

Cascading Failure Based on Load Redistribution of a Smart Grid with Different Coupling Modes^{*}

WenJie Kang¹, PeiDong Zhu^{2*}, and Gang Hu¹

¹ College of Computer, National University of Defense Technology, Changsha 410073, China

² Department of Electronic Information and Electrical Engineering, Changsha University, Changsha 410022, China

{kangwenjie, pdzhu, hugang}@nudt.edu.cn

* Corresponding Author

Abstract. As one of the most important properties of the power grid, the voltage load plays an important role in the cascading failure of the smart grid and load redistribution can accelerate the speed of the failure by triggering more nodes to overload and fail. The subnet structure and different coupling modes also affect the robustness of the smart grid. However, the research on the effect of load, subnet structure and coupling mode on the cascading failure of the smart grid is still rare. In this paper, the smart grid with two-way coupling link consists of a power grid with small world topology and a communication network with scale-free topology. An improved load-capacity model is applied to overload-induced failure in the power grid and node importance (NI) is used as an evaluation index to assess the effect of nodes on the power grid and communication network. We propose three kinds of coupling modes based on NI of nodes between the cyber and physical subnets, i.e., Random Coupling in Subnets (RCIS), Assortative Coupling in Subnets (ACIS) and Disassortative Coupling in Subnets (DCIS). In order to improve the robustness of the smart grid, a cascading failure model based on load redistribution is proposed to analyze the influence of different coupling modes on the cascading failure of the smart grid under both a targeted attack and random attack. Some findings are summarized as: (I) The robustness of the smart grid is improved by increasing the tolerance α . (II) ACIS applied to the bottom-up coupling link is more beneficial in enhancing the robustness of the smart grid than DCIS and RCIS, regardless of a targeted attack or random attack.

Keywords: Cascading failure · Load redistribution algorithm · Node importance · Two-way coupling relationship.

1 Introduction

As a kind of critical infrastructure, the smart grid is considered as an interdependent network with two-way coupling links[1]. Most recently, Buldyrev et

^{*} Supported by National Natural Science Foundation of China (Grants 61572514 and 61501482) and Changsha Science and Technology Program (Grant K1705007)

al.[2] utilized the idea of complex networks to establish a mathematical model in order to explain the principle of cascading failure. However, many complex network models did not consider functional features, which do not reflect the real situation of the smart grid[3]. For instance, the characteristics of power flow can trigger load redistribution when some nodes fail. In addition, interdependence between cyber and physical networks may cause the cascading failure of interdependent networks. When a cyber node fails, it can cause its coupled physical node to fail and may lead to the failure of more physical nodes due to overload; in turn, those failed physical nodes will result in the failure of more coupled cyber nodes.

Buldyrev et al. [4] used "giant component" to represent the functional integrity of the composite network when a network is divided into multiple small components, and they establish a framework to analyze the mechanism of catastrophic failures in interdependent networks [5]. This framework breaks through the frontier of complex networks theory that still focuses on a single, non-interacting network[6]. Based on this theoretical model, many works used the giant component as a functional component to study the effect of partial support-dependence relationship [7] and coupling strength [2] on the robustness of interdependent networks.

The load has been used to study the cascading failure of interdependent networks in recent works [7][8][9]. Han et al.[10] proposed a load-capacity model to analyze cascading failure over networks in both interdependent and isolated statuses, and simulation results prove that network robustness is positively related to capacity and negatively related to the load. When a node is removed by a random attack or targeted attack, the load of the node is distributed to its neighbors, when the load of those nodes exceeds their capacity, they will fail. Recently, more and more details were considered to enhance the robustness of interdependent networks, such as the coupling strength, support-dependence relations, coupling preferences, spatial effect, clustered structures [11], and community structure [12], etc. Cheng et al. [13] studied in detail the robustness of interdependent networks coupled with different types of networks under both targeted and random attack. Babaei et al.[14] found that the robustness of modular small-world networks is improved by increasing inter-community links against both random and targeted attacks. Tian et al. [12] found that the number of inter-community connection is positively related to the robustness of interdependent modular scale-free (SF) networks.

However, the giant component used as the largest connected set of nodes does not apply to the smart grid, because the smaller components are still functional as long as the generation nodes and load nodes coexist in these components. Similarly, degree[12], betweenness [15][16], the degree of degree[17] considered as the node load also does not satisfy the reality, because they are still the properties of network structure and cannot be used to represent network function. In most cases, many interdependent networks have multiple dependency links, local dependency links, and two-way dependence links. Coupling relationship

between the physical and cyber network is not one-on-one correspondence[18] but two-way dependency[19].

In order to effectively enhance the robustness, China state power corporation has established a strategy that allows the physical nodes provide power supply to uncoupled cyber nodes. This means that we need to know which coupling mode will be beneficial in enhancing the robustness of the smart grid. As such, we propose three coupling modes between nodes in cyber and physical networks, i.e. Random coupling in subnets (RCIS), Assortative coupling in subnets (ACIS) and Disassortative coupling in subnets (DCIS). Secondly, node importance (NI) is defined to evaluate the influence of nodes on the network. We divided two coupling edges into the top-down coupling link and the bottom-up coupling link. Three coupling modes are established by applying ACIS, DCIS, and RCIS to the bottom-up coupling link when the top-down coupling link remains unchanged. The load redistribution caused by power flow is considered in the cascading failure of interdependent networks.

The rest of this paper is organized as follows. In Section 2, we propose the coupling model of the smart grid. In Section 3, Experiments and analysis are presented, and Section 4 concludes this paper and discusses the future work.

2 Coupling Model of the Smart Grid

The smart grid consists of a power grid and a communication network. The power grid and the communication network can be divided into many subnets in terms of geographical location of substations and each subnet is considered an autonomous system. Fig 1 shows two-layer network structure of a smart grid. The upper network is a communication network and different colored nodes form different subnets. Square nodes represent control centers and circular nodes represent measuring/controlling nodes. The lower network is a power grid that contains generation nodes and load nodes. There are internal edges and coupling edges in the smart grid, the internal edge is the link between nodes in a single network and coupling edge is the link between two-layer networks. Coupling edge has two types: $P \rightarrow C$ and $C \rightarrow P$. P represents the physical layer and C represents the communication layer. $C \rightarrow P$ is named the top-down coupling link and is shown as the red dotted edges in Fig. 1. $P \rightarrow C$ is named the bottom-up coupling link and is shown as the black dotted edges in Fig 1.

Definition 1: The smart grid can be described by $SG = \{V, E, R\}$, where node set $V = \{V^P, V^C\}$ contains the physical node set V^P and the cyber node set V^C . The coupling relationship is $R = \{r_{ij} | i \in V^P, j \in V^C\}$, and node i belongs to V^P and node j belongs to V^C . The power grid is described by $V^P = \{v_1^G, v_2^G, \dots, v_m^G, v_1^L, v_2^L, \dots, v_n^L\}$, where v_i^G represents the generation node i and v_j^L represents the load node j that contains transmission nodes and distribution nodes. The communication network is described by $V^C = \{v_1^C, \dots, v_k^C, v_1^M, \dots, v_q^M\}$, where v_i^C represents the control center node i and v_j^M represents the measuring/controlling node j .

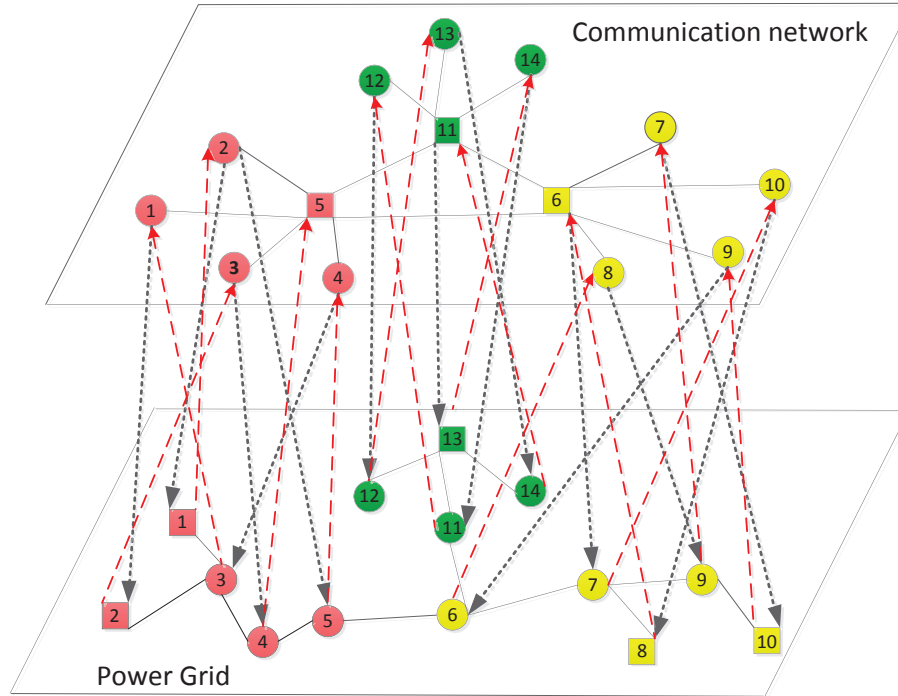


Fig. 1. The framework of the smart grid. Different colored nodes form different subnets and there is coupling relationship between nodes in same colored subnets. The red dotted edges represent the bottom-up coupling links and the black dotted edges represent the top-down coupling links.

Coupling relationship matrix R is used to describe dependence between the power grid and communication network. $R_{PC}(i, j) = r_{pi \rightarrow cj} = 1$ indicates that cyber node j depends on the physical node i . $R_{CP}(j, i) = r_{cj \rightarrow pi} = 1$ indicates that the physical node i depends on the cyber node j . $R_{PC}(i, j)$ or $R_{CP}(j, i) = 0$ indicates that there is no dependency relationship between nodes i and j . Here, special explanation $(R_{PC}(i, j) = 1) \neq (R_{CP}(j, i) = 1)$.

2.1 Node Importance Assessment in the Power Grid

The power grid is a special network, which contains the functional characteristic of the power flow. The power flow can cause the load of failed substations to distribute their neighbor nodes. When the load of a substation exceeds its capacity, it will fail. This will result in a new round load redistribution until there is no overloaded node. Wang et al.[9] used $w_{im} * w_{jn}$ as the initial load of an edge e_{ij} to study the cascading failure of interdependent networks, where $w_{im} = (k_i * k_m)^\alpha$ represents the coupled strength between two coupled nodes i and m , and k_i is the degree of node i . Similarly, Han et al.[10] used λs_i^α as

the initial load of node i to establish cascading load model, where s_i represents the total weights of all edges connected with node i . Crucitti et al. [20] used the total number of most efficient paths passing through node i as its initial load to study the cascading failure in complex networks. The load of a node is defined as the betweenness centrality in order to study the cascading failure of interdependent networks [12]. Similarly, the initial load of the node i is represented by the betweenness B_i of the node that is defined as the number of the shortest paths between pairs of nodes over the network passing through the node i [21][22].

It is clear that the load mentioned in the above literatures belongs to structural attributes (e.g., betweenness, degree, and coupled strength etc.) rather than functional attributes (e.g., electric current, voltage, frequency, active power, and reactive power etc.). This assumption has certain irrationality. In fact, high voltage or low voltage exceeding a certain threshold may cause substations to fail. In addition, the voltage is associated with active power and reactive power; therefore, the load of substations is defined as its voltage and is written as:

$$L(v_i) = Vol_i \quad (1)$$

where $L(v_i)$ is the load of node i and Vol_i represents the voltage of node i .

Definition 2: The capacity of nodes is defined as tolerance capacity to deal with load changes. The capacity of node i can be described by (2), where α represents a tolerance parameter. \pm represents the range of normal operation of substations, which means that the change of the voltage above α or below α can lead to the failure of node i .

$$C(v_i) = (1 \pm \alpha) * L(v_i) \quad (2)$$

Δf_{ij} represents the proportions of load distribution that the load of the failed node is distributed to the adjacent nodes by computing the impedance of the link between two nodes. $B(i)$ denotes neighbor nodes set of node i . I_{ij} denotes the impedance of a branch between node i and node j . I_{ik} represents the impedance of all branches passing through the node i and I_{Max} is the maximum value of I_{ik} . $\frac{1+(I_{Max}-I_{ij})}{(\sum_{k \in B(i)} I_{ik})}$ indicates that the larger the impedance of the branch is, the smaller the power flow passing through this branch is, which means that the smaller proportion of the load is distributed to the node j . β is a parameter, which determines that the load loss of node i is increased or decreased to its adjacent nodes. $\beta = 1$ denotes that load change $|\Delta f_{ij}| * L(v_i)$ of node i is added to the load of its neighbor node j , $\beta = -1$ denotes that the load of neighbor node j is reduced by $|\Delta f_{ij}| * L(v_i)$.

$$\Delta f_{ij} = \beta * \frac{1 + (I_{Max} - I_{ij})}{(\sum_{k \in B(i)} I_{ik})} \quad (3)$$

Definition 3: Node importance (NI) is used as an evaluation index to assess the influence of a failed node on the power grid, where f_i^P denotes failure node

set in which the failure of all nodes is caused by a failed node i due to overload. $n(f_i^P)$ denotes the size of failure node set. NI is described as:

$$NI(v_i^p) = n(f_i^P) \quad (4)$$

The algorithm of load redistribution can be expressed as follows:

Step 1(Initialization): Get information on the load of each node and the impedance of each branch.

Step 2(Node Failure): A node is removed from the physical node set V^P . It will lead to the load of the failed node to be distributed to its neighbor nodes by Δf_{ij} .

Step 3(Load Redistribution): If the removed node is load node, the load is distributed to neighbor nodes by Formula 3 and $\beta = 1$. If the removed node is the generation node, the load of its neighbor nodes changes to zero on the instant, then, the neighbor node's load of their neighbors will be distributed to them by Formula 3 and $\beta = -1$.

Step 4(Judgment of failure nodes): If the load of a node exceeds the range of its capacity, it will fail. This will break the overall equilibrium of the load and triggers a new round load redistribution.

Step 5(Iteration): Repeat step 3 and 4 until the network achieves stabilization state.

Step 6(Getting NI): Obtain FNS of the failed node until all nodes are handled.

2.2 Node Importance Assessment in the Communication Network

The communication network is an abstract overview of SCADA systems/ Energy Management Systems (EMS) in a smart grid, which is mainly responsible for collecting data and transmitting information. Therefore, the node passed by the bigger information flow has a significant role in transmitting data. Due to the real-time nature of information flow, we have no way to simulate the propagation of data flow in an experimental environment. As such, we assume that the cyber node with a bigger degree has large data transmission because its neighbor nodes must transmit data through it. Therefore, the degree can be used as an evaluation index to assess the importance of cyber nodes. In addition, The NI of cyber nodes also relies on the NI of its coupled physical nodes.

Definition 4: Node importance (NI) in the communication network depends on the degree of nodes and NI of the coupled physical nodes. The bigger degree is, the more important node is. When the degree of two nodes is different, the NI depends on its degree. When two nodes have the same degree, the NI of those cyber nodes depends on the NI of their coupled physical nodes. Where k_i is the degree of the cyber node i , NI_{Max} is the maximum of NI of physical nodes.

$$NI_i^C = k_i + \sum_{R_{CF}(j,i)=1} \frac{NI_j^P}{NI_{Max}^P} \quad (5)$$

2.3 Three Coupling Modes Based on Node Importance

The coupling mode refers to the connection mode of nodes between the cyber and physical networks and has three types: assortative coupling in subnets, disassortative coupling in subnets and random coupling in subnets. The coupling edges contain the top-down coupling link and the bottom-up coupling link. The former indicates that cyber nodes provide the physical nodes with remote monitoring, measurement and controlling. The latter indicates that physical nodes provide power support to the cyber nodes.

The aim of our research is to study which coupling mode applied to the coupling edges can enhance the robustness of interdependent networks. The research object is part of China power grid. Due to the long distance between the two substations, a cyber node coupled with a substation cannot monitor and control another substation. As such, three different coupling modes cannot be applied to the top-down coupling link. However, a substation can provide power-supply to another cyber node by accessing a wire. Similarly, long distances will increase costs, we can divide the cyber and physical network into multiple small subnets and apply ACIS, DCIS, and RCIS to the bottom-up coupling link to study how to improve the robustness of a smart grid when the top-down coupling link remains unchanged. We assume that the communication network A and the power grid B are divided into multiple subnets A_1, A_2, \dots, A_n and B_1, B_2, \dots, B_n , respectively. A_1 and B_1 have the same geographical area, similarly A_2 and B_2, \dots, A_n and B_n .

Random coupling in subnets (RCIS): The top-down coupling link between A and B keeps unchanged. A node in B_1 is randomly chosen to connect to a node in A_1 with one-to-one correspondence until all nodes are handled. Repeat this process until all subnets are handled.

Assortative coupling in subnets (ACIS): The top-down coupling link between A and B keeps unchanged. A node with the largest NI in B_1 is connected to a node with the largest NI in A_1 , and a node with the second largest NI in B_1 is selected to couple with a node with the second largest NI in A_1 until all nodes are handled. Repeat this process until all subnets are handled.

Disassortative coupling in subnets (DCIS): The top-down coupling link between A and B keeps unchanged. A node with the largest NI in B_1 is connected to a node with the smallest NI in A_1 , and a node with the second largest NI in B_1 is selected to couple with a node with the second smallest NI in A_1 until all nodes are handled. Repeat this process until all subnets are handled.

3 Experiments and Analysis

In this section, we first use a small part of the real network, which is used as an example to evaluate our approach. The power grid consists of 154 substations and more than 192 transmission lines. The communication network contains 154 nodes and 175 lines.

Fig.2 shows that the NI in the power grid and the communication network. The NI in the power grid represents the size of failure node set in which the

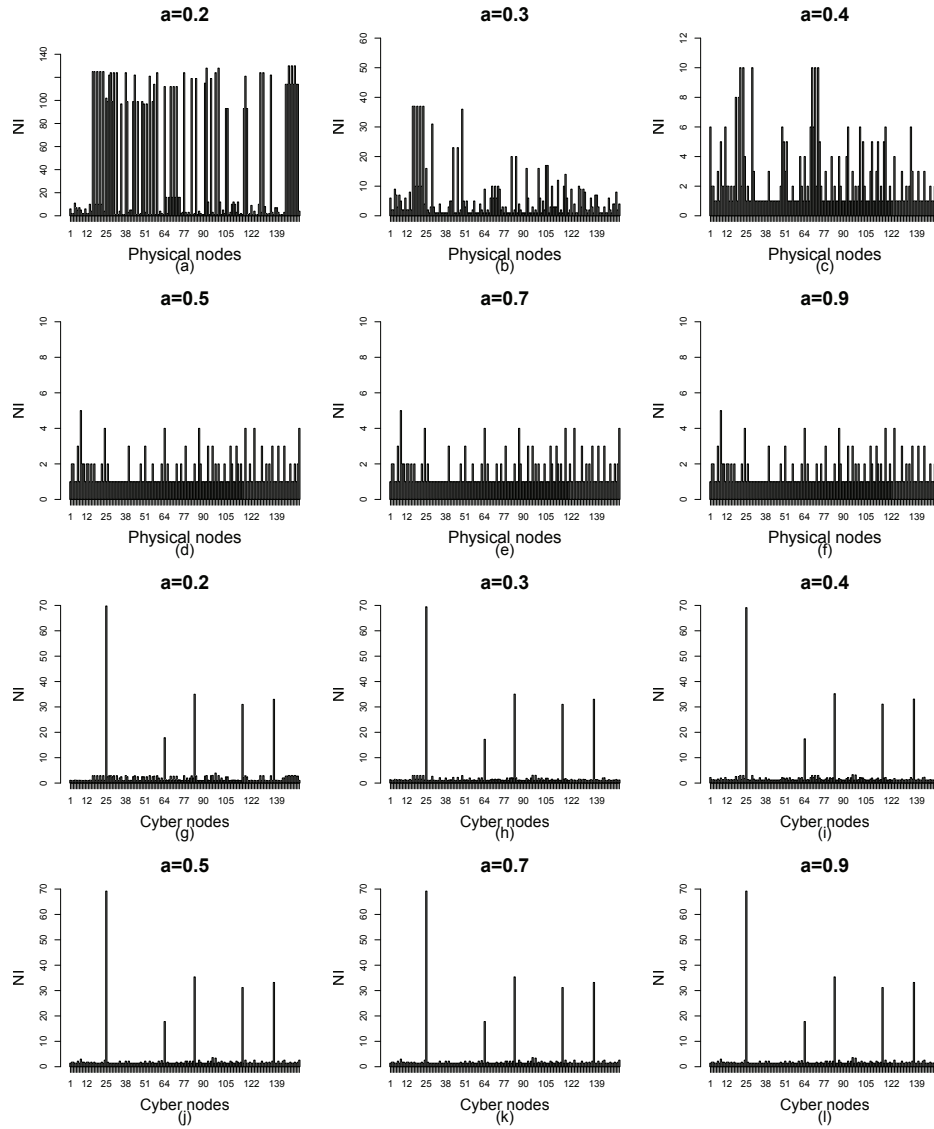


Fig. 2. (a)-(f) The NI of the power grid (g)-(i) The NI of the communication network

failure of any node is caused by a failed node. A bigger NI indicates that the removed node has a more important influence on the smart grid and the NI of each physical node is displayed with different tolerance parameter in Figs.2 (a)-(f). As α increases, NI of each node shows a downward trend, but it tends to be stable when α is greater than 0.5. When α is equal to 0.1, almost every failed node can lead to the breakdown of the entire power grid except for four

nodes. However, when α is greater than 0.5, any failed node cannot or can only cause very few node failures. The NI of the communication network is shown in Figs. 2 (g)-(i). Since the NI of the cyber nodes depends on its degree and NI of the coupled physical nodes, in addition, the NI of the physical nodes remains unchanged when $\alpha > 0.5$, the NI of the cyber nodes also has not changed. When the NI of the cyber and physical nodes is obtained, we can apply ACIS, DCIS, and RCIS to the bottom-up coupling link and simulate the cascading failure of the smart grid through removing a fraction $1 - p$ of nodes.

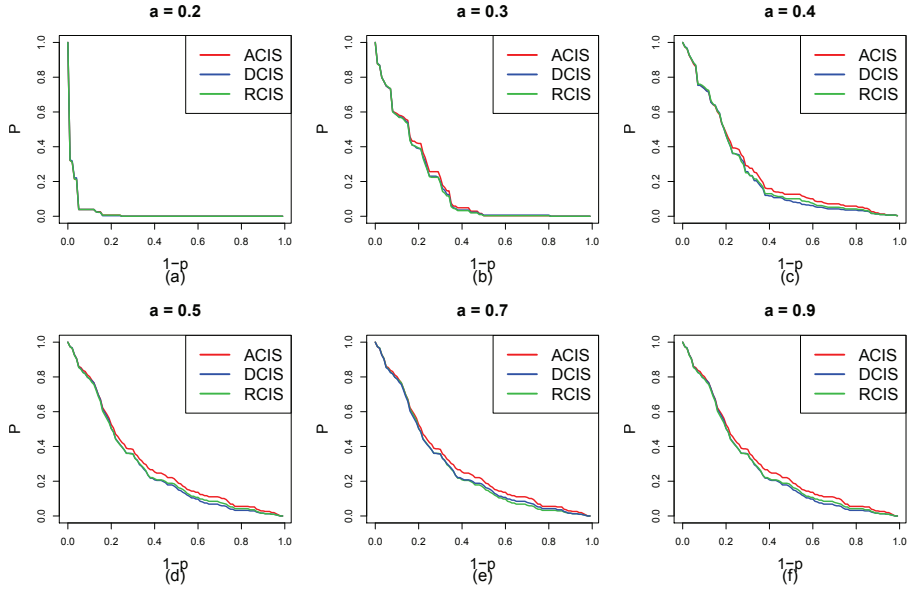


Fig. 3. The cascading failure of the smart grid according to which ACIS, DCIS, and RCIS are applied to the bottom-up coupling link under a targeted attack. (a) $\alpha = 0.2$ (b) $\alpha = 0.3$ (c) $\alpha = 0.4$ (d) $\alpha = 0.5$ (e) $\alpha = 0.7$ (f) $\alpha = 0.9$. It is clear that the ACIS applied to the bottom-up coupling link is more beneficial in enhancing the robustness of the smart grid under a targeted attack than DCIS and RCIS when $\alpha > 0.2$.

Fig.3 shows the robustness curve P of the smart grid with different α , where P represents the node survival rate after a fraction $1 - p$ of nodes is removed. A situation of $\alpha = 0.1$ is not discussed by us, because a failed node may lead to the failure of the entire power grid. When α is greater than 0.5, the curve P has no obvious change, which is because that any failed node cannot cause other nodes to fail or lead to the failure of a few nodes. This means that the robustness of interdependent networks remains unchanged when α exceeds a certain threshold. In Figs.3(a)-(f), it is easy to find that the ranking of the robustness curve P is $ACIS > DCIS > RCIS$ when a fraction $1 - p$ of nodes is removed. This means that ACIS applied to the bottom-up coupling links is better able to enhance

the robustness of the smart grid. That is because any failed physical nodes may cause the physical nodes with the smaller NI to fail, which further leads to the failure of the cyber nodes. If the physical nodes with the smaller NI are coupled with the cyber nodes with the higher NI , those failed physical nodes with the higher NI can lead to the failure of the physical nodes with the smaller NI . Furthermore, it will result in the failure of the more important cyber nodes. Therefore, ACIS applied to the bottom-up coupling link is more beneficial in enhancing the robustness of interdependent networks than DCIS and RCIS. It is clear that the robustness curve of the smart grid does not change because the power grid is sufficient to handle overload and nodes will not fail due to overload when $\alpha > 0.5$.

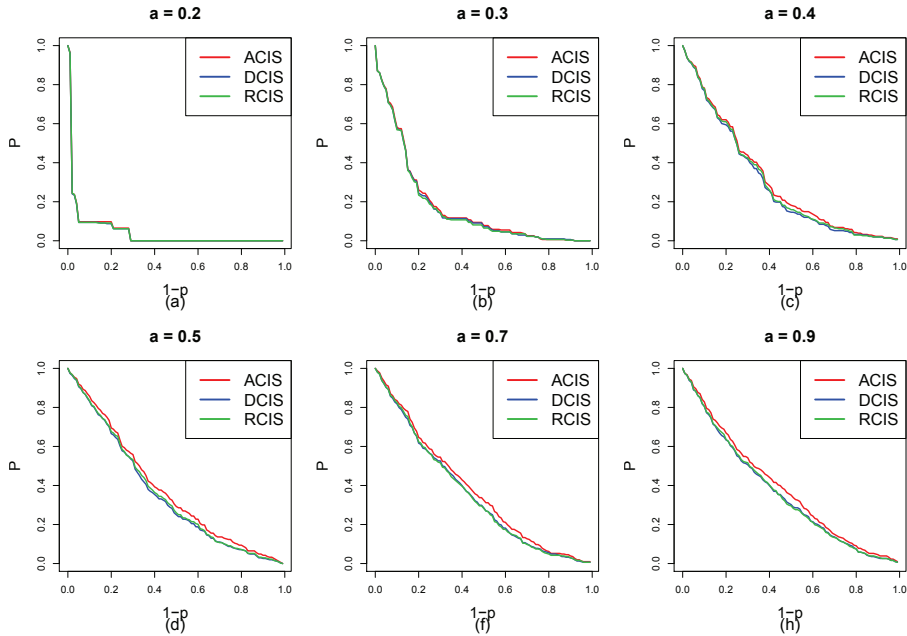


Fig. 4. The cascading failure of the smart grid according to which ACIS, DCIS, and RCIS are applied to the bottom-up coupling link under a random attack. (a) $\alpha = 0.2$ (b) $\alpha = 0.3$ (c) $\alpha = 0.4$ (d) $\alpha = 0.5$ (e) $\alpha = 0.7$ (f) $\alpha = 0.9$. It is clear that the ACIS applied to the bottom-up coupling link is more beneficial in enhancing the robustness of the smart grid under random attack than DCIS and RCIS when $\alpha > 0.2$.

The cascading failure of the smart grid according to which different coupling modes are applied to the bottom-up coupling link under random attack is shown in Fig 4. It is clear that the ranking of the robustness curve P of the smart grid is $ACIS > RCIS > DCIS$. This means that ACIS applied to the bottom-up coupling link is more beneficial in enhancing the robustness of interdependent

networks than DCIS and RCIS against random attack. When α equals 0.2, the robustness curve P suddenly drops to about zero after removing about 30 percent of the node. When α equals 0.3, the P falls to about 0.1 after removing about 50 percent of the node. When α is larger than 0.5, the power grid has enough capacity to handle the overload. Therefore, a failed node is not easy to cause other nodes to fail. At this time, the load redistribution has less impact on the cascading failure of interdependent networks and the robustness curve P is close to the function curve $y + x = 1$ when α is equal to 0.6, 0.7, 0.8, and 0.9.

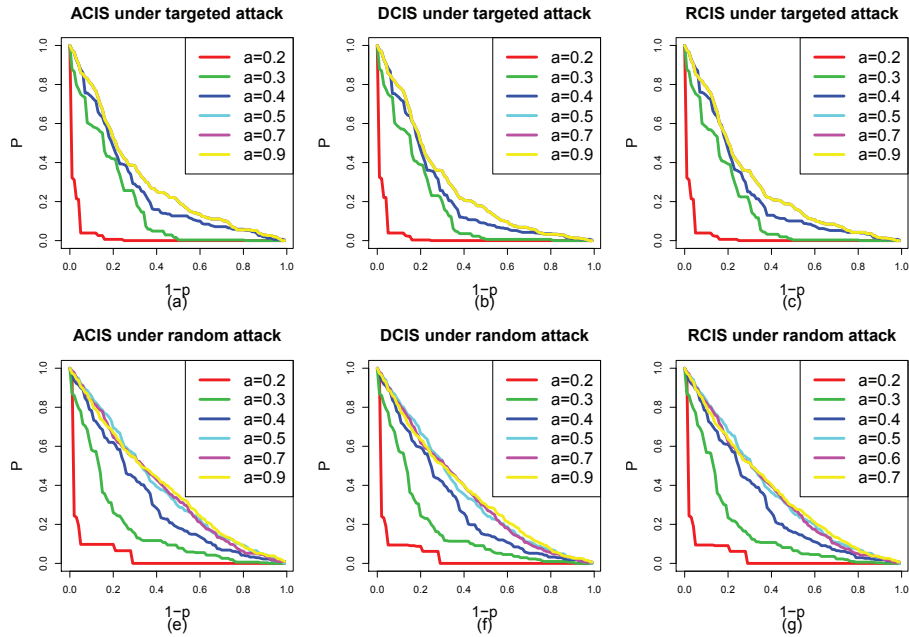


Fig. 5. A comparison of the robustness curves of the smart grid with different α according to which ACIS, DCIS, and RCIS are applied to the bottom-up coupling link. (a) ACIS under targeted attack. (b) DCIS under targeted attack. (c) RCIS under targeted attack. (d) ACIS under random attack. (e) DCIS under random attack. (f) RCIS under random attack. It is clear that α is positively related to the robustness of the smart grid when $\alpha \leq 0.5$.

Figs. 5 (a)-(g) show that the robustness curve P of the smart grid with different α according to which ACIS, DCIS, and RCIS are applied to the bottom-up coupling link. It is clear α is positively related to the robustness of the smart grid regardless of ACIS, DCIS, and RCIS against both targeted attack and random attack when $\alpha \leq 0.5$, but it has less impact on the robustness of the smart grid when α is larger than 0.5. This is why the yellow line of $\alpha = 0.9$ covers other lines of $\alpha = 0.5$ and $\alpha = 0.7$ in Figs.5 (a)-(c). Two interesting

conclusions can be drawn as follows: (I) ACIS applied to the bottom-up coupling link is more beneficial in enhancing the robustness of the smart grid than DCIS and RCIS regardless of a targeted attack or random attack when the top-down coupling link remains unchanged. (II) The robustness of interdependence network is improved by increasing the tolerance parameter α . Our research results can provide a meaningful guidance for network architects in order to improve the robustness of interdependent networks.

4 Conclusion

In this paper, we describe a special research scenario that different coupling modes are applied to the bottom-up coupling link when the top-down coupling link remains unchanged. This means that we study which coupling mode applied to the bottom-up link ($P \rightarrow C$) can enhance the robustness of a smart grid when the top-down coupling link ($C \rightarrow P$) remains unchanged. The voltage is used as the load of physical nodes to simulate load redistribution of failed nodes caused by power flow. The NI is used as an evaluation index to assess the influence of nodes on the communication network and power grid. Based on the NI, we proposed three coupling modes between the physical and cyber layers, i.e., ACIS, RCIS, and DCIS. Experiment results indicate that the robustness of the smart grid can be improved by increasing tolerance α , and we also find that the ACIS applied to the bottom-up coupling link is more beneficial in enhancing the robustness of the smart grid than RCIS and DCIS, regardless of a targeted attack or random attack.

In the future, we can extend the research scenario to the cyber-physical systems that different coupling modes are applied to both the top-down coupling link and the bottom-up coupling link. In addition, we can study the influence of ACIS, DCIS, and RCIS applied to different network types (e.g., Erdos-Renyi network, Small-World network, Scale-Free network, etc.) on the interdependent networks. The effect of global coupling and local coupling on the interdependent networks is also a very interesting direction. In fact, two coupled networks have different the number of nodes and the coupling relationship between the cyber and physical nodes is multiple-to-multiple correspondence. As such, the more complex coupling models are established in order to study the influence of network type, coupling mode, coupling link, coupling strength, and asymmetric coupling between the cyber and physical layer on the robustness of interdependent networks.

References

1. Rosato V, Issacharoff L, Tirittico F, et al. Modelling interdependent infrastructures using interacting dynamical models[J]. *International Journal of Critical Infrastructures*, 4(1/2), 63-79,(2008).
2. 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.[J]. *Physical Review Letters*, 105(4), 048701,(2010).

3. Gao J, Buldyrev S V, Stanley H E, et al. Percolation of a general network of networks.[J]. Physical Review E Statistical Nonlinear & Soft Matter Physics, 88(6), 062816 (2013).
4. Buldyrev S V, Parshani R, Paul G, Stanley H E, & Havlin S. Catastrophic cascade of failures in interdependent networks[J]. nature, 464, 1025-1028 (2010).
5. Vespignani A. Complex networks: The fragility of interdependency[J]. Nature, 464(7291), 984 (2010).
6. Chakravartula S. Complex networks: Structure and dynamics[J]. Dissertations & Theses - Gradworks, 424(4-5),175308 (2014).
7. Dong G, Tian L, Zhou D, et al. Robustness of n interdependent networks with partial support-dependence relationship[J]. Epl, 102(102), 68004 (2013).
8. Chen Z, Du W B, Cao X B, et al. Cascading failure of interdependent networks with different coupling preference under targeted attack[J]. Chaos Solitons & Fractals the Interdisciplinary Journal of Nonlinear Science & Nonequilibrium & Complex Phenomena, 80, 7-12 (2015).
9. Wang J, Li Y, Zheng Q. Cascading load model in interdependent networks with coupled strength[J]. Physica A Statistical Mechanics & Its Applications, 430, 242-253 (2015).
10. Han H, Yang R. Improvement on Load-Induced Cascading Failure in Asymmetrical Inter-dependent Networks: Modeling and Analysis[J]. Mathematical Problems in Engineering, 2015(8),1-10 (2015).
11. Huang X, Shao S, Wang H, et al. The robustness of interdependent clustered networks[J]. EPL (Europhysics Letters), 101(1),18002-18007(6) (2012).
12. Tian M, Wang X, Dong Z, et al. Cascading failures of interdependent modular scale-free networks with different coupling preferences[J]. Epl, 111(1) (2015).
13. Cheng Z, Cao J. Cascade of failures in interdependent networks coupled by different type networks[J]. Physica A Statistical Mechanics & Its Applications,430, 193-200 (2015).
14. Babaei M, Ghassemieh H, Jalili M. Cascading Failure Tolerance of Modular Small-World Networks[J]. Circuits & Systems II Express Briefs IEEE Transactions on, 58(8), 527-531 (2011).
15. Cai Y, Cao Y, Li Y, et al. Cascading Failure Analysis Considering Interaction Between Power Grids and Communication Networks[J]. IEEE Transactions on Smart Grid, 7(1), 530-538 (2016).
16. Zhao Z, Zhang P, Yang H, et al. Cascading failures in interconnected networks with dynamical redistribution of loads[J]. Physica A-statistical Mechanics and Its Applications,433, 204-210 (2015).
17. Yan J, Zhu Y, He H, et al. Multi-Contingency Cascading Analysis of Smart Grid Based on Self-Organizing Map[J]. Information Forensics & Security IEEE Transactions on, 8(4), 646 - 656 (2013).
18. Havlin S. Robustness of a network formed by n interdependent networks with a one-to-one correspondence of dependent nodes[J]. Physical Review E Statistical Nonlinear & Soft Matter Physics, 85(6), 3112-3113 (2012).
19. Habib M F. Cascading-Failure-Resilient Interconnection for Interdependent Power Grid - Optical Networks[C]// Optical Fiber Communications Conference and Exhibition. IEEE, 1-3 (2015).
20. Crucitti P, Latora V, Marchiori M. Model for cascading failures in complex networks[J]. Physical Review E Statistical Nonlinear & Soft Matter Physics, 69(4 Pt 2), 045104 (2004).

21. Zhang J, Song B, Zhang Z, et al. An approach for modeling vulnerability of the network of networks[J]. *Physica A Statistical Mechanics & Its Applications*, 412(10), 127-136 (2014).
22. Q. Hua, "Attack structural vulnerability of power grids: a hybrid approach based on complex networks," *Physica A: Statistical Mechanics and its Applications*, 2010, 389(3), pp. 595-603