Hindawi
International Transactions on Electrical Energy Systems
Volume 2022, Article ID 5820126, 13 pages
https://doi.org/10.1155/2022/5820126

Research Article

An Effective Node-To-Edge Interdependent Network and Vulnerability Analysis for Digital Coupled Power Grids

Yifan Li,[1] Bo Wang,[1] Hongxia Wang,[1] Fuqi Ma,[1] Hengrui Ma,[2] Jiaxin Zhang,[1] Yingchen Zhang,[1] and Mohamed A. Mohamed[3]

[1]*School of Electrical and Automation, Wuhan University, Wuhan, Hubei 430072, China*
[2]*Tus-Institute for Renewable Energy, Qinghai University, Xining, Qinghai 810016, China*
[3]*Electrical Engineering Department, Faculty of Engineering, Minia University, Minia 61519, Egypt*

Correspondence should be addressed to Bo Wang; whwdw@whu.edu.cn

Received 25 July 2022; Revised 20 August 2022; Accepted 23 August 2022; Published 29 September 2022

Academic Editor: Martin Calasan

With the deep coupling between the cyber side and the physical side of power systems, the failure of any link of both sides may lead to power outages, so it is necessary to analyze their vulnerability and vulnerable links for targeted improvement of systems. By dynamically attacking the coupled network nodes, this paper proposes a multilevel model and node-to-edge cyber-physical power system and the corresponding indexes system to analyze the vulnerability of the coupled power grid and its key components. The results showed that in the order of the indexes proposed in this paper, attacking surviving power nodes and cyber nodes results in a network crash rate of 25.0% and 66.7% faster than that in the order of "betweenness" and that attacking surviving cyber nodes results in a network crash rate of 89.4% faster than that in the order of "degree." In terms of attacking power nodes, the index proposed in this paper has the same rate as "degree." Therefore, the proposed model can better describe the vulnerability of the power grid to withstand attacks.

1. Introduction

With the digital transformation of modern power systems, the number of sensors of power systems, intelligent terminals, and decision-making units of information systems has surged [1]. A growing amount of external information directly or indirectly affects the power system through various business channels, bringing convenience to the power system [2]. However, physical power systems and electrical power communication networks (EPCN) are deeply coupled to form the cyber-physical power systems (CPPS) [3, 4], which makes it more likely to form interactive chain faults and further expand the scale of power accidents [5, 6]. For instance, blackouts in Ukraine in 2015 and Venezuela in 2019, both linked to cyber-attacks, caused huge loses to the national economy [7, 8]. The deep coupling between the cyber side and the physical side of power systems leads to the superposition of structural vulnerability and increases the possibility of expanding the fault range. Therefore, to maintain the security and stability of the power system, it is necessary to identify the vulnerable and critical components or devices and master the system structure vulnerability so as to carry out targeted and differentiated maintenance of complex and diverse devices and improve the system stability.

Related studies about vulnerability evaluation of CPPS are primarily based on two kinds of modeling, cosimulation [9–12] and complex networks [13–18].

The advantages of cosimulation lie in clear physical meaning and accurate calculation results. The authors in Ref. [9] developed a WAMS cyber-physical testbed using a real-time digital simulator with hardware-in-the-loop simulation integrating hardware, software, and wide area measurement systems components and protocols. In Ref. [10], the authors proposed a state-caching-based synchronization mechanism to balance accuracy and efficiency. In Ref. [11], a virtualized cyber-physical testbed was developed using real industrial communication protocols. A joint simulation platform of

cyber physical systems based on RT-LAB, OPENT, and control platform has been developed in Ref. [12]. It follows that cosimulation requires fine interface construction, and it has a limitation of high cost in platform construction, which demands the combination of hardware, software, and communication protocol.

Complex network focus on the most intuitive physical properties of networks. For power systems, the theory of complex networks is a proper tool to identify the robustness of the existing architecture from a long-term planning perspective and has better adaptability. From the perspective of model granularity, this paper introduces the modeling of CPPS by complex networks into two aspects: plant-level networks and device-level networks as follows:

In plant-level networks, a complex network model regards the power plant, substation, control center, and other plant stations as the basic nodes, which can analyze the network topology vulnerability of a large power grid with high computational efficiency. The authors in Ref. [13] came up with a flexible framework to analyze cascading effects in CPPS, with buses represented as nodes and lines represented as edges of a graph. Li et al. [14] took the substation and the dispatching terminal as the communication nodes. In Ref. [15], the authors proposed a heterogeneous interdependent network model in which the substations, control centers, and generators are abstracted as nodes. All those studies take the plant-level (bused and real stations) as the node. It is impossible to formulate targeted operation and maintenance strategies for specific devices because the model is not fine-grained enough.

In device-level networks, a complex network model regards the part of the communication business, communication devices, and power devices as the basic nodes. In Ref. [16], communication devices are mapped as the nodes, and communication links between devices are mapped as the edges, ignoring the impact of the physical grid. Qi et al. [17] and Xu et al. [18] considered the information link and took the business of the information network as the node. The latter one is practical to recognize the significant power and communication services, but they map the influence of the physical system to the edge weight or service importance of the information system. Therefore, they lack the modeling of the dynamic process of topological interaction of coupled networks, and cannot evaluate the structural robustness of the coupled network.

Literature proves that existing studies when analyzing the influence of more fine-grained components, failed to consider the impact of the chain reaction on the whole system resulting from the interdependent interaction between the component and its other side. Nonetheless, the deep coupling between the cyber side and the physical side is one of the most important reasons for the rapid expansion of the fault scope. Therefore, it is important to assess the vulnerability of networks and components, even as small as a device. In view of the mentioned above, this paper proposes a node-to-edge interdependency between EPCN and the physical power grid and a fine-grained CPPS model to analyze the vulnerability of coupled power systems. The contributions of this research are summarized as follows:

(a) Aiming at the limitation that plant-level models are not fine-grained enough, the method of a multilevel CPPS model establishment by combining the device-level model and site-level model according to the logical connection of devices in the power business.

(b) To overcome the limitation of the device-level networks caused by the lack of modeling dynamic process of topological interaction of coupled networks, a node-to-edge interdependent relationship is put forward. It can both conforms to the interaction of EPCN and physical power grids and model a device instead of an entire site.

(c) An index system of vulnerability evaluation including 3 indexes is constructed to distinguish the influence of nodes and analyze the vulnerability of power grids.

The rest of the paper is organized as follows: In Section 2, the "node-to-edge" interdependent network model is proposed. In Section 3, the fine-grained and device-level communication model of the substation is put forward and its corresponding constraint conditions are listed. In Section 4, the vulnerability evaluation of a local power grid cyber-physical system model is investigated by comparing the traditional indexes about complex networks and the indexes in this paper. Section 5 concludes this paper.

2. Node-to-Edge Interdependent Network

Although breakers control the on-off of the power line in the physical power grid, they belong to status information controlled by intelligent terminals of EPCN. Consequently, the breaker and its corresponding power line are a "cyber node-power edge" correspondence, where the device (breaker) on the cyber side is equivalent to a node, and a power line on the power side is equivalent to an edge. Based on that, this paper first introduces a variety of coupling relations of the interdependent network, and analyzes the limitations of the original interdependent network, then proposes a "node-to-edge" interdependent network model.

2.1. Theory of Interdependent Network and Its Limitations. With the development of network theory, many researchers have investigated the interaction between CPPS by extracting the topology of the power network and the cyber network to establish the dependency. Various approaches for coupling two unilateral networks into a dependent network were proposed by different researchers and classified as follows: "one-to-one" [19], "partially" [20], "multidependent" [21], "one-to-many" [22], "many-to-many" [23] interdependent networks. The models are shown in Figure 1. The interdependent network in each subfigure is made up of two-part: a power grid and an EPCN. The edge between them is called the dependent edge. Components of the grid and the EPCN were mapped to nodes. Then, a connecting edge was formed by connecting components on the same side in electrical or communication relations. The

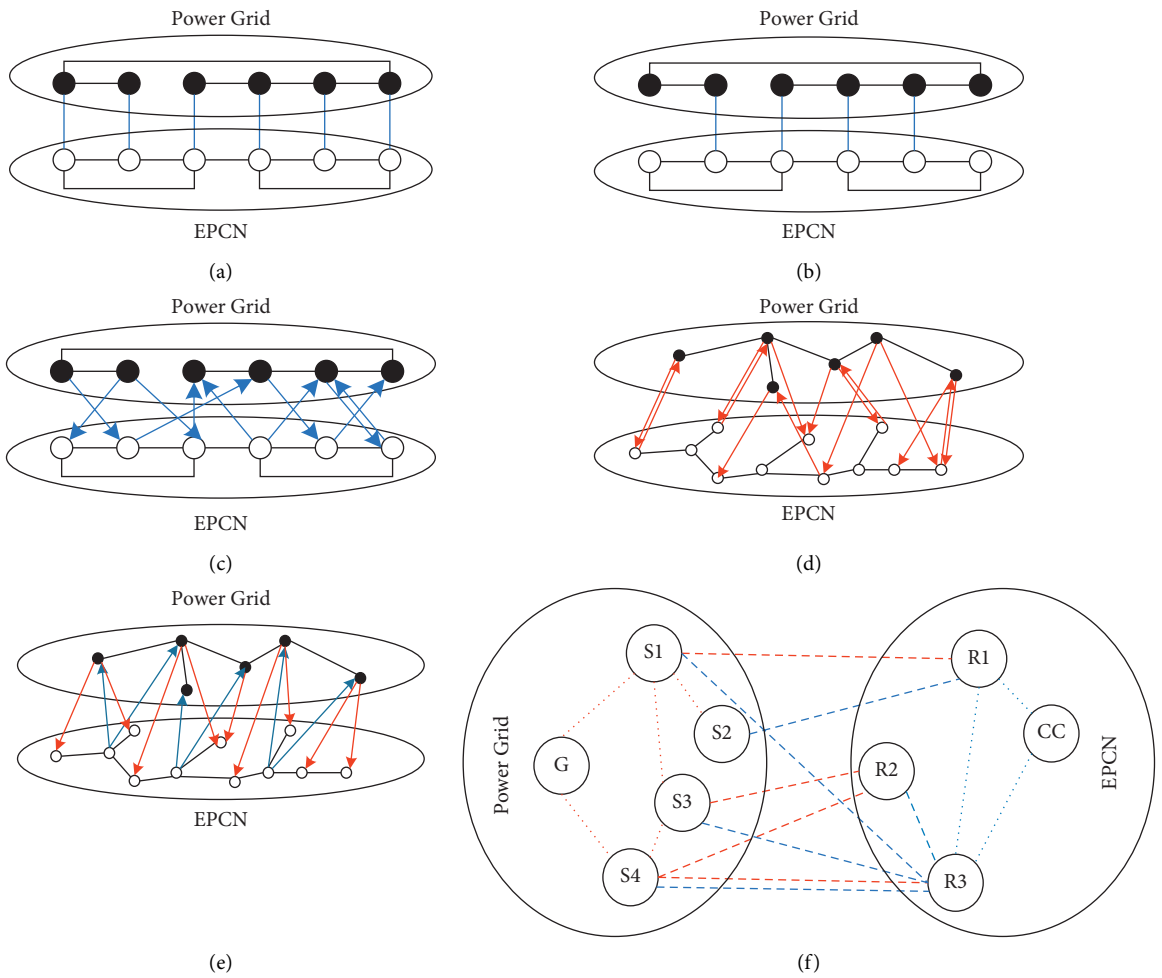

Figure 1: Origin models for interdependent networks. (a) "One-to-one" interdependent network. (b) "Partially interdependent" network. (c) Multidependent interdependent network. (d) "One-to-many" interdependent network. (e) "Many-to-many" interdependent network. (f) Cyber-physical power interdependent network considering node heterogeneity.

abovementioned models completely summarize "node-to-node" dependence relationships between two networks, which means both ends of a dependent edge are two nodes. They are suitable for cases where nodes are equivalent to plants or stations. However, when a more fine-grained model is established and a specific communication device needs to be evaluated, EPCN and power grid are not always coupled to each other through nodes. For example, there is a "device-power line" relationship between a circuit breaker and its corresponding power line as shown in Figure 2. A device is abstracted as a node, while a power line is abstracted as a connecting edge to connect two stations. Obviously, line 12 in Figure 2(a) is a complete power line, only connected and disconnected two states. But in Figure 2(b), when the system is abstracted as a graph, it is cut into three pieces so that three lines correspond to 2^3 states, which is illogical. The traditional theory cannot accurately involve the situation of coupling between "node" and "edge." This paper expands the original interdependent network and proposes a node-to-edge interdependent network model in Section 2.2, which describes the interdependent relationship between node (circuit breaker) and edge (power line).

2.2. Model of Node-to-Edge Interdependent Network

2.2.1. Model Description. Only cascading failures due to topological interactions are considered in this paper. Based on that, there are two hypotheses:

Hypothesis 1. The capacity of the power lines is sufficient.

Hypothesis 2. The capacity of generating units can meet the demand for electricity

For the "node-to-edge" interdependent network proposed here, the following descriptions are concluded based on the working characteristics of the power system:

Description 1: Faults are not transmitted between nodes in a one-sided network.

Description 2: When the node fails, all its connecting edges and dependent edges fail.

Description 3: Outliers belong to invalid nodes.

Description 4: In the initial network, if a node is connected to a dependent edge, the node will fail when the dependent edge disappears.

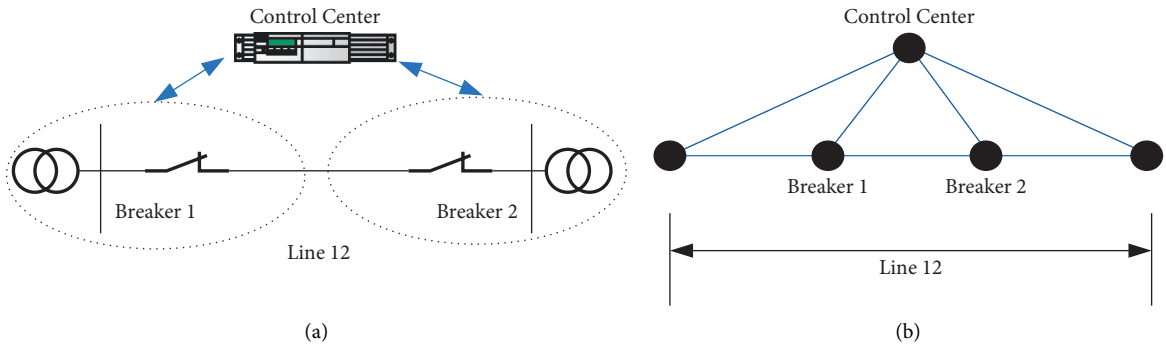

Figure 2: An example of node-to-node CPPS. (a) A micro CPPS. (b) The graph of the CPPS.

Description 5: In the initial network, if the connecting edge is connected to the dependent edge when the dependent edge disappears, the connecting edge also fails.

On the physical side, when a component disappears, the components around it can keep working after a proper scheduling process even though its working parameters will change. For the cyber side, nodes can work when they are charged. When a node fails, it cannot obtain external power and information support. So, that is why descriptions 1 and 2 are true. After a node becomes an outlier, it loses power and communication contact with the outside world and cannot affect the system. Therefore, it is a failed node, which is, why description 3 is true.

If a node is connected to a dependent edge in the initial network, it needs support from the other side of the interdependent network to keep working; otherwise, it does not need it. That is why description 4 is true. If an edge is connected to a dependent edge in the initial network, it needs support from the other side of the interdependent network to keep working; otherwise, it does not need it. That is why description 5 is true. When node failure occurs, the network structure changes according to the mentioned above.

2.2.2. Topological Change Process of the Model. A broken node is, respectively, set on both sides of the coupled network and analyzes the change process of topology. Meanwhile, this paper compares the model proposed in this paper with the "node-to-node" model with added virtual nodes (which is called the traditional model in this paper, proposed by Buldyrev et al. [19], the first people, who came up with the interdependent networks) by attacking nodes of both sides of the interdependent network. What is needed to explain first is that the attack here refers to the node being deleted from the topology due to some failure.

It is found that the "node-to-edge" model is more adaptable when the breaker is the key coupling node in terms of the topology complexity and the fault propagation mechanism.

(1) Attack on the cyber side. In the "node-to-edge" model, as shown in Figure 3(a), the black edge is the interdependent edge, the blue nodes and edges belong to the device-level EPCN, and the green nodes and edges belong to the physical power grid. Set the dark blue color as the failed node of the device-level EPCN without considering the chain failure of nodes belonging to the same network. Firstly, the dependent edge of the broken node and the connection edge of the device-level EPCN fail, as shown in Figure 3(b). Then, due to the failure of the dependent edge, the connecting edge on the physical power grid side of the dependent edge successively fails. Subsequently, the green node on the far left becomes an outlier. Thus, this isolated node fails finally. Figure 3(c) shows the ultimate maximum connected branch.

Virtual nodes are the ones with no actual meaning. Their existence is to meet the structure of the traditional model. Because present structures of the interdependent network are that both ends of dependent edges are nodes.

In the traditional model, as shown in Figure 4(a)v, virtual nodes are added at the junction of all dependent edges and physical grid connection edges. When a faulty node occurs in the device-level EPCN; both the connecting edge and the dependent edge of the corresponding device-level EPCN fail, as shown in Figure 4(b). Then, due to the failure of the dependent edge, the virtual node connected by the dependent edge in the physical power grid also fails, resulting in the disappearance of the connecting edge of the virtual node. Thus, the green node on the far left becomes an outlier, which successively fails as shown in Figure 4(c). A comparison of the two processes reveals that the results are equivalent in terms of cascading faults between networks, where the "node-to-node" model adds nodes to the physical power grid.

(2) Attack on the physical side. In the "node-to-edge" model, when a node failure occurs in the network where an edge of a dependent edge resides, the topology changes according to the descriptions in this paper, and the final steady-state is shown in Figure 5(c).

Similarly, in the traditional model, a virtual node is added at the junction of the dependent edge and the network side connecting edge, as shown in Figure 6. At this moment, the fault terminates at the established virtual node and cannot continue to propagate according to the hypotheses.

(3) Propagation mechanism of failure. In view of the topological evolution process of the abovementioned model, the following laws in the "node-to-edge" interdependent

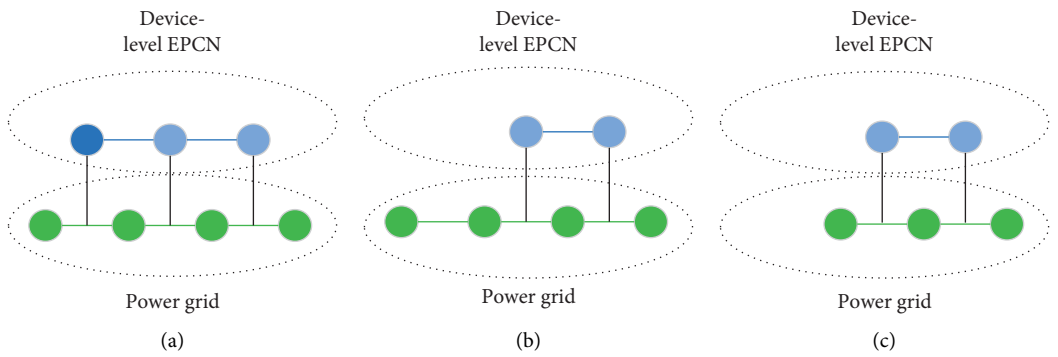

Figure 3: Cascading process of cyber node failure.

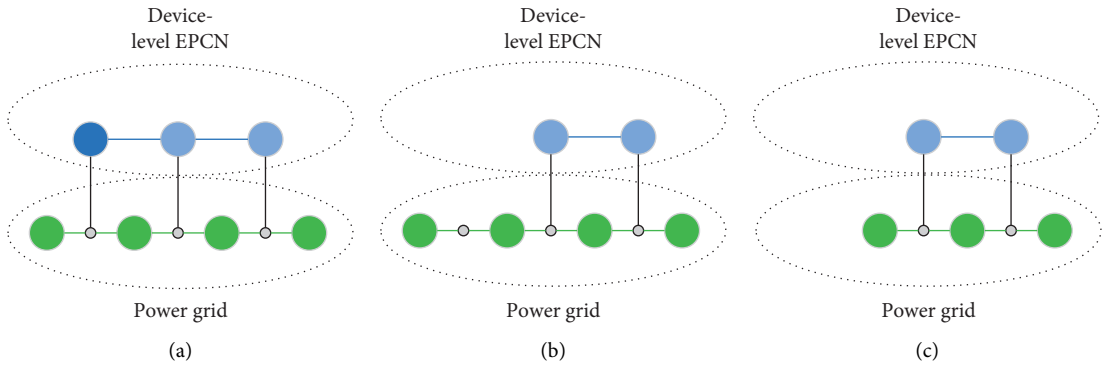

Figure 4: Cascading process with virtual nodes added to cyber node failure.

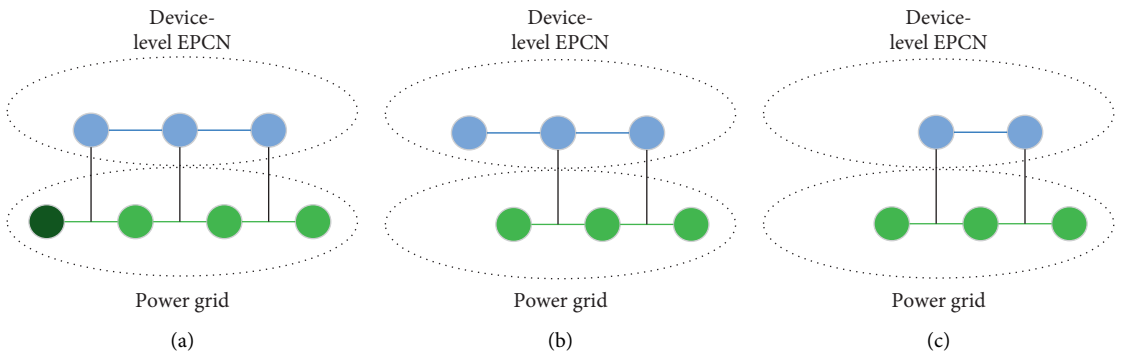

Figure 5: Cascading process of physical node failure.

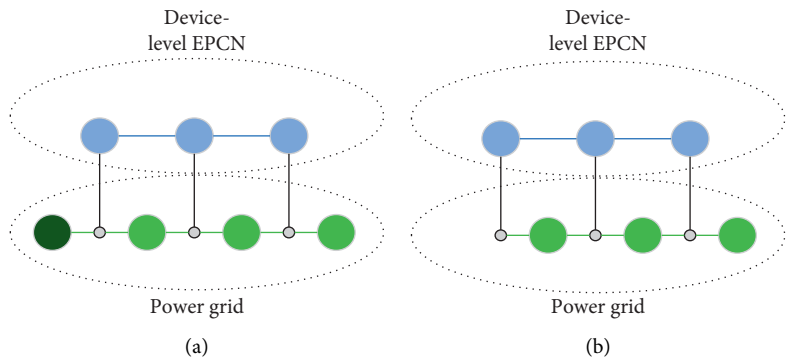

Figure 6: Cascading process with virtual nodes added to physical node failure.

network model can be summarized as follows: when one end of the dependent edge is a node and the other end is a connecting edge.

(i) Attacking a node of the network belonging to the "node" end, the model is equivalent to adding virtual nodes to the "edge" end of the "node-to-node" interdependent network. But the traditional model increases the complexity of the coupled network.

(ii) Attacking a node of the network to which the "edge" belongs, the failure may be terminated at the virtual node, to stop cross-system propagation, while it will not stop when attacking the same node in the "node-to-edge" model.

(4) Difference between the "node-to-node" model and "node-to-edge" model. As mentioned above, the difference between the two models lies in the topology complexity and the fault propagation mechanism.

(a) For the same power system, there are fewer nodes in "node-to-edge" model, because it has no virtual nodes compared with the traditional model.

(b) The node-to-node interdependent network cannot cover all coupling cases. When a node of the network to which the "edge" belongs is attacked, the resulting topologies of the two models are different. The failure may be terminated at the virtual node, to stop cross-system propagation, while it will not stop when attacking the same node in the "node-to-edge" model, that is to say, the equivalent of adding virtual nodes is conditional only in some cases. It is because the newly added nodes divide the power line into two pieces, and when an attack occurs on the side on which a newly added node lies, it will terminate at this intersection just like Figure 3(b). However, in the node-to-edge model, the edges, which are the end of dependent edges are a whole. Based original model, the undirected dependent edge model $E_{\leftrightarrow}$ is improved. Since one end of the dependent edge is a node of EPCN and the other end is an edge of the physical power grid, $E_{\leftrightarrow}$ is shown in (1)as follows:

$$E_{\leftrightarrow} = \begin{cases} \left\{ i \in V_A, j \in E_B | \left(V_{Ai}, E_{Bj} \right) \right\}, \\ \left\{ i \in V_B, j \in E_A | \left(V_{Bi}, E_{Aj} \right) \right\}, \\ \left\{ i \in V_A, j \in E_B, k \in V_B, l \in E_A | \left(V_{Ai}, E_{Bj} \right) \text{or} \left(V_{Bk}, E_{Al} \right) \right\}, \end{cases} \tag{1}$$

where V_A and V_B are, respectively, the sets of all nodes from network A and network B. E_A and E_B are, respectively, the sets of all edges from network A and network B.

3. Model of CPPS Based on Node-to-Edge Interdependent Network

In general, the control centers at all levels, power plants, and substations are regarded as undifferentiated nodes in the modeling method of cyber-physical interdependent networks. Then nodes are connected according to the actual connections. However, regarding a site as a node make it impossible to analyze the robustness of EPCN at the device level. Therefore, this paper refines the cyber-physical interdependent network composed of control centers at all levels and substations and establishes a complex network model of CPPS, of which one side is a device-level network and the other side is a plant-level network. First, the establishment of a device-level topology of a station is introduced. And then the topology of a multilevel power system is extended.

Through the establishment of the abovementioned model, this paper analyzes the vulnerability and weak links on this basis.

3.1. Device-Level Topology Modeling Based on Cyber-Physical Power Service. Compared with the abnormal alarm analyzed by a certain communication protocol, it is more intuitive for substation staff to know whether the secondary device services are running normally. Consequently, connections among services in the device business are referred to model the substation monitoring system to accurately evaluate the importance of devices inside the substation. According to the main power business that each secondary device needs to bear, the device of a smart substation can be divided into three layers: station control layer, interval layer, and process layer. The communication network model of the substation monitoring system is established as shown in Figure 7.

To simplify the model, a device-level topology model of a station is established, and the automation systems of control centers at all levels are regarded as control nodes. Each device in EPCN in each substation is regarded as a node, and the physical and cyber connection between devices is regarded as an edge. If there is information transferring between devices, such as control instructions or state information up and down, it indicates that there is a connection between the two devices.

3.2. Multilevel Topology Modeling of Power Grid and Communication Devices. Secondary devices of power systems play a critical role in power systems. It is difficult to reflect the reality of the power system to build a network model from the physical network or the EPCN only. Hence, the interaction between EPCN and the physical power grid should be taken into account. In view of that coupling relationship, the breaker is considered as the interactive node between the two systems. Consequently, this paper controls the connecting edge of the physical network through the state of the breaker node of EPCN. The bidirectional relationship between them is as follows: the circuit breaker controls the power line, and the on-off state of the power line is uploaded to the dispatching center through the circuit breaker and other devices. When a circuit breaker fails, the breaker node loses control of the power line, so the power line cannot be operated by the circuit breaker and disappears from the power topology. That is to say, the probability here is a 0–1 variable, which is 0% or 100%. It follows that one side of the model is a device-level network while the other side is a plant-level network, which is called the multilevel topology model in this paper.

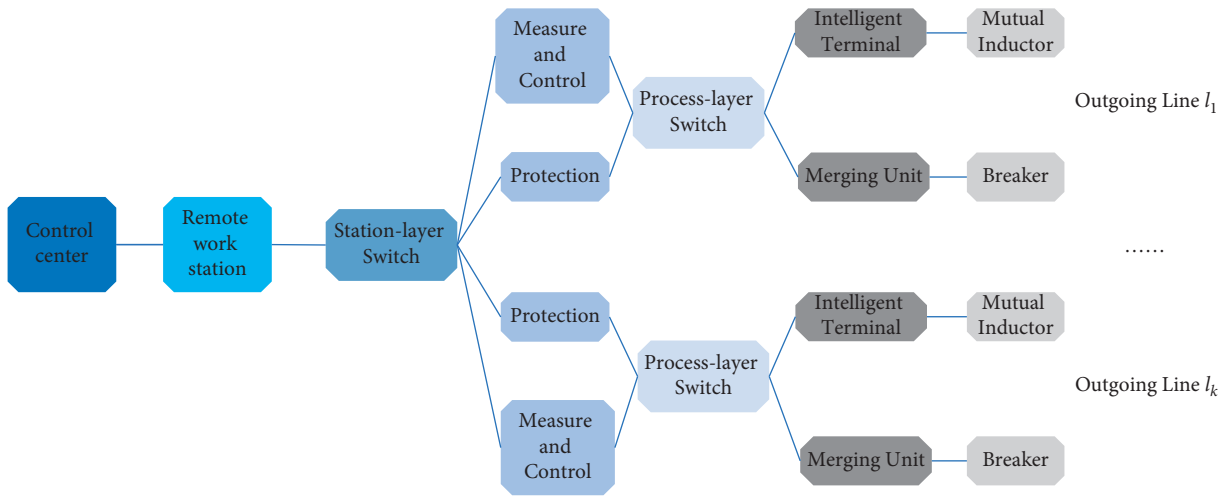

Figure 7: Communication network of substation monitoring system.

According to the topology modeling method presented in Section 2.2, for a general power grid, the steps of establishing the multilevel model are as follows:

Step 1: Model all substations based on the service chain (Section 3.1).

Step 2: Expand all the models in step 1 as the basic unit. And connect the remote workstations of the substations with the control nodes to which the substations, respectively, belong.

Step 3: Connect physical nodes according to the topology of the physical power grid.

Step 4: According to the outgoing lines of each substation, circuit breakers, and sensors, the set of all dependent edges can be obtained.

An undirected node-to-edge interdependent network model is established, accordingly. The model described above can be represented by the graph $G(V, E)$. The description $G(V, E)$ is shown in (2) and (3):

$$V = [V_p, V_c], \tag{2}$$

$$E = \{E_p, E_c, E_{\leftrightarrow}\}, \tag{3}$$

where $V_p = [v_{p1}, v_{p2}, \ldots v_{pn_p}]^T$, $V_c = [v_{c1}, v_{c2}, \ldots v_{cn_c}]^T$, respectively, denotes all nodes of the power grid and device-level EPCN. $E_p = \{i, j \in V_p | (i, j)\}$, which means that there is a connecting edge between node i and node j from the power grid. Same thing with E_c. $E_{\leftrightarrow} = \{E_{pi} \in E_p, \ V_{cj} \in V_c | E_{pi}, V_{cj}\}$, namely, "set of the dependent node to edge."

The adjacent matrix $A = \begin{bmatrix} A_p & 0 \\ 0 & A_c \end{bmatrix}$ can be obtained by $G(V, E)$.

$$A_x = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n_x} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n_x1} & a_{n_x2} & \cdots & a_{n_xn_x} \end{bmatrix}, \tag{4}$$

where $a_{ij} = 1$ when there is an edge between node i and node j, otherwise $a_{ij} = 0$ when there is no edge between node i and node j or $i = j$. x means p or c. n_x denotes the number of nodes of corresponding networks.

Obviously, an adjacent alone cannot represent the whole interdependent network on account of no equation representing the coupling relationship between two networks. Thus, $E_{\leftrightarrow}$ is needed, as shown in (5)as follows:

$$G(V, E) = G(A, E_{\leftrightarrow}). \tag{5}$$

3.3. Assessment of the Interdependent Vulnerability Based on Node Failure. For the reason of the influence evaluation of nodes in the coupled network, the attacked nodes are deemed completely invalidated. In the proposed model, the normal operation conditions of physical nodes are different after the failure of cyber nodes and physical nodes. Consequently, node attacks are classified into cyber node attacks and physical node attacks. Then, combined with constraints, a vulnerability index adapted to this paper's CPPS model is proposed in Section 3.3.3.

3.3.1. Constraints of Operations. All the power nodes are classified into 2 types: the first type is power generation nodes (which mean power stations) and the second type is what cannot generate electricity. If a fault occurs, the graph may be divided into several subgraphs. To ensure the operation of the second nodes, there must be a direct or indirect electrical connection between the two types of nodes.

"d_{kj}" ("d" denotes distance) is used to judge whether there is the connection mentioned above between node k and node j. d_{kj} is the length of the shortest path from k to j. If there is no path to get from k to j, then $d_{kj} = \infty$ or $1/d_{kj} = 0$.

Hence, if "d"s from a second node to any power generation nodes are all infinite, which indicates that the station has no power source, the second node will stop functioning. Purely from the perspective of the structure of networks, as long as this node has the abovementioned connection with at least one power generation node, the node still exists in the network. Then, the "d"s are calculated from node k (a second node) to all power generation nodes (node 1 to m).

$\sum_{j=1}^{j=m} 1/d_{kj} = 0$ means there is no connection between k and all power generation nodes.

So, $\sum_{j=1}^{j=m} 1/d_{kj} > \varepsilon$ $(0 < \varepsilon < \infty)$ is one of the prerequisites for the second node to run.

The normal operation of the physical nodes (except power generation nodes) shall meet the constraints: $\exists \varepsilon > 0$, in Equation (6), it is established in the case that the physical nodes of the physical power grid are attacked.

$$\text{S.t.} \quad \sum_{j=1}^{j=m} \frac{1}{d_{kj}} > \varepsilon, \tag{6}$$

where d_{kj} is the distance from physical node k to physical node j $(\forall j \in [1, m], d_{kj} \geq 0)$. Moreover, nodes l to m are power generation nodes.

For cyber nodes, the devices outside the giant component will stop working:

$$\text{S.t.} \quad i \in G_{C\max}, \tag{7}$$

where $G_{C\max}$ is the largest connected subgraph (LCS) of EPCN.

3.3.2. Indexes of Vulnerability. In the face of attacks, researchers study the vulnerability of networks from the perspective of giant components, average shortest path, k core, and entropy. In this paper, the ratio of lost nodes (*RLN*) is used to quantitatively calculate the changes of the network subjected to different faults to reflect the vulnerability of the network [24, 25]. In this paper, *RLN* is calculated by the following Equation (8):

$$\text{RLN} = \frac{N^* - N}{N^*}, \tag{8}$$

where N^* is the number of nodes of the initial network, and N is the number of nodes of the current network.

Different constraints on physical nodes and cyber nodes determine the different ways of calculating the number of nodes in normal operation. For cyber nodes, the nodes of LCS and their edges make up the current network. Yet even physical nodes that do not belong to the LCS may operate normally, resulting in the unsuitability of the LCS in describing the functioning physical power grid. Furthermore, physical nodes, power generation nodes, substation nodes, and connecting edges form together the current operating network [26]. If there is no generation node connected to substation nodes or vice versa, the substation nodes or the generation nodes do not belong to the current functioning network [27].

The influence of node i on network vulnerability can be revealed by the relative change of RLN before and after node i fail, as shown in Equation (9)as follows:

$$\Delta\overline{RLN_{ci}} = \frac{N_c^* - N_{ci}}{N_c^*}, \Delta\overline{RLN_{pi}} = \frac{N_p^* - N_{pi}}{N_p^*}, \tag{9}$$

where $\Delta\overline{RLN_c}$ is the index of the importance of node i for cyber-network, $\Delta\overline{RLN_p}$ is the index of the importance of node i for physical network, N_c^* is the number of initial EPCN's nodes, $N_{\max Gi}$ is the number of nodes of EPCN's LCS after node i fails, N_p^* is the number of the initial power grid, N_{pi} is the number of normal nodes of power grid after node i fails.

The importance of node i is defined as the weighted mean value of the damage of the coupled network which consists of $\Delta\ \overline{RLN}$ of the two single-sided networks:

$$\Delta\overline{RLN_i} = w_c\Delta\overline{RLN_{ci}} + w_p\Delta\overline{RLN_{p\,i}}. \tag{10}$$

The average distance of EPCN D_c and the physical power grid D_p is calculated first to measure pivotal nodes' proportion prone to high risk to the network. And failure is more likely to propagate across systems when there are many critical nodes. So, the weight calculation method is as follows Equation (11):

$$\begin{cases} w_c = \dfrac{D_p}{D_c + D_p}, \\ \\ w_p = \dfrac{D_c}{D_c + D_p}. \end{cases} \tag{11}$$

The calculation of the average distance is shown in (12).

$$D = \frac{2}{N(N-1)} \sum_{1 \leq i < j \leq N} \mathrm{d}_{ij}, \tag{12}$$

where $d_{ij}(i, j = 1, 2, \ldots, N)$ denotes the shortest distance from node i to node j.

4. Simulation and Discussion

This paper takes the local power grid shown in Figure 8 to conduct simulation verification on the proposed node-to-edge model and vulnerability assessment indexes. Brown nodes are power generation nodes, and yellow nodes are substation nodes. Table 1 presents the connections between substations and control centers.

The control center of each substation node is divided according to the region, as shown in Figure 9. The blue node is the control center of the backbone layer; it is connected to the main control center and the spare control center of the core layer.

A coupled network with a total of 544 nodes and 65 dependent edges is obtained. There are 512 nodes in the EPCN, and 580 connecting edges. The number of nodes in the physical power grid is 32, and the number of connected edges is 39.

The premise of the analysis is that the capacity of the power lines is sufficient and that the capacity of generating units can meet the demand for electricity. Based on the hypotheses, first, the nodes of EPCN are attacked. Then, nodes of the physical power grid follow. Furthermore, attacks are divided into two major types, that is, traversal attacks and continuous attacks. The former type means each attack is based on the origin coupled network, and the latter type means each attack is on the basis of the attacked network.

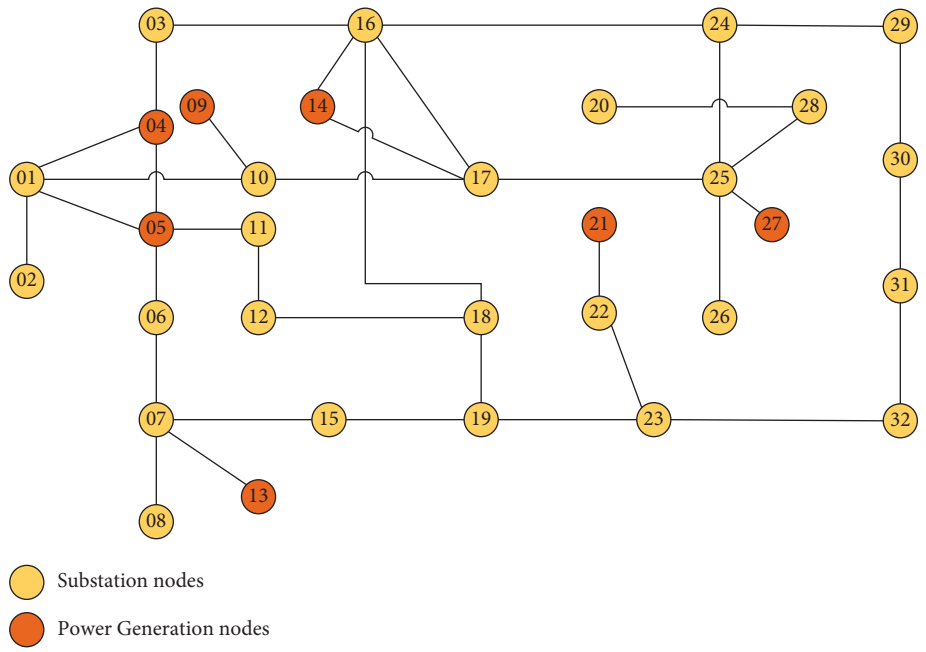

Figure 8: Topology of local power grid.

Table 1: Connection between substations and control centers.

Control centers	Substations
Control center a	1 2 3 10 11
Control center b	6 7 8 15
Control center c	12 16 17 18 19
Control center d	22 23
Control center e	20 24 25 26 28 29 30 31 32

4.1. Results of Vulnerability

4.1.1. Impact Analysis of Communication Attacks

(1) Node Importance of Device-Level EPCN. For the node traversal attack of the communication network, the value of RLN after the topology reaches the steady state is calculated. It should be noted that every cyber node is attacked on the basis of the original coupled network each time, so as to rank the influence of nodes on the network.

By comparing the three curves in Figure 10, the red curve shows a distinct stepped shape, indicating that the index, RLN, of the power grid has multiple nodes with the same value, which is insufficient to distinguish all nodes. The blue curve has the same weakness. The RLN of the coupled network integrates characters of both sides of the network, and the line segment parallel to the X-axis is shorter than the other two curves, which has a better result to distinguish the influence of nodes.

(2) Network Vulnerability Analysis under Multimode Attack Based on Node Importance. Three kinds of descending order of node importance in three kinds of modes were obtained in Section 4.2.1 (1), and calculated the betweenness and degree of the original network nodes. Then 5 vectors of descending order were generated: RLN of communication network,

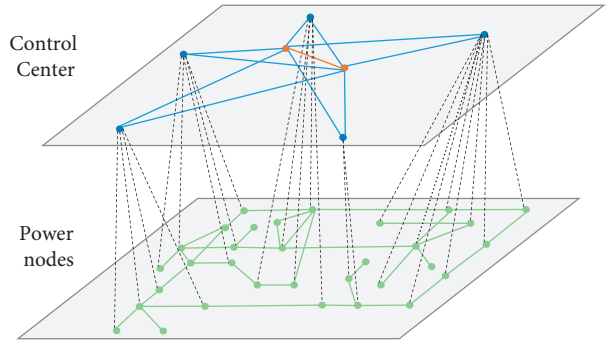

Figure 9: "Node to node" interdependent network of the local grid.

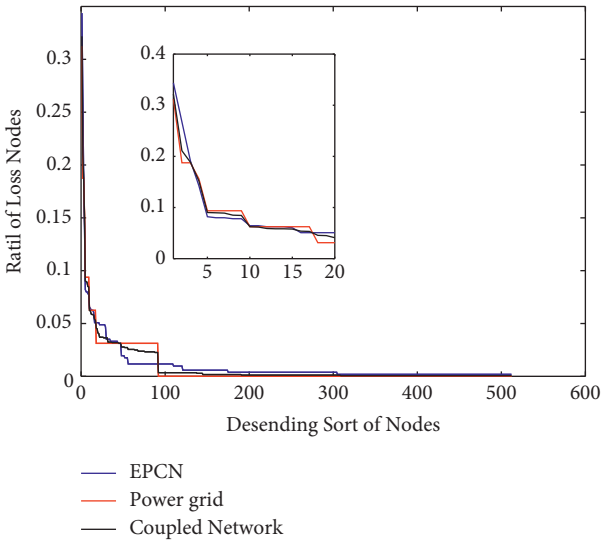

Figure 10: Rln of cyber nodes of three subjects.

RLN of the power grid, RLN of the coupled network, betweenness of communication network, degree of communication network, corresponding to attacking mode 1 to attacking mode 5, respectively.

Based on the five attacking modes, this section carries out multiple continuous attacks on the established coupled network. The nodes under each attack are the remaining normal nodes in the network after the last attack. Attack stops when all nodes in the EPCN fail. Figure 11 shows the results. "Attacking times" is used to measure the evaluation ability of different indexes. The larger the value of attack times is, the more nodes need to be attacked for network collapse. On the one hand, it shows the attack capability of different modes. On the other hand, it can reflect the vulnerability of a network.

Under different attack modes, the curve trend is roughly the same, but the inflection points of the five curves are very different. So are the lengths of the curves. Table 2 summarizes the results of the abovementioned five attack modes.

From Table 2, the coupled network has the fastest crash speed in mode 1, followed by mode 3 and mode 4. So, EPCN has more importance in coupled networks. Under the corresponding mode, coupled network crashes, respectively, 25.0% and 89.4% more easily than in modes 4 and 5.

Beginning RLN refers to damage of the first attack. Modes 1 to 4 are the same beginning value because the first node of the four-node attacking vectors is the same node, no.510. Therefore, the betweenness of no.510 is the highest, and their failures cause the most serious damage to both EPCN and the power grid. The beginning RLN of mode 5 is much lower than the others. Nevertheless, the *degree* is a common index to evaluate the centrality status of whole networks. It is concluded that centrality status cannot always reveal the impact of nodes on networks due to the interdependent edges.

The lowest value of attacking times is 9 of mode 1. The first nine RLNs of each mode are adopted. And the number of overlapped nodes is calculated. Figure 12 indicates that nodes that cause the collapse of the coupled network 9 times in mode 1 are the same components of mode 3, and it is similar to those of mode 4. The important cyber nodes to EPCN coincide highly with those to the coupled network and the high-betweenness cyber nodes. The curves of the three in Figure 11 are similar in length. Even so, the turning points are not consistent, because the nodes have similar compositions but different orders.

4.1.2. Impact Analysis of Physical Attacks

(1) Node Importance of Physical node. In accordance with the same method as 3.2.1, the node traversal attack on the physical power grid is carried out, and the value of RLN after the topology reaches a steady state is calculated to obtain three curves as shown in Figure 13.

There are quantities of nodes whose RLN are close to each other among the three curves of Figure 13. One of the reasons is that the number of nodes in the power grid is small. However, the black curve still distinguishes the nodes better than the others, while the other two curves only have two or three kinds of value.

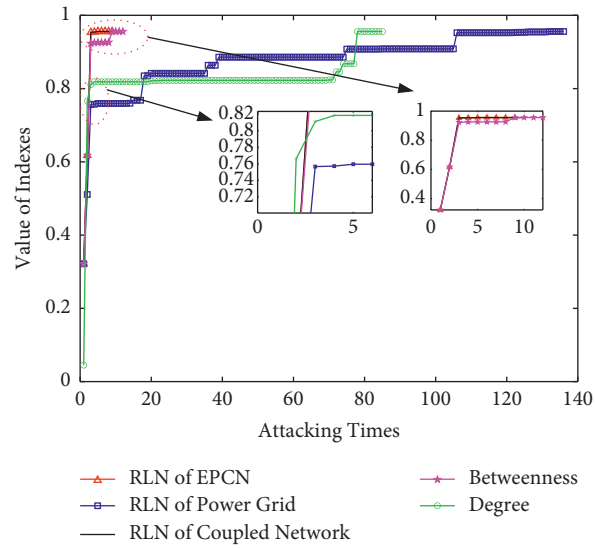

Figure 11: Indexes curve of 5 modes under cyber attacks.

Table 2: Attacking times and beginning RLN of 5 modes.

	Mode 1	Mode 2	Mode 3	Mode 4	Mode 5
Attacking times	9	136	10	12	85
Beginning RLN	0.3217	0.3217	0.3217	0.3217	0.0451

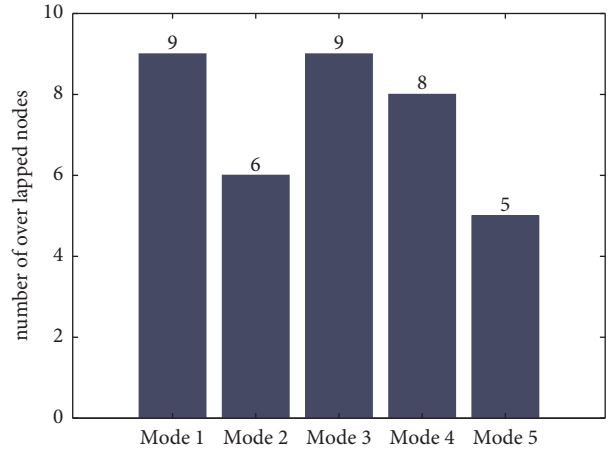

Figure 12: Number of overlapped nodes.

(2) Network Vulnerability Analysis under Multimode Attack Based on Node Importance. In the same way, 5 physical node vectors in descending order were obtained: RLN of communication network, RLN of the power grid, RLN of the coupled network, betweenness of power grid, degree of the power grid, corresponding to attacking mode 1 to attacking mode 5, respectively. Figure 14 is the results after the multiple continuous attacks on the established coupled network.

Under different attack modes, the turning nodes are also before and after, and the lengths of the curves are different. Table 3 summarizes the results of the abovementioned five attack modes:

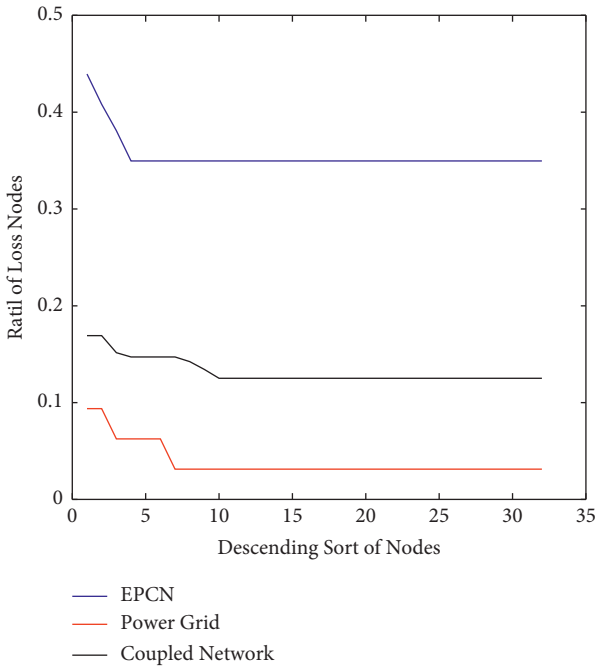

Figure 13: Rln of physical nodes of three subjects.

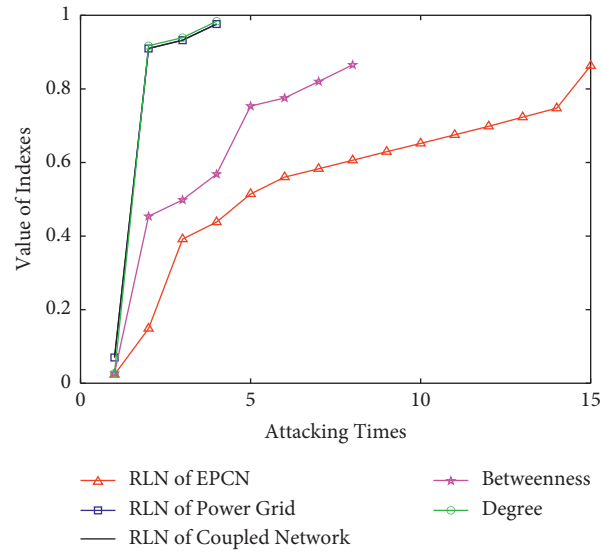

Figure 14: Indexes curve of 5 modes under physical attacks.

Table 3: Attacking times and beginning RLN of 5 modes.

	Mode 1	Mode 2	Mode 3	Mode 4	Mode 5
Attacking times	15	4	4	12	4
Beginning RLN ($\times 10^{-2}$)	2.38	7.01	7.01	2.72	2.72

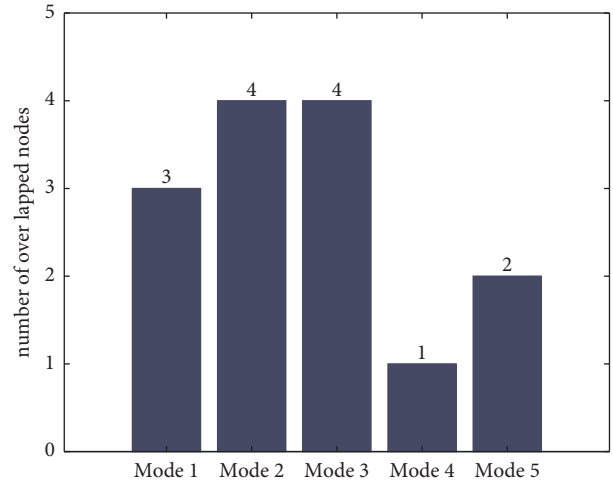

Figure 15: Number of overlapped nodes.

From Table 3, the coupled network has the fastest crash speed in modes 2, 3, and 4, much less than modes 1 and 4. So, the power grid has more importance in coupled networks, the coupled network crashes 66.7% more easily than mode 4. Although mode 5 behaves in the same way, both attacks show that mode 5 behaves in an erratic manner according to cyber-attacks.

The beginning value of modes 2 and 3 are the same, and the highest. It means that the physical node, which is the most significant to EPCN is the most crucial to the coupled network at the same time. Moreover, the curves of modes 2 and 3 coincide exactly; both are similar to the curve of mode 5.

From the results of section 4.2.1, the high-betweenness cyber nodes are quite important, while the high-betweenness physical nodes are not more vital to coupled networks than high-degree nodes. So, it is concluded that the same evaluation index has different effects on different sides of the node-to-edge network. This is because traditional indexes of a complex network evaluate the structural significance of nodes on a single side.

From Table 3, the lowest value of attacking times is 4 of mode 1. The first four RLNs of each mode are adopted. And the number of overlapped nodes is calculated. Figure 15 indicates that nodes that cause the collapse of the coupled network 4 times in mode 2 are the same components of mode 3.

Compared with *betweenness*, the indexes proposed under cyber and physical attack is, respectively, 25.0% and 66.7% easier in-network crash. Compared with a *degree*, the indexes proposed under cyber-attacks is 89.4% easier in-network crash and behave the same under physical attacks. Therefore, the indexes in this paper presented a more robust accuracy than *betweenness* and *degree*. *Betweenness* and *degree* are static process calculation network indexes and difficult to adapt to the general network structure. The dynamic process based on node failure evaluation in this paper solves the abovementioned problems well.

5. Conclusion

Based on the structure of power systems and interdependency between power sites and control centers, a multilevel CPPS model with a node-to-edge interdependent network

and an index system including 3 indexes are proposed in this paper to distinguish vulnerable components and the vulnerability of the coupled system. The following conclusions are drawn:

(1) The node-to-edge interdependent coupling relationship proposed is more suitable than the existing interdependent network about breaker services in transmission network substations with a simpler topology and a wider range of applications.

(2) The trajectory of indexes under continuous attack in this paper can characterize the vulnerability of the power grid to withstand attacks.

(3) The proposed indexes presented a better accuracy than "betweenness" and "degree."

The study presented in this paper is helpful for the long-term planning of each station and dispatching center of power systems and also contributes to the differential maintenance of key equipment and power stations. However, the presented research fails to define "multidependent," "many-to-many," "partially" interdependency like the traditional models. It can be easily extended in several directions, such as the vulnerability analysis with different node-to-edge interdependencies. And further work will be dedicated to research on how to enhance the robustness of CPPS.

Data Availability

Data are available in the paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This paper is supported by National Key Research and Development Program (Grant No. 2021YFB2401302).

References

[1] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): a review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151019–151064, 2020.

[2] J. Chen, M. A. Mohamed, U. Dampage et al., "A multi-layer security scheme for mitigating smart grid vulnerability against faults and cyber-attacks," *Applied Sciences*, vol. 11, no. 21, p. 9972, 2021.

[3] L. Shi, Q. Dai, and Y. Ni, "Cyber–physical interactions in power systems: a review of models, methods, and applications," *Electric Power Systems Research*, vol. 163, no. A, pp. 396–412, 2018.

[4] R. Zhou, M. Peng, and X. Gao, "Vulnerability assessment of power cyber-physical system considering nodes load capacity," in *2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP)*, pp. 1438–1441, Xi'an, China, 2021.

[5] L. Liu, B. Wang, F. Ma et al., "A concurrent fault diagnosis method of transformer based on graph convolutional network and knowledge graph," *Frontiers in Energy Research*, vol. 10, 2022.

[6] M. A. Mohamed, S. Mirjalili, U. Dampage, S. H. Salmen, S. A. Obaid, and A. Annuk, "A cost-efficient-based cooperative allocation of mining devices and renewable resources enhancing blockchain architecture," *Sustainability*, vol. 13, no. 18, Article ID 10382, 2021.

[7] F. Li, X. Yan, Y. Xie, Z. Sang, and X. Yuan, "A review of cyber-attack methods in cyber-physical power system," in *2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP)*, pp. 1335–1339, Xi'an, China, 2019.

[8] L. F. Fang, L. Huang, Q. Zhao, and A. Q. Pan, "Discussion on megalopolis power grid safety from the perspective of Venezuelan blackout," *Power and Energy*, vol. 40, no. 6, pp. 674–677, 2019.

[9] U. Adhikari, T. Morris, and S. Pan, "WAMS cyber-physical test bed for power system, cybersecurity study, and data mining," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2744–2753, 2017.

[10] Q. Wang, Z. Liu, and Y. Tang, "SCCO: a state-caching-based coagulation platform for cybor-physical power system evaluation," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1615–1625, 2021.

[11] D. L. Marino, C. S. Wickramasinghe, V. K. Singh, J. Gentle, C. Rieger, and M. Manic, "The virtualized cyber-physical testbed for machine learning anomaly detection: a wind powered grid case study," *IEEE Access*, vol. 9, pp. 159475–159494, 2021.

[12] Y. Li, B. Wang, H. Wang et al., "Importance assessment of communication equipment in cyber-physical coupled distribution network based on dynamic node failure mechanism," *Frontiers in Energy Research*, p. 654, 2022.

[13] N. Wirtz and A. Monti, "A flexible framework to investigate cascading in interdependent networks of power systems," in *2020 6th IEEE International Energy Conference (ENERGYCon)*, pp. 38–41, Gammarth, Tunisia, 2020.

[14] B. Li, J. Zhang, S. S. Chen, C. Y. Zhu, D. S. Jing, and B. Qi, "Expansion strategy of power communication network survivability based on complex network," *Power System Technology*, vol. 42, no. 06, pp. 1974–1980, 2018.

[15] A. Sturaro, S. Silvestri, M. Conti, and S. K. Das, "A realistic model for failure propagation in interdependent cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 817–831, 1 April-June 2020.

[16] B. Fan, C. Zheng, and L. Tang, "Risk assessment of power communication network based on node importance," in *2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, pp. 818–821, Chongqing, China, 2019.

[17] B. Qi, S. F. Liu, B. Li, Y. Sun, D. Jing, and Z. Cheng, "Routing optimization strategy for power communication network with shared risk link group and risk balance," *Automation of Electric Power Systems*, vol. 44, no. 08, pp. 168–175, 2020.

[18] L. Xu, Q. L. Guo, X. Z. Liu, and H. Sun, "Robust optimization method of communication network to improve resilience of cyber-physical power system," *Automation of Electric Power Systems*, vol. 45, no. 03, pp. 68–75, 2021.

[19] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[20] D. Zhou, J. Gao, H. E. Stanley, and S. Havlin, "Percolation of partially interdependent scale-free networks," *Physical Review E*, vol. 87, no. 5, Article ID 052812, 2013.

[21] J. Shao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Cascade of failures in coupled network systems with multiple support-dependence relations," *Physical Review E*, vol. 83, no. 3, Article ID 036116, 2011.

[22] H. Zhen, W. Cheng, S. Ruj, M. Stojmenovic, and A. Nayak, "Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory," in *8th IEEE Conference on in Industrial Electronics and Applications*, pp. 1023–1028, IEEE, Melbourne, Australia, 2013.

[23] Z. Huang, C. Wang, M. Stojmenovic, and A. Nayak, "Balancing system survivability and cost of smart grid via modeling cascading failures," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 45–56, 2013.

[24] A. Almalaq, S. Albadran, A. Alghadhban, T. Jin, and M. A. Mohamed, "An effective hybrid-energy framework for grid vulnerability alleviation under cyber-stealthy intrusions," *Mathematics*, vol. 10, no. 14, p. 2510, 2022.

[25] A. Almalaq, S. Albadran, and M. A. Mohamed, "Deep machine learning model-based cyber-attacks detection in smart power systems," *Mathematics*, vol. 10, no. 15, p. 2574, 2022.

[26] M. Ćalasan, A. F. Zobaa, H. M. Hasanien, S. H. Abdel Aleem, and Z. M. Ali, "Towards accurate calculation of supercapacitor electrical variables in constant power applications using new analytical closed-form expressions," *Journal of Energy Storage*, vol. 42, Article ID 102998, 2021.

[27] O. Lukačević, A. Almalaq, K. Alqunun et al., "Optimal CONOPT solver-based coordination of bi-directional converters and energy storage systems for regulation of active and reactive power injection in modern power networks," *Ain Shams Engineering Journal*, vol. 13, no. 6, Article ID 101803, 2022.