importance, which means that the top $\lfloor N\eta \rfloor$ nodes in the ranking are protected, where η is a parameter that specifies the fraction of protected nodes and N is the number of nodes. Because the main purpose of this paper is to analyze the impact of different interdependent mechanisms under weak interdependency on the robustness of CPS, the importance of the nodes considered are mainly from two aspects: (i) Degree, reflecting the node connection centrality and (ii) Load, reflecting the node functional importance. For comparison purposes, we conducted simulations using two additional methods: (i) a random protection scheme, where the nodes to be protected are chosen randomly and (ii) a scenario in which no nodes are protected, which we refer to as the "No protection".

Primarily, we study how the robustness of CPS is affected by the fraction of protected nodes, noted as η. Figure 5 shows PUN as a function of η from 0 to 1 in steps of 0.1 when failure propagation probability P is equal to 0.5. It can be observed from Figure 5 that, in two cases of different interdependent mechanisms of CPS, the value of PUN based on protecting nodes using measures of node importance is lower than using random protection scheme, which means that protecting nodes using measures of node importance significantly improves the robustness of CPS with different interdependent mechanisms. Taking the protection schemes in the PG as an example, since the protected node does not fail, the impact of failure propagation to the CN is prevented when that node fails; At the same time, when the counterpart node in the CN fails and propagates into the power grid by the interdependent mechanism of CPS, the node protected in PG will not be affected by the interdependence mechanism. So the impact of failure propagation from the CN to the PG is also prevented by protecting the nodes in the PG. In addition, it can be found that the results after the cascading failure of CPS are different when choosing to protect the important nodes in the CN or PG. From Figure 5a,b, choosing to protect the important nodes in the PG is the best protection scheme for CPS, which means that it is better improving the robustness of CPS by protecting electrical nodes when conservation resources are limited.

Figure 6 shows the effects of different protection strategies of important nodes on the robustness of CPS for two interdependent mechanisms: Node–Link, RC ((a), (b) and (c)), and Node–Node, RC ((d), (e) and (f)). We set different proportions of protected nodes in the following simulations: 0.1 ((a) and (d)), 0.5 ((b) and (e)) and 0.9 ((c) and (f)). From Figure 6, we find that compared with no node protection, any protection strategy can effectively reduce the proportion of failed nodes after cascading failure in CPS and the values of PUN increase with the increase in failure propagation probability P. This is because under limited conservation resources, the greater the failure propagation probability between networks in CPS, the easier the failure propagation from one network to another network. Meanwhile, we find an interesting result that when the protection proportion of the nodes is fixed, the protection to protect the important nodes in the PG can more effectively impede the

cascading process in the CPS and reduce the value of PUN after the cascading process, which is consistent with the previous conclusions in this paper. In particular, when η is large enough, the cascading failure can only cause a few percent of nodes because we have protected most nodes in the network. This is why the values of PUN remain constant horizontally regardless of how P changes when $\eta = 0.9$ in Figure 6c,f. However, the performance of a single PG and CN is still different. The measures to protect important electrical nodes are still better than those to protect the important communication nodes, which further shows that primarily protecting the important electrical nodes is more beneficial with respect to improving the robustness of the system.

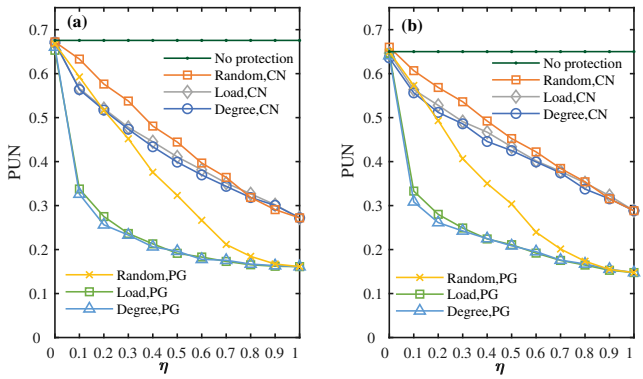

Figure 5. Robustness of CPS changes as a function of proportion of protected nodes η when P = 0.5. (**a**) Node–Link, RC; (**b**) Node–Node, RC.

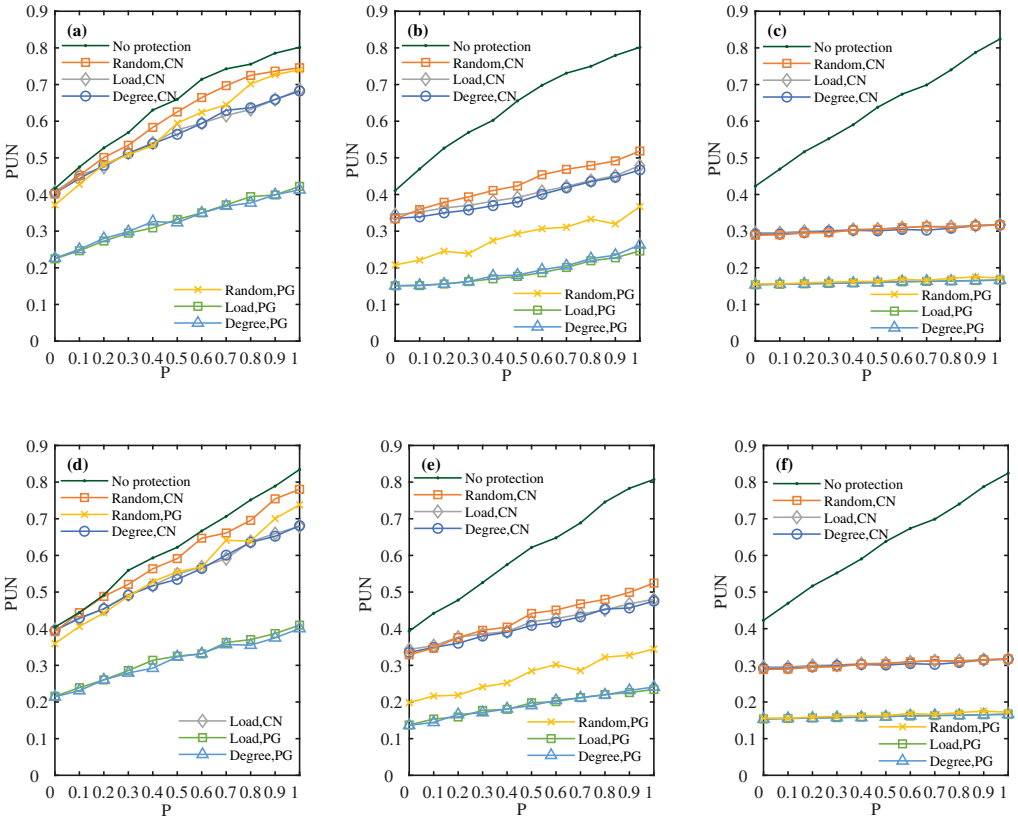

Figure 6. The effects of different protection strategies of critical nodes on Robustness of CPS under (**a**) $\eta = 0.1$, Node–Link, RC; (**b**) $\eta = 0.5$, Node–Link, RC; (**c**) $\eta = 0.9$, Node–Link, RC; (**d**) $\eta = 0.1$, Node–Node, RC; (**e**) $\eta = 0.5$, Node–Node, RC; (**f**) $\eta = 0.9$, Node–Node, RC.

4. Discussion

The above simulation results show that the CPS is the most vulnerable when the disassortative coupling is determined and the CPS is more sensitive to the failure propagation when the Node–Link is used as the failure propagation object. In addition, considering the real situation, the interdependency mechanism of CPS is often determined. Therefore, the protection strategy based on critical nodes is usually adopted to improve the CPS robustness. With limited protection resources, choosing to protect the critical nodes of the power grid improves the robustness of the CPS under deliberate attacks most significantly.

While this paper focuses on the smart grid as a specific example of a CPS, the concept of weak interdependent mechanisms can be applied to other CPSs, such as water distribution systems, intelligent transportation systems and logistic networks. The analytical method proposed in this paper has good expansibility, which can reveal the relationship between internal and external parameters and system performance with different coupling mechanisms based on the modeling of interdependent networks.

5. Conclusions

In this paper, we study a CPS by using the smart grid as an example, which is composed of a power grid and a communication network. To begin, we propose a new CPS model which considers the facts that (i) there are three coupling modes between two parts of a CPS, including assortative, disassortative and random. (ii) Failure propagation objects in a CPS include not only Node–Node but also Node–Link. These facts are seldom considered together in the interdependent mechanisms of previous studies but do exist in practice. Then, based on this model and interdependent mechanisms, we analyze the robustness of CPS with six different interdependent mechanisms. The results show that the robustness of CPS is the worst when the disassortative coupling is chosen. In addition, we consider Node–Link as the failure propagation object of the interdependent mechanism of CPS and compare it with the case that only Node–Node is considered as the failure propagation object. It is found that the robustness of CPS under intentional attacks with the Node–Node interdependent mechanism is better than that with the Node–Link interdependent mechanism. However, in many real-world systems, the failure propagation objects of the interdependent mechanisms of these systems are Node–Link. This is why most CPSs in real-world systems will be less robust than in previous studies under intentional attacks. Finally, based on the strategic node protections, the results show that primarily protecting the important electrical nodes is more beneficial to improving the robustness of the system.

Due to the weak interdependent mechanism in CPS, we use simulation results to show the robustness of CPSs and find the most beneficial node protection to enhance the robustness of CPSs. It is important to understand the interdependent mechanisms of a complex system like the CPS and theoretical analysis can provide valuable insights in this regard. Hence, it is a direction worth exploring in future work to further analyze the model and gain a deeper understanding of the system.

Author Contributions: Conceptualization, P.W., H.T. and Y.X.; methodology, P.W.; formal analysis, P.W. and Q.W.; investigation, Q.W.; writing—original draft preparation, P.W.; writing—review and editing, Q.W. and H.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Zhejiang Provincial Natural Science Foundation of China under Grant No. LQ23F030012 and the Fundamental Research Funds for the Provincial Universities of Zhejiang (Grant No. GK229909299001-018).

Data Availability Statement: The data that support the findings of this study are available from the authors upon reasonable request.

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

References

1. Loveček, T.; Straková, L.; Kampová, K. Modeling and Simulation as Tools to Increase the Protection of Critical Infrastructure and the Sustainability of the Provision of Essential Needs of Citizens. *Sustainability* **2021**, *13*, 5898. [CrossRef]
2. Carter, B.; Adams, S.; Bakirtzis, G.; Sherburne, T.; Beling, P.; Horowitz, B.; Fleming, C. A Preliminary Design-Phase Security Methodology for Cyber–Physical Systems. *Systems* **2019**, *7*, 21. [CrossRef]
3. Li, N.; Wang, F.; Magoua, J.J.; Fang, D. Interdependent effects of critical infrastructure systems under different types of disruptions. *Int. J. Disaster Risk Reduct.* **2022**, *81*, 103266. [CrossRef]
4. Xia, Y.; Small, M.; Wu, J. Introduction to focus issue: Complex network approaches to cyber–physical systems. *Chaos Interdiscip. J. Nonlinear Sci.* **2019**, *29*, 093123. [CrossRef]
5. Xu, S.; Tu, H.; Xia, Y. Resilience enhancement of renewable cyber–physical power system against malware attacks. *Reliab. Eng. Syst. Saf.* **2023**, *229*, 108830. [CrossRef]
6. Serru, T.; Nguyen, N.; Batteux, M.; Rauzy, A. Modeling Cyberattack Propagation and Impacts on Cyber–Physical System Safety: An Experiment. *Electronics* **2023**, *12*, 77. [CrossRef]
7. Babadi, N.; Doustmohammadi, A. A moving target defence approach for detecting deception attacks on cyber–physical systems. *Comput. Electr. Eng.* **2022**, *100*, 107931. [CrossRef]
8. Zhang, Y.; Jiang, T.; Shi, Q.; Liu, W.; Huang, S. Modeling and vulnerability assessment of cyber physical system considering coupling characteristics. *Int. J. Electr. Power Energy Syst.* **2022**, *142*, 108321. [CrossRef]
9. Yu, X.; Xue, Y. Smart grids: A cyber–physical systems perspective. *Proc. IEEE* **2016**, *104*, 1058–1070. . jproc.2015.2503119. [CrossRef]
10. Lázaro, J.; Astarloa, A.; Rodríguez, M.; Bidarte, U.; Jiménez, J. A Survey on Vulnerabilities and Countermeasures in the Communications of the Smart Grid. *Electronics* **2021**, *10*, 1881. [CrossRef]
11. Alonso, M.; Turanzas, J.; Amaris, H.; Ledo, A.T. Cyber–physical vulnerability assessment in smart grids based on multilayer complex networks. *Sensors* **2021**, *21*, 5826. [CrossRef] [PubMed]
12. Tu, H.; Gu, F.; Zhang, X.; Xia, Y. Robustness analysis of power system under sequential attacks with incomplete information. *Reliab. Eng. Syst. Saf.* **2023**, *232*, 109048. [CrossRef]
13. Muir, A.; Lopatto, J. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. 2004. Available online: https://www.osti.gov/etdeweb/biblio/20461178 (accessed on 26 January 2023).
14. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Trans. Power Syst.* **2016**, *32*, 3317–3318. [CrossRef]
15. 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]
16. Gao, J.; Buldyrev, S.V.; Stanley, H.E.; Havlin, S. Networks formed from interdependent networks. *Nat. Phys.* **2012**, *8*, 40–48. [CrossRef]
17. Zhang, Y.; Yağan, O. Robustness of interdependent cyber–physical systems against cascading failures. *IEEE Trans. Autom. Control.* **2019**, *65*, 711–726. [CrossRef]
18. Chen, L.; Yue, D.; Dou, C.; Cheng, Z.; Chen, J. Robustness of cyber–physical power systems in cascading failure: Survival of interdependent clusters. *Int. J. Electr. Power Energy Syst.* **2020**, *114*, 105374. [CrossRef]
19. Akella, R.; Tang, H.; McMillin, B.M. Analysis of information flow security in cyber–physical systems. *Int. J. Crit. Infrastruct. Prot.* **2010**, *3*, 157–173. [CrossRef]
20. Tu, H.; Xia, Y.; Wu, J.; Zhou, X. Robustness assessment of cyber–physical systems with weak interdependency. *Phys. A Stat. Mech. Its Appl.* **2019**, *522*, 9–17. [CrossRef]
21. Jiang, J.; Xia, Y.; Xu, S.; Shen, H.L.; Wu, J. An asymmetric interdependent networks model for cyber–physical systems. *Chaos Interdiscip. J. Nonlinear Sci.* **2020**, *30*, 053135. [CrossRef]
22. Kazawa, Y.; Tsugawa, S. Robustness of networks with skewed degree distributions under strategic node protection. In Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, USA, 10–14 June 2016; Volume 2, pp. 14–19. [CrossRef]
23. Wang, Z.; Hill, D.J.; Chen, G.; Dong, Z.Y. Power system cascading risk assessment based on complex network theory. *Phys. A Stat. Mech. Its Appl.* **2017**, *482*, 532–543. [CrossRef]
24. Kracík, J.; Lavička, H. Fluctuation analysis of high frequency electric power load in the Czech Republic. *Phys. A Stat. Mech. Its Appl.* **2016**, *462*, 951–961. [CrossRef]
25. Yang, R.; Wang, W.X.; Lai, Y.C.; Chen, G. Optimal weighting scheme for suppressing cascades and traffic congestion in complex networks. *Phys. Rev. E* **2009**, *79*, 026112. [CrossRef] [PubMed]
26. Xiao, F.; Li, J.; Wei, B. Cascading failure analysis and critical node identification in complex networks. *Phys. A Stat. Mech. Its Appl.* **2022**, *596*, 127117. [CrossRef]
27. Motter, A.E. Cascade control and defense in complex networks. *Phys. Rev. Lett.* **2004**, *93*, 098701. . physrevlett.93.098701. [CrossRef] [PubMed]
28. Candelieri, A.; Galuzzi, B.G.; Giordani, I.; Archetti, F. Vulnerability of public transportation networks against directed attacks and cascading failures. *Public Transp.* **2019**, *11*, 27–49. [CrossRef]

29. Zhang, X.; Zhan, C.; Chi, K.T. Modeling the dynamics of cascading failures in power systems. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2017**, *7*, 192–204. [CrossRef]
30. Wu, J.; Zeng, J.; Chen, Z.; Chi, K.T.; Chen, B. Effects of traffic generation patterns on the robustness of complex networks. *Phys. A Stat. Mech. Its Appl.* **2018**, *492*, 871–877. [CrossRef]
31. Ibrahim, A.S.; Seddik, K.G.; Liu, K.R. Improving connectivity via relays deployment in wireless sensor networks. In Proceedings of the IEEE GLOBECOM 2007—IEEE Global Telecommunications Conference, Washington, DC, USA, 26–30 November 2007; pp. 1159–1163. [CrossRef]
32. Liu, Y.; Garnaev, A.; Trappe, W. Maintaining throughput network connectivity in ad hoc networks. In Proceedings of the 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Shanghai, China, 20–25 March 2016; pp. 6380–6384. [CrossRef]
33. Freeman, L.C. A set of measures of centrality based on betweenness. *Sociometry* **1977**, *40*, 35–41. [CrossRef]
34. Tan, F.; Xia, Y.; Zhang, W.; Jin, X. Cascading failures of loads in interconnected networks under intentional attack. *EPL (Europhys. Lett.)* **2013**, *102*, 28009. [CrossRef]
35. Tu, Haicheng and Xia, Yongxiang and Iu, Herbert Ho-Ching and Chen, Xi. Optimal robustness in power grids from a network science perspective *IEEE Trans. Circuits Syst. II Express Briefs* **2019**, *66*, 126–130. [CrossRef]
36. Zhang, X.; Tse, C.K. Assessment of Robustness of Power Systems From a Network Perspective. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2015**, *5*, 456–464. [CrossRef]