Robustness analysis of cyber-physical power system based on reachable matrix

Zhengwei Xu, Yuan Ge, Jin Cao, Qiyou Lin and Shuquan Yang

School of Electrical Engineering, Anhui Polytechnic University, Wuhu, People’s Republic of China; State Grid Anhui Electric Power Co., Ltd., Wuhu Power Supply Company, Wuhu, People’s Republic of China; Anhui Conch New Energy Co., Ltd., Wuhu, People’s Republic of China

ABSTRACT
The traditional modelling and simulation analysis methods based on graph theory are difficult to present the structural characteristics and dynamic laws of cyber-physical power systems (CPPS). In order to reduce the complexity of the attack graph, this paper proposes a CPPS robustness analysis method based on the reachable matrix. Based on the evolution of the augmented adjacency matrix of cyber-physical power system, this method uses the reachable matrix to obtain the maximum connectivity matrix of the system (the adjacency matrix corresponding to the largest connected subgraph of cyber-physical power system), and then, evaluates and analyses the robustness of cyber-physical power system. The IEEE118 node standard model is taken as an example to carry out the simulation experiment. The experimental results show that the reachable matrix has feasibility in the robustness analysis of cyber-physical power systems. Further through the contrast experiment found that compared with the robustness analysis method based on graph theory, the proposed method in this paper can reduce the modelling complexity of the mutual coupling network, reduce the complexity of the attack graph, and clearly and intuitively show the structural characteristics and dynamic laws of the network connection in the system.

1. Introduction
In reality, the power network and the information network do not exist in isolation. The traditional power system based on the primary power network has gradually developed into a system in which power network and information network coexist and close-coupled, namely cyber-physical power system (CPPS) (Jia et al., 2019; Jin & Tan, 2019; Li et al., 2021; Tan et al., 2018). CPPS introduces advanced information and communication technology, which not only deepens the integration of information network and power network, but also makes the system face severe security challenges, among which system robustness is the primary problem. Failure of the power network may lead to the loss of power supply of related information equipment, and failure of the communication network may lead to unmeasurable or uncontrollable related power equipment, so that failure cascade propagation between the two networks, may eventually lead to the sharp decline of the robustness of the system and even the collapse of the system (Chen & Li, 2020; Qin & Liu, 2020; Yaacoub et al., 2020). Several major power outages in history were caused by the cascading propagation of such faults, such as the North American power outage in 2003 (Vespignani, 2010), the Rome power outage in 2004 (Bobbio et al., 2010), the power failure caused by the ice disaster in southern China in 2008 (Huang et al., 2013), and the ’8.15’ Taiwan power outage in 2017 (Yan et al., 2019). Therefore, it has great significance to study the failure cascade propagation mechanism and robustness analysis of CPPS.

At present, the academia generally adopts the modelling and simulation analysis method based on graph theory to study CPPS robustness (Chen et al., 2020; Jimada-Ojuolape & Teh, 2020; Wang et al., 2018). First, establish the respective mathematical models of the physical network and the information network in the system based on graph theory; Then, excavates the coupling relationship between the two networks and establishes an interdependent network model of the entire system (Chen et al., 2019; Dong et al., 2019; Zhou et al., 2020); Finally, the robustness of the system is analysed based on percolation theory (Zhang & Wang, 2020). Literature (Tang et al., 2016) and Literature (Long et al., 2019) analyse the robustness of CPPS from the perspective of connectivity based on the graph theory method. However, the modelling and simulation analysis methods based on graph theory are difficult to present the structural characteristics and dynamic laws of complex...
networks. Some scholars have extended the description method of the network adjacency matrix to interdependent networks and define the intra-network adjacency matrix and the inter-network dependency matrix (Li et al., 2019; Wang et al., 2021). But they did not further reveal the mechanism of cascading failure propagation of system nodes through the intra-network adjacency matrix and the inter-network dependency matrix (Jin, 2016; Su et al., 2012; Wang et al., 2016).

CPPS network contains massive nodes, and the connection relationship and actual operation situation are complex, which brings great difficulties to the automatic construction and analysis of the attack graph. To reduce the complexity of the attack graph, this paper proposes a CPPS robustness analysis method based on the reachable matrix on the basis of power network adjacency matrix, information network adjacency matrix and inter-network dependency matrix. The proposed method combines the intra-network adjacency matrix and the inter-network dependency matrix to generate the CPPS augmented adjacency matrix, and simulates the attack on the system by removing the rows and columns of the CPPS augmented adjacency matrix. When network nodes are attacked, delete the rows and columns corresponding to the failure nodes in the subnet adjacency matrix, then use the reachable matrix to extract the maximum connectivity matrix of the subnet adjacency matrix, finally, reveal the cascading failure propagation mechanism of the rows and columns of the two subnet adjacency matrices through the dependency matrix, so as to realize the system robustness analysis. The reachable matrix refers to the use of matrix form to describe the degree that the nodes of the directed graph can reach after a certain length of the path. The reachable matrix can completely characterize the direct or indirect connection relationship of all nodes in the graph, which is commonly used in system structure models and system structure hierarchical divisions, etc. Therefore, this paper can use the reachable matrix to extract the maximum connectivity matrix of the system (the adjacency matrix corresponding to the largest connected subgraph of the network physical power system).

The main contribution of this paper is to reveal the failure cascade propagation mechanism of the system by using the evolution process of the system network adjacency matrix, and obtain the maximum connectivity matrix of the system through the reachable matrix, so as to realize the robustness calculation, evaluation and analysis of CPPS. By observing the change curve of the robustness index of CPPS under different attack modes, study the damage of the system and identify the weak links of the system. The comparative experiment shows that the method in this paper has good feasibility and superiority for studying the robustness of CPPS. The proposed method in this paper can reduce the modelling complexity of the mutual coupling network, and clearly and intuitively show structural characteristics and dynamic laws of the network connection in the system.

2. Cyber-physical power system modelling

In this paper, power network, information network modelling to make the following definition: In the power network, large equipment such as power plants, substations and converter stations as power nodes, and high voltage transmission lines as edges between nodes in the power network. In the communication network, routers, switches and other equipment as communication nodes, and communication lines such as cables and optical fibre as edges between nodes in the communication network. All edges identified as undirected edges and multiple lines in the same direction are merged into one edge to eliminate multi-links and self-loops, ignore issues such as equipment and line capacity, new and old, and load. The coupling relationship (energy or information exchange, etc.) between power network and communication network nodes is represented by dependency edges (Chen et al., 2018).

Based on the above assumptions, the power network and communication network were modelled as complex network graphs, respectively, \( G_P = (V_P, E_P) \), \( G_C = (V_C, E_C) \), where \( V_P = V_P(G) = \{v_{p1}, v_{p2}, \ldots, v_{pn}\} \), \( V_C = V_C(G) = \{v_{c1}, v_{c2}, \ldots, v_{cm}\} \). \( V_P \) represents the node-set of the power network, \( E_P \) is the adjacency matrix of the power network, \( n \) is the number of nodes in the power network, \( V_C \) is the node-set of the communication network, \( E_C \) is the adjacency matrix of the communication network, and \( m \) is the number of nodes in the communication network.

The adjacency matrix \( E_P \) of the power network is defined as follows:

\[
E_P = \begin{bmatrix}
e_{1,1} & e_{1,2} & \cdots & e_{1,n} \\
e_{2,1} & e_{2,2} & \cdots & e_{2,n} \\
\vdots & \vdots & \ddots & \vdots \\
e_{n,1} & e_{n,2} & \cdots & e_{n,n}
\end{bmatrix}
\]  

(1)

when there is a relationship between two nodes in the network, \( e_{ij} = 1 \); when there is no relationship between two nodes in the network, \( e_{ij} = 0 \). Similarly, the adjacency matrix \( E_C \) of the communication network is expressed in the same way.
For the dependence relationship of nodes between two networks, it can be represented by $E_{PC}(E_{P})$, $E_{PC}$ is $E_{P}$ transpose, $E_{PC}$ is defined as follows:

$$E_{PC} = \begin{bmatrix} e_{1,1} & e_{1,2} & \ldots & e_{1,m} \\ e_{2,1} & e_{2,2} & \ldots & e_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ e_{n,1} & e_{n,2} & \ldots & e_{n,m} \end{bmatrix}$$ (2)

when there is a dependency between the node $v_{pi}$ in $G_P$ and node $v_{cj}$ in $G_C$, $e_{ij} = 1$; otherwise, $e_{ij} = 0$.

Based on the above definition, this paper introduces the augmented adjacency matrix $E$ to uniformly model the cyber-physical power system as a complex network graph $G = (V_P, V_C, E)$, where $E$ is defined as follows:

$$E = \begin{bmatrix} E_P & E_{PC} \\ E_{CP} & E_C \end{bmatrix}$$ (3)

3. Robustness analysis of cyber-physical power system

3.1. Robustness index

This paper evaluates the robustness of CPPS from the perspective of connectivity. When CPPS is attacked, its robustness can be measured by the scale of the largest connected subgraph, expressed by the ratio of the number of nodes in the largest connected subgraph of CPPS after the attack to the number of nodes in the original CPPS. Therefore, when the CPPS is attacked, the robustness of the system can be measured by the maximum connectivity matrix of CPPS (the adjacency matrix corresponding to the largest connected subgraph of CPPS). Robustness is expressed by the ratio of the order $N'$ of the maximum connectivity matrix of CPPS after the attack to the order $N$ of the original augmented adjacency matrix of CPPS, and on this basis, consider the element changes in the maximum connectivity matrix of CPPS. Here $N'$ represents the sum of elements in the original augmented adjacency matrix of CPPS, and $N'_S$ represents the sum of elements in the maximum connectivity matrix of CPPS after the attack. At this time, the robustness index is

$$p = \frac{N' + N'_S}{N + N'_S}$$ (5)

3.2. Calculation of reachable matrix

In this paper, we can use the reachable matrix to obtain the maximum connectivity matrix of CPPS. The reachable matrix calculation method is as follows:

$$B = (A + I)^n = I + A + A^2 + \cdots + A^n$$ (6)

where $I$ represents the unit matrix, $A$ represents the adjacency matrix of the graph, and $B$ represents the reachable matrix of the graph.

The reachable matrix indicates whether there is at least one chain between any two nodes in the graph and whether there is a loop at the node. The power network structure of Figure 2(b) is taken as an example to illustrate, and its connection relationship is shown in Figure 1. According to the connected relations of the nodes in Figure 1, the adjacency matrix $A$ is as follows:

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 & 6 \\ 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 \\ 3 & 1 & 1 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 \end{bmatrix}$$

According to Equation (6), the reachable matrix $B$ in Figure 1 is calculated as:

$$B = \begin{bmatrix} 1 & 2 & 3 & 4 & 6 \\ 1 & 21 & 21 & 21 & 0 & 0 \\ 2 & 21 & 21 & 21 & 0 & 0 \\ 3 & 21 & 21 & 21 & 0 & 0 \\ 4 & 0 & 0 & 0 & 1 & 0 \\ 6 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

According to the definition and properties of the reachable matrix, in the reachable matrix, the number of
3.3. Robustness evaluation algorithm of cyber-physical power system

This paper analyses the interaction process of the information network and the power network from the evolution process of the system network and system augmented adjacency matrix. In the interdependent network model abstracted by Buldyrev et al. (2010), each node is numbered, as shown in Figure 2. In Figure 2(a), the power network (hollow nodes) and the information network (solid nodes) are interdependent networks, where each node in the power network uniquely corresponds to a node in the information network and vice versa.

When node 5 in the power network is attacked, the node and its connected edges are all deleted, and node 11 in the dependent information network is also deleted. At this time, the power network splits into three clusters, namely three relatively independent and disconnected parts (see Figure 2(b)). The maximal cluster in the power network is (1, 2, 3), which indicates that nodes 1, 2, and 3 are valid, and other nodes have failed. The failure of nodes 4 and 6 in the power network leads to the fault of nodes 10 and 12 in the information network through the dependency edge (see Figure 2(c)). Affected by the split clusters of the information network, the maximal cluster (1, 2, 3) in the power network continues to split, and the system finally reaches stability. Finally, the maximal cluster of the stable system is (1, 2, 7, 8) (see Figure 2(d)).

According to the original interdependent network model in Figure 2(a), the adjacency matrix $E_P$ of the power network, the adjacency matrix $E_C$ of the information network and the inter-network dependency matrix $E_{PC}$ ($E_{CP}$) (Rueda & Calle, 2017) are constructed. For ease of calculation and understanding, each row and each column of the matrix are numbered, and the results are as follows:

### $E_P$

\[
E_P = \begin{bmatrix}
0 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
7 & 8 & 9 & 10 & 11 & 12
\end{bmatrix}
\]

### $E_{PC}$

\[
E_{PC} = \begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 0 \\
2 & 0 & 1 & 0 & 0 & 0 \\
3 & 0 & 0 & 1 & 0 & 0 \\
4 & 0 & 0 & 0 & 1 & 0 \\
5 & 0 & 0 & 0 & 1 & 0 \\
6 & 0 & 0 & 0 & 0 & 1 \\
7 & 8 & 9 & 10 & 11 & 12
\end{bmatrix}
\]

### $E_C$

\[
E_C = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
7 & 8 & 9 & 10 & 11 & 12
\end{bmatrix}
\]

When node 5 in the power network is attacked, delete its corresponding row and column in the adjacency matrix $E_P$, and use the reachable matrix to obtain the maximum connectivity matrix in the adjacency matrix $E_P$. The
result is as follows:

\[
E_P = \begin{bmatrix}
1 & 2 & 3 & 4 & 6 \\
1 & 0 & 1 & 1 & 0 \\
2 & 1 & 0 & 1 & 0 \\
3 & 1 & 1 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 \\
6 & 0 & 0 & 0 & 0 \\
\end{bmatrix}
\]

\[
E_P = \begin{bmatrix}
1 & 2 & 3 \\
1 & 0 & 1 \\
2 & 1 & 0 \\
3 & 1 & 1 \\
\end{bmatrix}
\]

Through the inter-network dependency matrix \(E_{PC}\), detect nodes 10, 11, 12 failure, and delete the rows and columns corresponding to the failure nodes in the subnet adjacency matrix \(E_C\). The maximum connectivity matrix in adjacency matrix \(E_C\) is obtained by reachable matrix, and the result is as follows:

\[
\begin{bmatrix}
7 & 8 & 9 \\
7 & 0 & 1 & 0 \\
8 & 1 & 0 & 0 \\
9 & 0 & 0 & 0 \\
\end{bmatrix}
\]

\[
E_C = \begin{bmatrix}
7 & 8 \\
0 & 1 \\
1 & 0 \\
\end{bmatrix}
\]

Through the inter-network dependency matrix \(E_{CP}\), detect node 3 failure, and delete the row and column of the faulty node in the adjacency matrix \(E_P\). The maximum connectivity matrix in adjacency matrix \(E_P\) is obtained by reachable matrix, and the result is as follows:

\[
E_P = \begin{bmatrix}
1 & 2 \\
1 & 0 \\
2 & 1 \\
\end{bmatrix}
\]

At this time, the adjacency matrix of the power network and the information network has reached steady state and no longer splits, and the maximum connectivity matrix of the system is the output

\[
E = \begin{bmatrix}
1 & 2 & 7 & 8 \\
1 & 0 & 1 & 1 & 0 \\
2 & 1 & 0 & 0 & 1 \\
7 & 1 & 0 & 0 & 1 \\
8 & 0 & 1 & 1 & 0 \\
\end{bmatrix}
\]

From the evolution process of system network and system augmented adjacency matrix, the interactive influence process of information network and power network is analysed. The results obtained from the analysis are the same, and the robustness indexes are \(P = \frac{4 + 8}{12 + 3} = 0.273\). The evolution process of the network adjacency matrix can clearly and intuitively display the structure characteristics and dynamic laws of the network connection in the system. The steps of the proposed CPPS robustness evaluation algorithm are as follows (Table 1).

| Step | Description |
|------|-------------|
| 1    | When nodes in the power network fail. |
| 2    | Delete the row and column corresponding to the failure nodes in the adjacency matrix \(E_P\). |
| 3    | Calculate the maximum connectivity matrix in \(E_C\), and delete the rows and columns that do not belong to the maximum connectivity matrix. |
| 4    | Based on the deleted rows and columns in the adjacency matrix \(E_P\), determine the failure nodes of the information network by the dependency matrix \(E_{PC}\). |
| 5    | Delete the row and column corresponding to the failure nodes in the adjacency matrix \(E_C\). |
| 6    | Calculate the maximum connectivity matrix in \(E_C\), and delete the rows and columns that do not belong to the maximum connectivity matrix. |
| 7    | Based on the deleted rows and columns in the adjacency matrix \(E_C\), determine the failure nodes of the power network by the dependency matrix \(E_{PC}\). |
| 8    | Both the adjacency matrix \(E_P\) and \(E_C\) reach steady state. |

Return System augmented adjacency matrix \(E\), Robustness index \(P\). |

### 4. Example simulation

#### 4.1. Simulation model construction

The IEEE118 node standard model is used to construct the power network of the simulation experiment in this paper, and the corresponding communication nodes are set for 54 power nodes to form the communication network. The power nodes and communication nodes are connected according to one-to-one correspondence, namely each power node is controlled by a communication node, so there are 54 communication nodes. The connection mode between the communication nodes according to the principle of proximity, namely 54 power nodes are connected by only one line or one substation, which are regarded as the adjacent power nodes, and the corresponding communication nodes have connections. According to the topological data of the power network, construct the adjacency matrix of the power network, the power network model is established on this basis. Figure 3 shows the schematic diagram of power network topology modelling.

Similarly, according to the topological data of the communication network, construct the adjacency matrix of the communication network. And on this basis, establish the communication network model. Figure 4 shows the schematic diagram of communication network modelling.

According to the topology and dependency relationship of power network and communication network, constitute an incomplete symmetry interdependent network with 118 power nodes and 54 communication nodes. CPPS is modelled as a set of the power network, communication network and dependency edges. Figure 5 shows the degree distribution curve of CPPS nodes, and the results show that the node degree of most nodes in the
Figure 3. Schematic diagram of power network topology modelling.

Figure 4. Schematic diagram of communication network modelling.

CPPS network is low, while the node degree of very few nodes is high, which conforms to the characteristics of a scale-free network. Therefore, it is suitable for the analysis of complex network theory (Pan et al., 2019).

The clustering coefficient of the whole network is 0.1303, the average path length of the entire network is 6.328, and the average node degree is 3.622. The average shortest distance and clustering coefficient of a random network with the same number of nodes and edges as the CPPS in this paper are:

\[
\begin{align*}
L_{\text{random}} & \approx \frac{\ln n}{\ln d} = 2.79 \\
C_{\text{random}} & \approx \frac{5}{d} = 27.18
\end{align*}
\]

According to the small-world criterion, that is
\[
\begin{align*}
L & >> L_{\text{random}} \\
C & >> C_{\text{random}}
\end{align*}
\]  
(Pan et al., 2019), the CPPS network established in this paper conforms to the small-world property.

### 4.2. Node importance research

In the study of network topology, node degree is generally taken as the standard to measure the importance of nodes. However, some key nodes in many real networks do not necessarily have a large node degree. This paper introduces a concept of node importance to measure the importance of nodes in the network and prioritizes power nodes as nodes with high node importance. The definition of node importance (Liu & Gu, 2007) is

\[
\alpha_i = \frac{1}{n_i \cdot l_i}
\]

where \( n_i \) represents the total number of nodes in the new network after node contraction and \( l_i \) represents the average shortest distance of the new network after node contraction.

The network X calls the algorithm to calculate the parameters of each node in the CPPS network, and sorts the nodes in the order of node degree (random arrangement with the same degree of nodes), node betweenness (Ji et al., 2016), and node importance from high to low. Tables 2–4 show the ranking results of the top 7% of the nodes.

The results show that most of the 12 nodes in each table are power nodes or dependent on power nodes, which indicates that power nodes have a relatively important position in the system. Among them, 69 (152), 80...
Table 3. CPPS node betweenness ranking.

| Node number | Node betweenness | Node number | Node betweenness |
|-------------|------------------|-------------|------------------|
| 65          | 0.231513         | 80          | 0.188324         |
| 38          | 0.223324         | 49          | 0.179602         |
| 152         | 0.200330         | 77          | 0.164151         |
| 30          | 0.197024         | 161         | 0.132039         |
| 69          | 0.189458         | 100         | 0.127378         |

Table 4. CPPS node importance ranking.

| Node number | Node importance | Node number | Node importance |
|-------------|-----------------|-------------|-----------------|
| 69          | 0.001066        | 12          | 0.0009957       |
| 65          | 0.001037        | 99          | 0.0009875       |
| 77          | 0.0010351       | 70          | 0.0009843       |
| 80          | 0.001033        | 92          | 0.0009875       |
| 49          | 0.00103334      | 15          | 0.0009837       |
| 100         | 0.00102648      | 103         | 0.0009817       |

(161), 77 (155), 100 (165) in the system not only have high node degree, but also have high node betweenness and high node importance. We can see that the importance of nodes is highly consistent, as is the significance of dependent nodes. The reason is that power nodes that are pivotal in the actual power system always have more developed communication hubs, and they are interdependent.

4.3. Robustness analysis

In this paper, the power network, communication network, and the system itself are regarded as attack targets. Random attack, node degree attack, node importance attack, and node betweenness attack are regarded as attack strategies (Buldyrev et al., 2010). The robustness of the system is analysed by observing the change of the CPPS augmented adjacency matrix. The attack strategy is subdivided as follows:

(1) Random attack: a certain number of nodes are randomly selected from the attack target network, and delete the rows and columns corresponding to the nodes in the subnet adjacency matrix in order of selection.

(2) Node degree attack: the node degree of all nodes in the attack target network is calculated and sorted. According to the order of node degree from high to low, delete the rows and columns corresponding to nodes in the subnet adjacency matrix.

(3) Node importance attack: the node importance of all nodes in the attack target network is calculated and sorted. According to the order of node importance from high to low, delete the rows and columns corresponding to nodes in the subnet adjacency matrix.

(4) Node betweenness attack: the node betweenness of all nodes in the attack target network is calculated and sorted. According to the order of node betweenness from high to low, delete the rows and columns corresponding to nodes in the subnet adjacency matrix.

The robustness index is obtained by the robustness evaluation algorithm of CPPS in section 3.3. After each attack, if the maximum connected matrix of the system changes, the attack is successful. If the maximum connected matrix of the system does not change, the attack is invalid, and the number of attacks is not included. The robustness change curves of CPPS under four different attack strategies are plotted with attack times as abscissa and robustness index $P$ as ordinate, as shown in Figures 6–8.

By comparing the system robustness curves under different attack strategies in Figures 6–8, we can draw the following conclusions:
Figure 8. Change curve of system robustness index under different attack strategies in communication network.

(1) The system shows stronger robustness under random attacks than under deliberate attacks. The reason is that deliberate attacks will destroy nodes with high importance in the system, which will cause more severe damage to the system. The system also shows different levels of robustness in the face of various deliberate attacks, and the whole system is basically connected at the beginning of the attack, but with constant attacks, the connectivity of the system has sharply decreased.

(2) From the comparison of the robustness change curve in Figure 8 with the robustness change curves in Figures 6 and 7, we can see that the attack on the communication network cause more severe damage to the CPPS. The reason is that the topology of the communication network is simpler than that of the power network, which makes the system network more prone to splitting and losing connectivity. From the comparison of the robustness change curve in Figure 6 with the robustness change curve in Figure 7, we can see that the robustness changes of the two are similar. Because the topology of the power network is more complicated, and the characteristic parameters of the complex network arrange from largest to smallest and more concentrated in the power network.

(3) The results in Figure 6 show that attacking power supply nodes with high node importance in CPPS will cause more damage to the entire system, followed by node degree attack and node betweenness attack. The results in Figure 8 show that node importance attacks cause more damage to the system than other deliberate attacks, so the node importance cannot fully evaluate the significance of nodes. When evaluating the significance of nodes, network structure, node type and realistic factors (system operation, management, etc.) should be considered comprehensively.

5. Conclusions

This paper proposes a CPPS robustness analysis method based on the reachable matrix on the basis of power network adjacency matrix, information network adjacency matrix and inter-network dependency matrix. The experimental results show that the system shows stronger robustness under random attacks than under deliberate attacks, and also displays different levels of robustness in the face of various deliberate attacks. When the information network of a simple topology is destroyed, it is very harmful to the system. When the power network of a complex topology is destroyed, the system shows relatively strong robustness. If priority is to destroying nodes with higher importance, it will cause more damage to the system.

This paper uses the intra-network adjacency matrix and the inter-network dependency matrix to reveal the cascading propagation mechanism of system nodes fault, and it is feasible to analyse the robustness of the system. This method in the paper can reduce the modelling complexity of the mutually coupled network, clearly and intuitively show structural characteristics and dynamic laws of each network connection in the system. It reduces the complexity of the attack graph and is easy to understand and analyse, which is of great significance to study the robustness of the cyber-physical power system. In our future research, we will consider the impact of the actual operation of CPPS (such as the load changes, power balance, power flow characteristics, etc.), and evaluate and analyze the robustness of CPPS based on the evolution of the network adjacency matrix. In addition, we will further optimize and improve the CPPS robustness evaluation algorithm proposed in this paper.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported in part by the National Natural Science Foundation of China (NSFC) [61572032], the State Key Laboratory of Power System and Generation Equipment [SKLD21KM09], and the Synergy Innovation Programme of Anhui Polytechnic University and JiuJiang District [2021cyxta2].

References

Bobbio, A., Bonanni, R., Ciancamerla, R., Clemente, R., Iacomini, R., & Minichino, M. (2010). Unavailability of critical scada communication links interconnecting a power grid and a telco network. Reliability Engineering & System Safety, 95(12), 1345–1357. https://doi.org/10.1016/j.ress.2010.06.011
Bulyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291), 1025. https://doi.org/10.1038/nature08932

Chen, S., & Li, K. (2020). Distributed optimal control of transient stability for a power information physical system. *Mathematical Problems in Engineering*, 2020, 1–11. https://doi.org/10.1155/2020/1393216

Chen, S., Ma, F., & Gao, Y. (2020). Modeling and vulnerability analysis of electrical cyber-physical system. *Computer Applications and Software*, 37(5), 90–95. https://doi.org/10.13334/j.0258-8013.pcce.160492

Chen, S. M., Dai, Y. M., & Cheng, Y. H. (2019). Research of the transient stability for a power information physical system. *Electric Power Automation Equipment*, 39(8), 104–112. https://doi.org/10.16081/j.epae.201908002

Chen, Z., Wu, J., Xia, Y., & Zhang, X. (2018). Robustness and Control of Cyber-Physical System. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(1), 103–109. https://doi.org/10.1109/TSMC.2017.2705758

Dong, G., Chen, Y., Wang, F., Du, R., & Stanley, H. E. (2019). Robustness on interdependent networks with a multiple-to-multiple dependent relationship. *Chaos*, 29(7), 073107. https://doi.org/10.1063/1.5093074

Huang, Z., Wang, C., Stojmenovic, M., & Nayak, A. (2013, July 25). Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory. In *2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA)*, Melbourne, VIC, Australia (pp. 1023–1028).

Ji, X., Wang, B., Dong, Z., Chen, G., & Wang, X. (2016). Vulnerability evaluation and link protection strategy research of electrical cyber-physical interdependent networks. *Power System Technology*, 40(6), 1867–1873. https://doi.org/10.13335/j.1000-3673.pst.2016.06.038

Jia, H., Ding, Y., Song, Y., Hu, Y., & Liu, Y. (2019). Review of reliability analysis for integrated energy systems with integration of cyber-physical systems. *Power System Technology*, 43(1), 1–11. https://doi.org/10.13335/j.1000-3673.pst.2018.2135

Jimada-Ojuolape, B., & Teh, J. (2020). Impact of the integration of information and communication technology on power system reliability: A review. *IEEE Access*, 8, 24600–24615. https://doi.org/10.1109/ACCESS.2020.2970598

Jin, J., & Tan, Y. (2019). Unified modeling analysis of electrical cyber-physical interdependent networks. *Power Grid Technology*, 43(7), 2361–2367. https://doi.org/10.13335/j.1000-3673.pst.2018.1416

Jin, W. (2016). The vulnerability evaluation of the interconnected and interdependent NoNs based on the matrix ranks. In *17th CCSSTA 2016, China*.

Li, G., Huang, H., & Shu, Q. (2019). Evaluation method for node importance in power telecommunication network based on interdependent network theory. *Power System Protection and Control*, 47(11), 143–150. https://doi.org/10.19783/j.cnki.pspc.180921

Li, L., Wang, W., Ma, Q., Pan, K., Liu, X., Lin, L., & Li, J. (2021). Cyber attack estimation and detection for cyber-physical power systems. *Applied Mathematics and Computation*, 400(16), 126056. https://doi.org/10.1016/J.AMC.2021.126056

Liu, Y., & Gu, X. (2007). Skeleton-network reconfiguration based on topological characteristics of scale-free networks and discrete particle swarm optimization. *IEEE Transactions on Power Systems*, 22(3), 1267–1274. https://doi.org/10.1109/TPWRS.2007.901486

Long, Q., Wang, T., Xueping, G. U., & Wang, T. (2019). Modeling and invulnerability analysis of power communication interdependent network based on community overlapping. *Electric Power Automation Equipment*, 39(11), 165–173. https://doi.org/10.16081/j.epae.201911021

Pan, H., Xiao, Y., Liang, Z., Zhu, Z., & Hui, H. E. (2019). Robustness analysis of electricity-gas-heat integrated energy system based on complex network. *Electric Power Automation Equipment*, 39(8), 104–112. https://doi.org/10.16081/j.epae.201908002

Qin, B., & Liu, D. (2020). Research progresses and prospects on analysis and control of cyber-physical system for power grid. *Proceedings of the CSEE*, 40(18), 5816–5827. https://doi.org/10.13334/j.0258-8013.pcce.200422

Rueda, D. F., & Calle, E. (2017). Using interdependency matrices to mitigate targeted attacks on interdependent networks: A case study involving a power grid and backbone telecommunications networks. *International Journal on Critical Infrastructure Protection*, 16, 3–12. https://doi.org/10.1016/j.ijcip.2016.11.004

Su, T. T., Pan, X. Z., Xiao, H. Y., & Shen, J. W. (2012). Research on attack graph based on attributes adjacency matrix. *Journal of Electronics & Information Technology*, 34(7), 1744–1747. https://doi.org/10.1016/j.jelit.2012.07-037

Tan, Y., Luo, Y., Tan, X., & Jiang, P. (2018). Analysis on structural vulnerabilities of cyber physical power systems. *Journal of Hunan University*, 45(8), 91–98. https://doi.org/10.16339/j.cnki.hdxkbzkb.2018.08.013

Tang, F., Wei, D., Ji, X., Liu, D., & Tu, L. (2016). Improving interdependent networks robustness by adding connectivity links. *Physica A: Statistical Mechanics and its Applications*, 444, 9–19. https://doi.org/10.1016/j.physa.2015.10.010

Vespignani, A. (2010). Complex networks: The fragility of interdependency. *Nature*, 464(7291), 984. https://doi.org/10.1038/464984a

Wang, C., Dong, X., Sun, H., Wang, F., Wang, Y., & Wang, Y. (2021). Modeling method of power cyber-physical system considering multi-layer coupling characteristics. *Automation of Electric Power Systems*, 45(3), 83–91. https://doi.org/10.7500/AEPS20200109004

Wang, T., Sun, C., Gu, X., & Qin, X. (2018). Modeling and vulnerability analysis of electric power communication coupled network. *Proceedings of the CSEE*, 38(12), 3556–3567. https://doi.org/10.13334/j.0258-8013.pcce.170233

Wang, X., Zhijian, H. U., Fangjie, W. U., Shi, M., Tang, P., & Qiu, X. (2016). Improved adjacent matrix based sparse technology and its application in power system calculation. *Power System Protection and Control*, 44(9), 50–56. https://doi.org/10.7667/PSPC151094

Yaacoub, J., Salman, O., Noura, H., Kaaniche, N., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, 77, 103201. https://doi.org/10.1016/j.micpro.2020.103201

Yan, C., Bie, Z., & Wang, C. (2019). Risk assessment studies for new generation energy system. *Power System Technology*, 43(1), 12–22. https://doi.org/10.13334/j.0000-3673.pst.2018.2482
Zhang, W., & Wang, J. (2020). Robustness analysis of electric-gas-information coupled system based on percolation theory. *Electric Power Science and Engineering, 36*(8), 17–24. https://doi.org/CNKI:SUN:DLQB.0.2020-08-003

Zhou, F., He, X., Yuan, Y., & Zhang, M. (2020). Influence of interlink topology on multilayer network robustness. *Sustainability* 12*(3)*, 1202. https://doi.org/10.3390/su12031202