energies

MDPI

Article

Modeling and Vulnerability Analysis of Cyber-Physical Power Systems Considering Network Topology and Power Flow Properties

Jia Guo [1,*], Yuqi Han [1], Chuangxin Guo [1], Fengdan Lou [2] and Yanbo Wang [2]

[1] College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China; hanyuqi@zju.edu.cn (Y.H.); guochuangxin@zju.edu.cn (C.G.)

[2] State Grid Zhejiang Electric Power Company, Hangzhou 310027, China; loufengdan@163.com (F.L.); happyper@163.com (Y.W.)

* Correspondence: guojia_ee@zju.edu.cn; Tel.: +86-571-8795-2296

Academic Editors: Mashrur (Ronnie) Chowdhury and Kakan Dey
Received: 30 September 2016; Accepted: 5 January 2017; Published: 12 January 2017

Abstract: Conventional power systems are developing into cyber-physical power systems (CPPS) with wide applications of communication, computer and control technologies. However, multiple practical cases show that the failure of cyber layers is a major factor leading to blackouts. Therefore, it is necessary to discuss the cascading failure process considering cyber layer failures and analyze the vulnerability of CPPS. In this paper, a CPPS model, which consists of cyber layer, physical layer and cyber-physical interface, is presented using complex network theory. Considering power flow properties, the impacts of cyber node failures on the cascading failure propagation process are studied. Moreover, two vulnerability indices are established from the perspective of both network structure and power flow properties. A vulnerability analysis method is proposed, and the CPPS performance before and after cascading failures is analyzed by the proposed method to calculate vulnerability indices. In the case study, three typical scenarios are analyzed to illustrate the method, and vulnerabilities under different interface strategies and attack strategies are compared. Two thresholds are proposed to value the CPPS vulnerability roughly. The results show that CPPS is more vulnerable under malicious attacks and cyber nodes with high indices are vulnerable points which should be reinforced.

Keywords: vulnerability analysis; cyber-physical power system (CPPS); cascading failure; complex network theory; interdependence

1. Introduction

Modern power systems contain huge amounts of cyber devices, which form the cyber network to monitor, control and protect the physical network. The interdependence of the cyber network and physical network makes modern power systems typical cyber-physical systems, i.e., cyber-physical power systems (CPPS). However, the cyber layer in a CPPS brings new uncertainties while improving the power supply quality. Unexpected malfunctions in the cyber layer may lead to the loss of visibility and control of the physical layer, placing the CPPS at great risk. Supervisory control and data acquisition (SCADA)/energy management system (ENS) failures were major factors leading to the 2003 Italy blackout and 2003 Northeast blackout [1,2]. In addition, the Ukraine power grid suffered a blackout in 2015 due to hacker attacks, which shows that malicious attacks on CPPS may lead to more serious consequences [3]. Therefore, it is necessary to research the impact of the cyber layer during the cascading failure process, and analyze the vulnerability of CPPS, especially the vulnerability of the cyber layer.

Multiple methods were introduced in [4–11] to assess the vulnerability of conventional power systems. These studies ignore the cyber layer and focus on physical layer vulnerability assessment. In the CPPS environment, such a consideration is not appropriate since the influence of the cyber layer is too great to ignore. Interdependences between cyber layer and physical layer should be analyzed. In the aspects of CPPS modeling and interdependence assessment, reference [12] established a cyber-based dynamic model which had network structure-preserving properties that could improve the efficiency of distributed electric power system decision making. A cyber-physical equivalent model for a hierarchical control system (HCS) had been proposed in [13]. The HCS network was abstracted to a node-branch graph using this model, and information flow was expressed by a series of mathematical equations for the sake of cyber-contingency assessment. Falahati et al. [14,15] discussed direct and indirect interdependencies in modern power systems, introduced a state mapping method to map the cyber layer failures to physical layer failures, and two optimization models were presented to minimize the losses. The impact of direct cyber-power interdependencies (DCPIs) was also studied in [16], and risk assessment methods under different distributed generation (DG) scenarios were proposed. Reference [17] incorporated WAMS malfunction in power system reliability assessment. The authors indicated that wide-area measurement system (WAMS) malfunctions might lead to power systems being unobservable and uncontrollable, which would prevent the operators from taking remedial actions. Lei et al. designed a typical IEC-61850-based protection system incorporating physical and cyber components, and developed the cyber-physical interface matrix (CPIM) which defined the relationship between the cyber subsystems and physical subsystems in terms of failure modes and effects [18]. Then, the concepts were extended from substation to integrated system, and the consequent event matrix (CEM) was established to provide detailed information about affected transmission lines [19]. The applications of CPIM and CEM could decouple the cyber part analysis from the physical part analysis, and provide a more tractable method for CPPS reliability assessment.

Considering the impact of the cyber layer, several studies have focused on vulnerability assessments of power systems. Zonouz et al. [20] presented a security-oriented cyber-physical contingency analysis (SOCCA) framework to evaluate the impacts of both accidental contingencies and malicious attacks. Security indices were calculated for the power grid's corresponding Markov decision process (MDP) model, and various security incidents were ranked for proactive intrusion prevention solutions. Vulnerabilities of SCADA systems at three levels—system, scenarios, and access points—were evaluated in [21], and the impacts of a potential electronic intrusion were expressed by its potential loss of load in power systems. The result showed that a lower password policy threshold would lead to a lower probability of success for the intrusion attempts. Reference [22] indicated that failures in one network might result in failures in the other networks, and the allocation of interconnecting links between physical nodes and cyber nodes would greatly infect the robustness of the entire system. Then, an optimum inter-link allocation strategy was characterized under the condition of unknown subsystem topology. Chen et al. [23] proposed two models of hidden failures in protection systems, and analyzed the contribution of hidden failures to cascading failure. Risk indices of power system cascading collapse were set up, including bus isolated risk, load isolated risk, grid break-up risk and integrated system risk. Reference [24] presented CPINDEX, a security-oriented stochastic risk management technique to calculate the vulnerability rank of cyber-physical contingencies. Considering cyber network configurations, power system topology and the interdependencies among them, stochastic Bayesian network models of the entire cyber-physical infrastructure were established, and the security level of the current cyber-physical state was calculated using a graph-theoretic algorithm. Huang et al. [25,26] studied the cascading failure process in CPPS using percolation theory, and presented a detailed mathematical analysis of cascading failure propagation. For interdependences in CPPS, Huang et al. made the following assumptions: a node can operate only if it has at least one inter link (a link that connects cyber node and physical node) with a node that functions. Based on the assumption, the fraction of nodes that could still function after the

cascading failure was estimated. The results showed that there exists a threshold for the proportion of faulty nodes, above which the system collapses.

In the CPPS environment, with wide application of communication, computer and control technologies, operators have a clear view on the real-time state of the physical layer and are able to control it from control centers. The cyber layer and physical layer have various impacts on the other layer, and failures in one layer may cause and affect the cascading failure. Reference [17] studied the impacts of monitoring/control functions on power systems, but did not take the cyber layer topology and properties into account, and the model is not precise enough. Reference [25] made an assumption about interdependence in CPPS and proposed a cascading failure model which could simulate the failure propagation between two layers. However, the model did not consider the characteristics of power flow in the physical layer, and the assumption about interdependence was not quite reasonable. For example, substation automation systems (SAS), which are abstracted into cyber nodes, are usually equipped with an uninterruptible power supply (UPS). During the cascading failure process, cyber nodes won't fail due to the lack of power supply even if related physical nodes fail. Besides, when related cyber nodes fail, physical nodes will be unobservable and uncontrollable, but these physical nodes may still operate if there is no disturbance to the current system state. Physical nodes won't fail due to the lack of monitoring and control either. To describe the cascading failure process and identify the vulnerable parts in CPPS more comprehensively, this paper proposes a practical CPPS model based on complex network theory, and introduces a vulnerability analysis method incorporating information processing analysis and power flow analysis. Vulnerabilities under different cyber-physical interface strategies and attack strategies are analyzed and compared to provide suggests to CPPS planners and operators. The main contributions of this paper are summarized below:

- Considering cyber layer topology, physical layer topology and cyber-physical interface strategy, the CPPS model is proposed based on complex network theory.
- Incorporating information processing analysis and power flow analysis into topological analysis, a vulnerability analysis method is introduced to simulate the interactions between cyber layer and physical layer during the cascading failure process.
- Two vulnerability indices are proposed from the perspective of both topology structure and network property, vulnerabilities under different conditions are analyzed and compared.

The remainder of this paper is organized as follows: a detailed CPPS model is proposed in Section 2. In Section 3, the consequences of cyber node failures are analyzed, and a CPPS vulnerability analysis method is introduced. Case studies and result analysis are presented in Section 4. Finally, Section 5 concludes the paper.

2. CPPS Modeling

A CPPS consists of numerous cyber devices and physical devices, which form a cyber layer and a physical layer, respectively. The control center is in charge of calculation and decision making while the rest of the cyber layer is in charge of data acquisition and transmission. A typical CPPS structure is shown in Figure 1. Based on the complex network theory, the whole CPPS can be abstracted into an undirected network which consists of cyber nodes, physical nodes and connections between them. The topological relationship of CPPS can be expressed by the CPPS adjacency matrix $A = (a_{i,j})_{N+M \times N+M}$. Assuming that the CPPS includes N cyber nodes $(C_1 \cdots C_N)$ and M physical nodes $(P_1 \cdots P_M)$, the rank of A will be $N + M$, and the structure of A is as follows:

$$A = \begin{bmatrix} A_c & A_{c-p} \\ (A_{c-p})^T & A_p \end{bmatrix} = \begin{array}{c} \\ C_1 \\ \vdots \\ C_N \\ P_1 \\ \vdots \\ P_M \end{array} \begin{array}{c} \begin{array}{cccccc} C_1 & \cdots & C_N & P_1 & \cdots & P_M \end{array} \\ \begin{bmatrix} a_{1,1} & \cdots & a_{1,N} & a_{1,N+1} & \cdots & a_{1,N+M} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{N,1} & \cdots & a_{N,N} & a_{N,N+1} & \cdots & a_{N,N+M} \\ a_{N+1,1} & \cdots & a_{N+1,N} & a_{N+1,N+1} & \cdots & a_{N+1,N+M} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{N+M,1} & \cdots & a_{N+M,N} & a_{N+M,N+1} & \cdots & a_{N+M,N+M} \end{bmatrix} \end{array} \quad (1)$$

where A_c is the adjacency matrix of cyber layer which represents the connections inside cyber layer; A_p is the adjacency matrix of physical layer which represents the connections inside physical layer; A_{c-p} is the cyber-physical interface matrix which represents the interconnections between cyber layer and physical layer; $(A_{c-p})^T$ is the transposed matrix of A_{c-p}.

Obtaining of A_c, A_p and A_{c-p} will be presented in the following subsections.

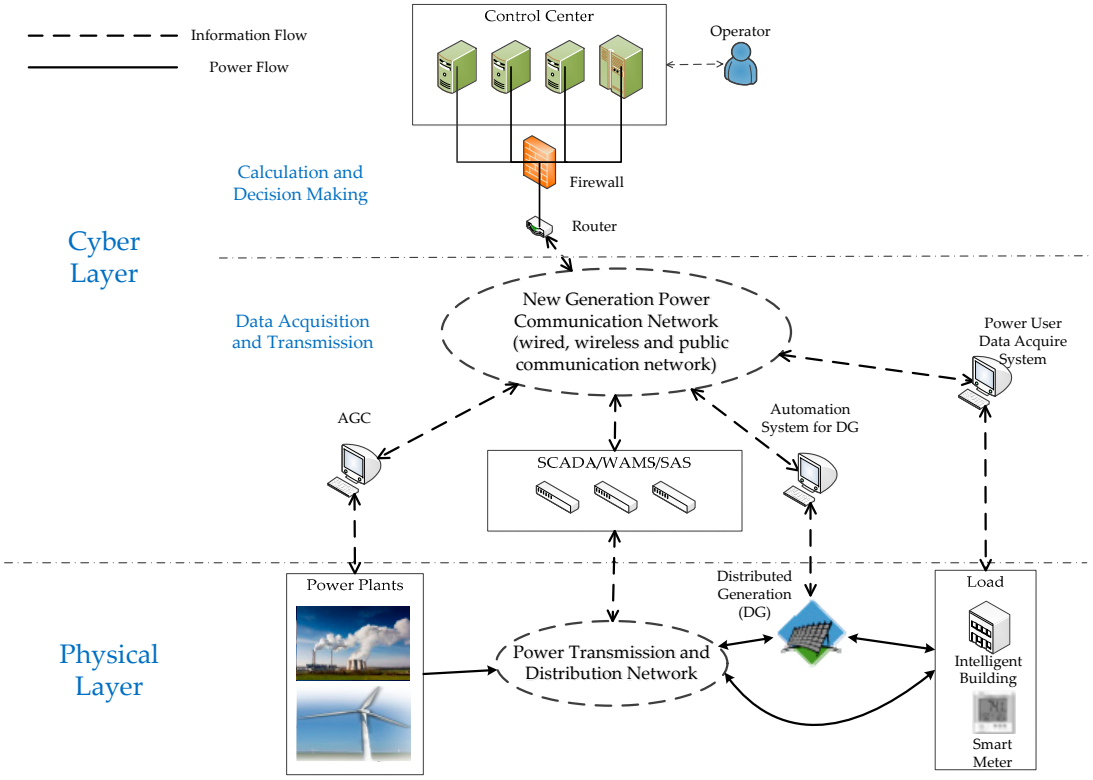


Figure 1. A typical structure of a CPPS.

2.1. Cyber Layer Model

The cyber layer is an Ethernet-based communication network which monitors and controls the physical layer. Cyber nodes are the abstractions of cyber devices and related algorithms, such as SAS. Cyber edges are the abstractions of communications links. Scale-free network [27] is a typical complex network which widely exists in the real world. A scale-free network is a network whose degree distribution follows a power law asymptotically. The main characteristic in a scale-free network is the distribution of the degree of node inhomogeneity. Massive amounts of data show that the Ethernet-based power system communication network is also a scale-free network. The Ethernet-based power system communication network can be divided into three layers: the core layer, the distribution layer and the access layer. The core layer and the distribution layer only include several nodes, but these nodes have much higher node degrees than nodes in the access layer. With the development

of the network, more nodes would access the access layer and make degree distribution more inhomogeneous. For example, a double-star power system communication network is a scale-free network [28]. Therefore, the cyber layer is considered to be a scale-free network, which can be modeled using the Barabási-Albert model. The modeling procedure is as follows:

1. Network growth: The initial network consists of three nodes and three edges. Every two nodes are connected by an edge. Each time, add a new node to the network which is connected to two existing nodes in the current network.
2. Preferential attachment: The probability that the new node will be connected to an existing node depends on the degree of the existing node. Assuming that k_i is the degree of existing node i, $\sum_j k_j$ is the sum of all existing node degrees, The probability p_i that the new node will be connected to existing node i will be:

$$p_i = \frac{k_i}{\sum_j k_j} \tag{2}$$

After $N-3$ times, a scale-free network with N nodes is established as the cyber layer of CPPS. $A_c = \left(a_{i,j}\right)_{N\times N}$ is the adjacency matrix of the cyber layer network. The element $a_{i,j}$ in A_c is 1 if there exists a cyber edge connecting cyber nodes C_i and C_j, otherwise is 0. Especially, $a_{i,i} = 0$.

A cyber node is the abstraction of a subsystem in the cyber layer instead of a specific cyber device, which are the set of all the related cyber devices and algorithms to monitor or control a physical node. Actually, cyber nodes can be seen as the automation systems of substations or power plants. It is noteworthy that one cyber node (or several) should represent the control center (power dispatch center). The high degree nodes in a scale-free network are often considered to serve specific purposes in their networks. Therefore, the node C_K with the highest degree is considered to represent the control center.

Due to the properties of the cyber layer, the control center receives measurements, calculates and provides control commands but would cannot directly act on the physical layer. Therefore, the control center node should only be directly connected to other cyber nodes. Unless otherwise stated, the cyber nodes mentioned in the following of this paper mean other cyber nodes aside from the control center node.

2.2. Physical Layer Model

The physical layer is the current-carrying grid in CPPS, i.e., the conventional power system. Physical nodes are the abstractions of substations or power plants ignoring the internal structures inside them. Physical edges are the abstractions of transmission lines. For a given conventional power system structure, the physical layer model can be expressed by a complex network with M physical nodes after these abstractions. $A_p = \left(a_{i,j}\right)_{M\times M}$ is the adjacency matrix of physical layer network. The element $a_{i,j}$ in A_p is 1 if there exists a physical edge connecting physical nodes P_i and P_j, otherwise is 0. Especially, $a_{i,i} = 0$.

2.3. Cyber-Physical Interface Strategy

There are various interdependences between the cyber layer and the physical layer. Cyber nodes require state data provided by the physical nodes, and physical nodes require control commands provided by the cyber nodes to operate safely. The corresponding relationship between cyber nodes and physical nodes could greatly affect the characteristics of the entire CPPS. Reference [29] showed that different interface strategies of nodes in two networks have different influences on cascading failure processes between coupled networks, and proposed that the corresponding relationship of nodes in the two networks should have inter-similarity instead of randomness (i.e., nodes in two networks with similar topological properties tend to connect to each other).

In this paper, the cyber nodes and physical nodes are abstractions of subsystems instead of specific devices, and redundant devices inside a SAS would not affect the interconnection between cyber nodes and physical nodes. Therefore, we assume cyber nodes and physical nodes have a one-to-one correspondence (i.e., one cyber node only connects to one physical node and vice versa). To find out the optimal cyber-physical interface strategy to reduce the CPPS vulnerability, two cyber-physical interface strategies are analyzed and compared in this paper:

(1) Degree-betweenness interface strategy: This strategy states that cyber nodes with higher degrees and physical nodes with higher node betweennesses tend to connect to each other. The cyber nodes are sorted by node degree in descending order, and the physical nodes are sorted by node betweenness in descending order. Corresponding nodes in two sequences are connected by cyber-physical edges (i.e., the cyber node with highest degree is connected to the physical node with highest node betweenness, the cyber node with second highest degree is connected to the physical node with second highest node betweenness and so on). Cyber-physical edges are considered to be the abstractions of the interconnections between cyber layer and physical layer. For example, there are three cyber nodes (C_1, C_2, C_3) with degrees $(1, 2, 1)$ and three physical nodes (P_1, P_2, P_3) with node betweennesses $(1, 0, 0)$, the cyber-physical edges should be $(C_2 - P_1, C_1 - P_1, C_3 - P_3)$. Other degree and betweenness combination strategies are not considered, because reference [30] already verified that the degree-betweenness interface strategy could reduce vulnerability more than others.

(2) Closeness centrality interface strategy: This strategy represents that cyber and physical nodes with higher closeness centrality tend to connect to each other. The cyber and physical nodes are all sorted by closeness centralities in descending order, and the corresponding nodes in two sequences are connected with cyber-physical edges (i.e., the cyber node with highest closeness centrality is connected to the physical node with highest closeness centrality, the cyber node with second highest closeness centrality is connected to the physical node with second highest closeness centrality, and so on). Closeness centrality [31] is a node centrality index to measure the importance of a node, which can be expressed as follows:

$$C_c(i) = [\sum_{j \in V \cap j \neq i} d_{ij}]^{-1} \tag{3}$$

where $C_c(i)$ represents the closeness centrality of node i; V is the set of nodes in network; d_{ij} is the shortest distance from node i to node j.

$A_{c-p} = (a_{ij})_{N \times M}$ is the cyber-physical interface matrix. The element $a_{i,j}$ in A_{c-p} is 1 if there exists a cyber-physical edge connecting cyber node C_i and physical node P_j, otherwise is 0. Because control center node C_K is not directly connect to physical nodes, all the elements of Kth row in A_{c-p} are 0.

3. CPPS Vulnerability Analysis Method

The cyber layer acquires the operation state of the physical layer as the input information. After evaluation and calculation, control commands are sent to the physical layer. The physical layer receives the control commands, and adjust its operation state to satisfy the economy and security. This closed-loop control could prevent a cascading failure. The failure control process in CPPS can be described by the following brief steps:

Step 1: A physical layer failure happens, the physical layer state changes from s_0 to s_1.

Step 2: The physical layer state s_1 is acquired by cyber nodes through cyber-physical edges, and the acquired information is sent to the control center node through cyber layer network.

Step 3: In the control center node, the physical layer state s_1 is evaluated to judge whether the physical layer operates safely or not. If the evaluate result shows that there are limit violations in the physical layer, remedial actions should be calculated and generated.

Step 4: The remedial actions are sent to cyber nodes through the cyber layer network, then, sent to physical nodes through cyber-physical edges.

Step 5: The physical layer adjusts to a safely operation state s_2 according to the remedial actions. The initial physical layer failure is prevented from extending.

However, this process could face a critical problem when cyber nodes suffer from random failures or malicious attacks. In such situations, Step 2 and Step 4 will be influenced. If Step 2 is incorrect, part of the physical layer is unobservable to the control center node, and limit violations of the unobservable part cannot be known. Therefore, remedial actions may not be taken, and the violated component will eventually go off-line. If Step 4 is incorrect, part of the physical layer is uncontrollable, and parameters of the uncontrollable part cannot be dispatched. Therefore, the generated remedial action may not be the global optimal solution, and physical layer would suffer more losses.

3.1. Cyber Node Faliure Analysis

Due to the properties of the cyber layer, cyber nodes that cannot exchange information with the control center node and physical nodes are consider to be failed. Certainly, the cyber nodes that suffer from random failures or malicious attacks will directly fail. Besides, the cyber layer topology changes caused by the direct cyber node failure can cause more cyber nodes to lose communication with the control center node. Considering the cyber layer property and topology, the cyber nodes failure analysis is described as follows:

1. Choosing the direct failure cyber nodes. For each direct failure cyber node C_i, remove all edges connecting to C_i, i.e., set all the elements of ith row and ith column in the CPPS adjacency matrix A to be 0.
2. Getting the cyber layer adjacency matrix A_c from A, calculate the shortest distance from cyber nodes to the control center node C_K using Floyd-Warshall algorithm.
3. For each cyber node C_j, if the shortest distance from C_j to the control center node C_K is infinity, C_j is considered to be fail. Remove all edges connecting to C_j, and modify the CPPS adjacency matrix A.

3.2. Unobservable Consequence Analysis of Cyber Node Failure

The physical devices that can't send their measurements to the control center are considered to be unobservable. The cyber-physical interface matrix A_{c-p} is obtained from the modified A in Section 3.1. If all the elements of the jth column in A_{c-p} are zeros, it means that physical node P_j has no cyber-physical edge, and the bus abstracted to P_j is unobservable. For a transmission line, if the two buses connected by this line are all unobservable, the line is also unobservable. All the limit violations in unobservable bus set UB and unobservable line set UL cannot be observed.

Making B and L represent the bus set and the line set respectively. Only if there are limit violations in $B - UB$ or $L - UL$, remedial actions will be taken, otherwise, no remedial actions will be taken.

3.3. Uncontrollable Consequence Analysis of Cyber Node Failure

The physical devices that can't receive control commands from the control center are considered to be uncontrollable. Due to the one-to-one correspondence of cyber nodes and physical nodes, the unobservable bus must be uncontrollable, and vice versa. Therefore, UB can also represent the uncontrollable bus set, which is exactly the same as the unobservable bus set in Section 3.2.

Remedial actions taken by operators are simulated by optimal power flow algorithm (OPF) [32]. Assuming that the control center is aware of uncontrollable buses, the OPF is described as follows:

$$\min \sum_{i \in B} LS_i \tag{4}$$

subject to:

$$PG_i + P_i - PD_i + LS_i = 0 \quad i \in B \tag{5}$$

$$QG_i + Q_i - QD_i = 0 \quad i \in B \tag{6}$$

$$T_l \leq T_l^{\max} \quad l \in L \tag{7}$$

$$V_i^{\min} \leq V_i \leq V_i^{\max} \quad i \in B \tag{8}$$

$$PG_i^{\min} \leq PG_i \leq PG_i^{\max} \quad i \in B - UB \tag{9}$$

$$QG_i^{\min} \leq QG_i \leq QG_i^{\max} \quad i \in B - UB \tag{10}$$

$$0 \leq LS_i \leq PD_i \quad i \in B - UB \tag{11}$$

$$\Delta PG_i = 0,\ \Delta QG_i = 0,\ LS_i = 0 \quad i \in UB \tag{12}$$

where LS_i is the load shedding of bus i; P_i, Q_i are the injection active power and reactive power of bus i through lines; PD_i, QD_i are the active load and reactive load of bus i; PG_i, $PG_i^{\min}$, $PG_i^{\max}$, QG_i, $QG_i^{\min}$, $QG_i^{\max}$ are the active power and reactive power output, lower limit, upper limit of generating unit in bus i, if bus i actually has no generating unit, these parameters are all 0; T_l, $T_l^{\max}$ are the power flow and power flow limit of line l; V_i, $V_i^{\min}$, $V_i^{\max}$ are the voltage magnitude, voltage magnitude lower and upper limit of bus i; ΔPG_i, ΔQG_i are the increment of these parameters compared with the initial value before OPF; B and L are the bus set and the line set.

Equations (5)–(8) represent the bus active/reactive power balance constraint, transmission line power flow constraint and bus voltage constraint, which represent the properties of physical layer and will not change due to the cyber node failure. Equations (9)–(11) represent the generator active/reactive power constraint and load dispatch constraint, which will be affected by the cyber node failure. Equation (12) represents the uncontrollable consequence of cyber node failures. Several algorithm parameters become immutable, which may prevent the algorithm from converging to the global optimal solution and cause more loss in physical layer.

3.4. CPPS Vulnerability Index

The vulnerability of a system can be considered as the performance drop when a disruptive event emerges [33]. The main mission of a CPPS is to continue to provide a power supply. Therefore, we need to analyze the vulnerability of CPPS from the perspective of network properties. Besides, the remaining topological structure after the cascading failure is also important for vulnerability analysis. The more complete the remaining topological structure is, the faster the system recovers from the failure status. Therefore, we also need to analysis the vulnerability of CPPS from the perspective of topological structure. For this purpose, two vulnerability indices are proposed: ratio of edge loss (ROEL) and ratio of load loss (ROLL), to represent the CPPS performance drop from the perspective of both topological structure and power supply:

$$ROEN = \frac{N_e - N_e'}{N_e} \tag{13}$$

$$ROLL = \frac{P - P'}{P} \tag{14}$$

where N_e and N'_e represent the number of edges in the largest connected components of CPPS before and after the cascading failure caused by the disruptive event; P and P' represent the sum of load on all buses before and after the cascading failure caused by the disruptive event.

3.5. Overall Procedure

This paper proposed an analysis method to evaluate the vulnerability of CPPS. The flowchart of the proposed method is depicted in Figure 2, and the overall procedure is summarized as follows:

Step 1: Analyze the CPPS performance in normal state, calculate N_e and P.
Step 2: Set the failure of cyber nodes and transmission lines as the disruptive event.
Step 3: Analyze the cyber node failures using the method mentioned in Section 3.1.
Step 4: Establish the UB and UL using the method mentioned in Section 3.2, and form the initial CPPS state s.
Step 5: Calculate the AC power flow, and check whether there are limit violations in $B - UB$ and $L - UL$. If so, go to the next step; otherwise, go to Step 7.
Step 6: Do the OPF described in Equations (4)–(12). If the OPF has feasible solutions, set the optimal solution as the control commands which are sent to corresponding physical devices, and refresh the CPPS state; otherwise, take no remedial action.
Step 7: Calculate the AC power flow again, check whether there are still limit violations in B and L. If so, set the violated physical devices failed, refresh the CPPS state and return to Step 5; otherwise, go to the next step.
Step 8: Finish the cascading failure, calculate N'_e and P' and then, calculate the CPPS vulnerability indices ROEL and ROLL.

If the physical layer is split into several isolated islands during the procedure, Steps 5–7 should be applied to each island instead of the biggest island. Only if there are no limit violations in all islands, the cascading failure can be considered to be finished.

Step 3 represents the impact of cyber layer topological structure on cyber layer performance. Steps 5 and 6 represents the unobservable and uncontrollable consequences of cyber node failures. Step 7 actually simulates this violated physical devices failure process, if limit violations still exist in B and L, the violated physical devices will eventually fail. Violated lines will be tripped, violated buses will fail and all the generators and load on it will be lost.

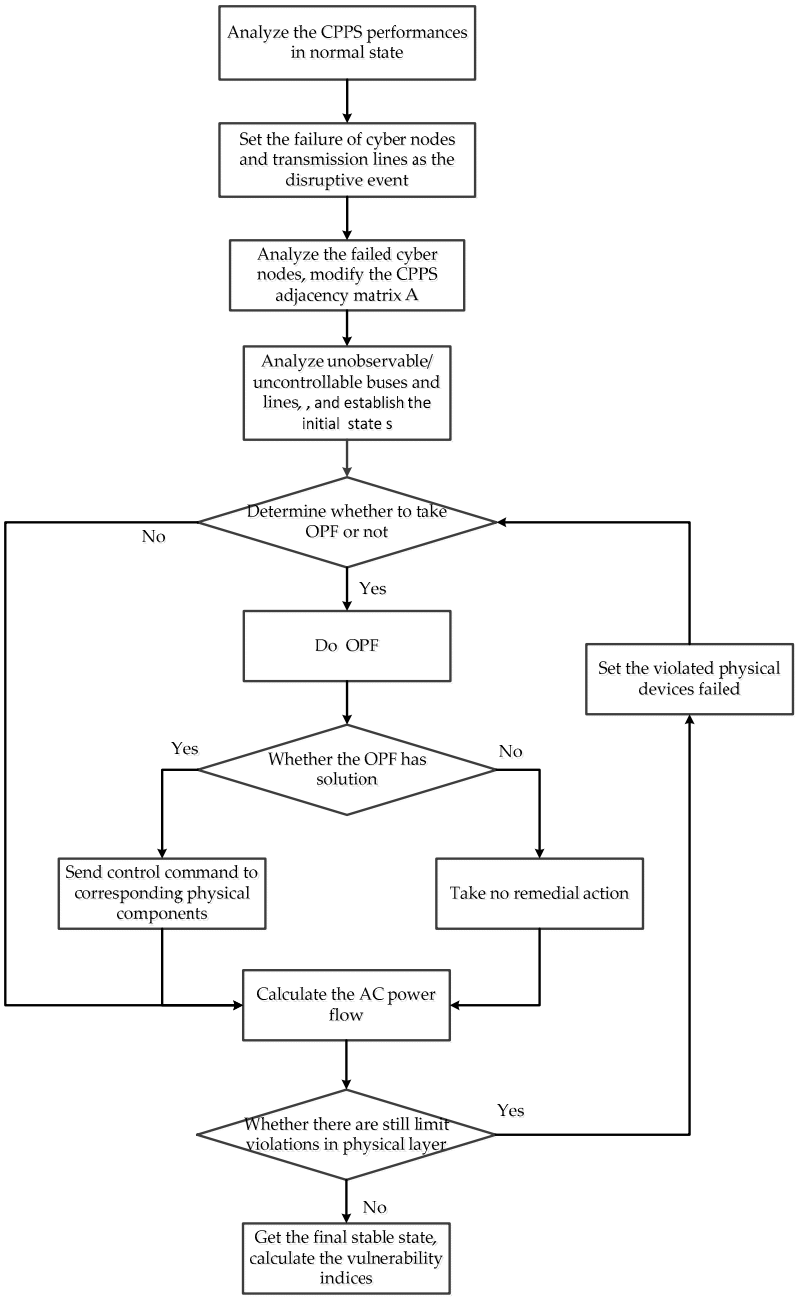


Figure 2. Flowchart of the CPPS vulnerability analysis method.

4. Case Study

The test system is modified from the IEEE 57-bus system. The physical layer of the test system is abstracted from the IEEE 57-bus system. The power flow limit of a transmission line is set to two times the initial power flow, which is shown in Table A1. Then, we take an economic dispatch for the physical layer and set the result as the normal state s_0. The cyber layer of the test system is a 58-node scale-free network which is generated using the method mentioned in Section 2.1, and the sparse expression of A_c is shown in Table A2.

The degrees and closeness centralities of cyber nodes, the betweennesses and closeness centralities of physical nodes are calculated and presented in Tables A3 and A4, respectively. Cyber node C_1 has the highest node degree 21. Therefore, C_1 is considered to represent the control center, and the other 57 cyber nodes are considered to represent the automation systems of substations and power

plants. The cyber-physical interface matrixes under two interface strategies are shown in Tables A5 and A6, respectively.

The disruptive event of CPPS consists of two parts: transmission line failures and cyber node failures. For transmission line failures, we only consider the N − 1 contingencies. The consideration of cyber node failures will be discussed in Section 4.2.

4.1. Scenario Analysis

To illustrate the proposed method more clearly, we assume cyber layer and physical layer are connected with degree-betweenness interface strategy in this subsection, and apply the proposed method on the following three typical scenarios:

Scenario 1: Line 13–15, connecting P_{13} and P_{15}, is failed without cyber node failures.
Scenario 2: Line 13–15 is failed while cyber node C_{14} is failed due to malicious attacks.
Scenario 3: Line 13–15 is failed while cyber nodes C_2, C_5, C_{18}, C_{25}, C_{35} and C_{38} are failed due to malicious attacks.

Scenario 1 simulates the failure control process in CPPS while the whole cyber layer is functioning normally. After Line 13–15 is failed, the power flow on Line 9–13 is 8.98 MVA while the limit of Line 9–13 is only 6.07 MVA. A limit violation is observed and the OPF algorithm is used to control the failure. The OPF result shows that it is only need adjusting generator outputs without load shedding to eliminate the limit violation. After the physical layer receives the control commands, CPPS is in a stable state again and the cascading failure is prevented. In this scenario, ROEL is 0.0040 and ROLL is 0. The generator outputs before and after the remedial action are shown in Table 1.

Table 1. The generator outputs before and after the remedial action in scenario 1.

Generator	Bus Location	P_{before} (MW)	Q_{before} (MVAR)	P_{before} (MW)	Q_{before} (MVAR)
1	1	203.7406	−16.1000	210.6361	9.3640
2	2	100.0000	−0.8000	100.0000	6.0882
3	3	65.2169	−1.0000	64.7753	−8.9589
4	6	70.0098	0.8000	92.7591	11.2877
5	8	416.9928	62.1000	388.1408	4.3116
6	9	0.0000	2.2000	0.0000	−2.9999
7	12	410.0000	128.5000	410.0000	29.7829

Scenario 2 simulates the uncontrollable consequences of a cyber node failure. When cyber node C_{14} is failed, Bus 8, which is abstracted to physical node P_8, is unobservable and uncontrollable. After the Line 13–15 outage happens and the limit violation of Line 9–13 is observed, although the OPF algorithm is activated, the parameters of Generator 5 located in Bus 8 cannot be dispatched in the optimization algorithm. In this scenario, the result shows that it requires not only adjusting generator outputs but also load shedding to eliminate the limit violation. The load on Bus 49 is curtailed from 18 MW to 16.83 MW. In this scenario, ROEL is 0.0280 and ROLL is 0.0009. The generator outputs before and after the remedial action are shown in Table 2.

Table 2. The generator outputs before and after the remedial action in scenario 2.

Generator	Bus Location	P_{before} (MW)	Q_{before} (MVAR)	P_{before} (MW)	Q_{before} (MVAR)
1	1	203.7406	−16.1000	441.8046	−2.4092
2	2	100.0000	−0.8000	100.0000	−17.0000
3	3	65.2169	−1.0000	0.0000	−10.0000
4	6	70.0098	0.8000	0.1340	−8.0000
5	8	416.9928	62.1000	416.9928	62.1000
6	9	0.0000	2.2000	0.0000	−3.0000
7	12	410.0000	128.5000	323.4762	95.7754

Scenario 3 simulates the unobservable consequence of cyber node failure. The initial failure may cause cascading failure, and physical layer may split into several isolated islands and suffer greater loss. When cyber nodes C_2, C_5, C_{18}, C_{25}, C_{35} and C_{38} are failed, Buses 9, 13, 19, 20, 21 and 22, which are abstracted to physical nodes P_9, P_{13}, P_{19}, P_{20}, P_{21}, P_{22}, are unobservable and uncontrollable. Therefore, Lines 9–13, 19–20, 20–21, 21–22 are also unobservable. After the Line 13–15 outage happens, the limit violation of Line 9–13 cannot the observed, so no remedial action will be taken and Line 9–13 will eventually fail. Then, Lines 19–20, 20–21 and 21–22 will fail one by one due to the unobservable consequences of cyber node failures. At this moment, Buses 20 and 21 have be split from the main island. Although the main island is in a stable state, the entire 2.3 MW load on Bus 20 is lost. In this scenario, ROEL is 0.1840 and ROLL is 0.0018.

4.2. Attack Strategy Comparision

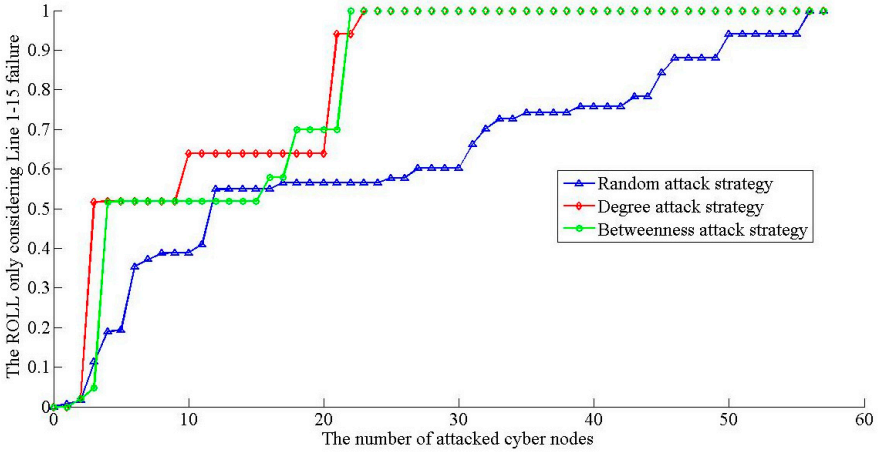
The vulnerabilities of CPPS under different attack strategies are different, so it is necessary to identify the attack strategy that is most dangerous to CPPS. Assuming the CPPS is modeled with degree-betweenness interface strategy in this subsection, we consider the following three possible attack strategies:

(1) Random attack strategy: The cyber node attack sequence is sorted randomly, the number of attacked cyber nodes increases from 0 to 57 gradually (i.e., the first attacked cyber node is selected randomly from all the cyber nodes, the second attacked cyber node is selected from the other cyber nodes except the first attacked cyber node, and so on). In order to guarantee the accuracy, we repeat the simulation 10 times and use the average value as the final result.

(2) Degree attack strategy: The cyber node attack sequence is sorted by node degrees in descending order, the number of attacked cyber nodes increases from 0 to 57 gradually (i.e., the first attacked cyber node is the cyber node with highest degree, the first attacked cyber node is the cyber node with second highest degree, and so on).

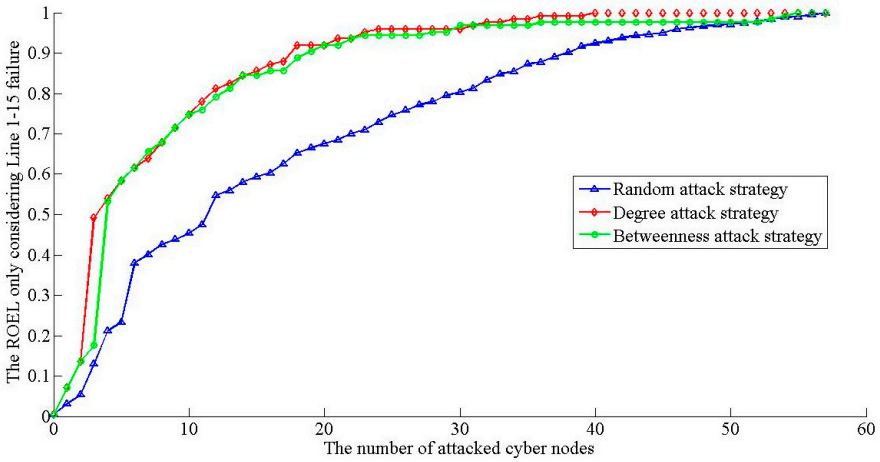
(3) Betweenness attack strategy: The cyber node attack sequence is sorted by node betweennesses in descending order, while the number of attacked cyber nodes increases from 0 to 57 gradually (i.e., the first attacked cyber node is the cyber node with highest node betweenness, the first attacked cyber node is the cyber node with highest node betweenness, and so on).

Under different attack strategies, the vulnerability indices of CPPS only considering Line 1–15 failure are shown in Figure 3, and the average vulnerability indices of CPPS considering line N − 1 contingencies are shown in Figure 4.



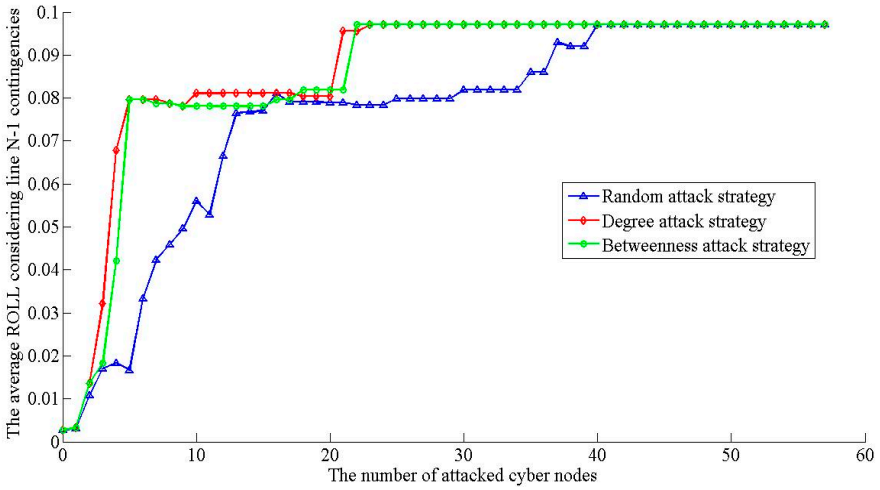
(**a**)

Figure 3. *Cont.*

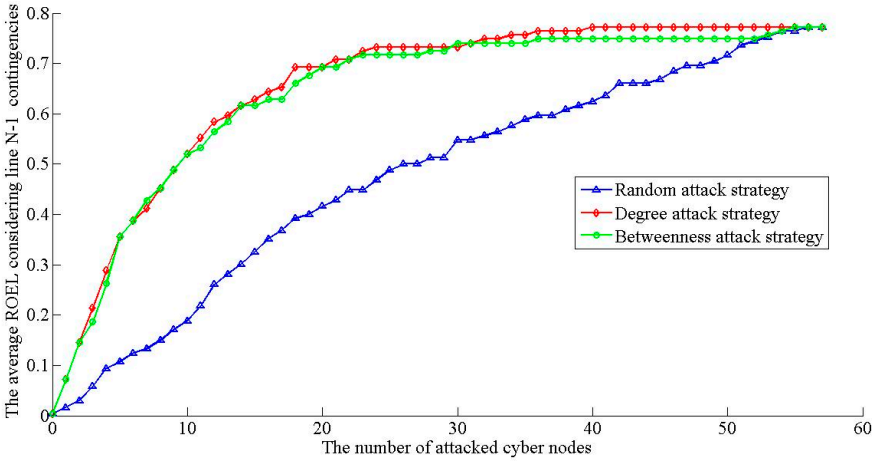


(**b**)

Figure 3. Under different attack strategies, the vulnerability indices of CPPS only considering Line 1–15 failure: (**a**) ROLL; (**b**) ROEL.



(**a**)



(**b**)

Figure 4. Under different attack strategies, the average vulnerability indices of CPPS considering line $N-1$ contingencies: (**a**) ROLL; (**b**) ROEL.

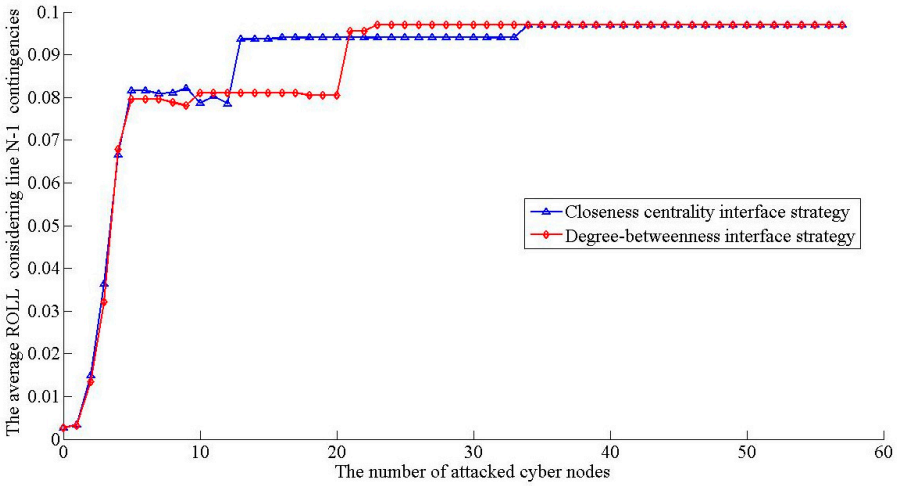
The results in Figures 3 and 4 show that CPPS is more vulnerable when suffering malicious attacks than random attacks. Because the cyber layer of CPPS is considered as a scale-free network, there are only several high degree cyber nodes. These cyber nodes are key nodes. When suffering random attacks, as long as these key nodes are still functioning, the whole system will maintain a high performance. The failures of key nodes could greatly damage the structure of the cyber layer, and make more physical nodes unobservable and uncontrollable. Once a line outage happens, it is can easily develop into a cascading failure. The curves of ROEL and ROLL are not similar, which means that influences of a disruptive event on topological structure and network performance are different. It is necessary to analyze the vulnerability of CPPS from both perspectives.

From both Figures 3a and 4a, we can see that there are two sudden changes in the ROLL curves. The first sudden change reflects the unobservable consequence of cyber node failures. Because the first several steps of cascading failure cannot be observed, the affected area will extend fast and more load will be lost. The second sudden change reflects the uncontrollable consequence of cyber node failures. Although the physical layer has split into several isolated islands, some islands may be still able to function alone. However, to ensure the frequency stability, the generators or load in a functioning island must be controllable. With more cyber nodes being attacked, the isolated islands will be totally uncontrollable and eventually collapse.

The attacked cyber node number of two sudden changes can be seen as two thresholds which can be used to value the CPPS vulnerability roughly. From Figure 4a, we can determine that the two thresholds under degree attack strategy are 5 and 21, and the two thresholds under betweenness attack strategy are 5 and 22. The result means a degree attack strategy is more dangerous to CPPS.

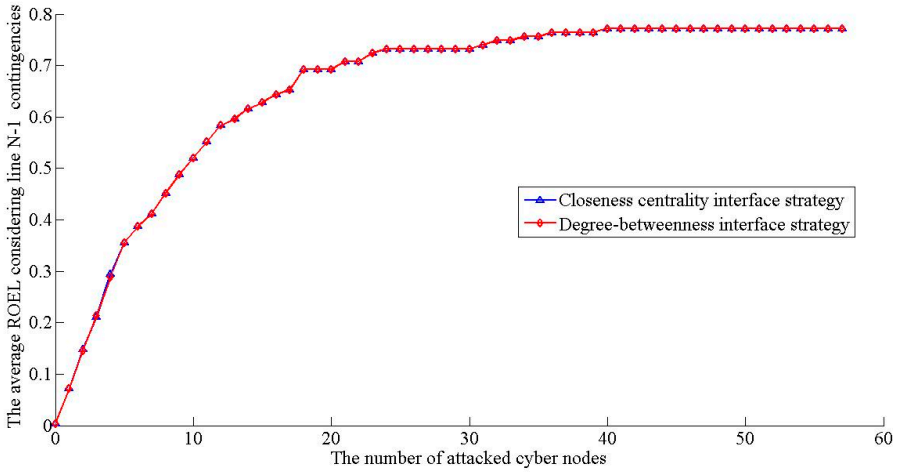
4.3. Cyber-Physical Interface Strategy Comparision

Since the scale-free property of cyber layer gives the CPPS great robustness against random attacks, we should find out the optimal cyber-physical interface strategy against malicious attacks. In this subsection, we assume a degree attack strategy is used, and compare the two cyber-physical interface strategies introduced in Section 2.3. The average vulnerability indices of CPPS considering line $N-1$ contingencies are shown in Figure 5.



(a)

Figure 5. *Cont.*



(**b**)

Figure 5. Using different cyber-physical interface strategies, the average vulnerability indices of CPPS considering line N − 1 contingencies: (**a**) ROLL; (**b**) ROEL.

Although the ROEL curves of the different interface strategies are quite similar, the ROLL curves are quite different. The second threshold of the CPPS using closeness centrality interface strategy is smaller. When the CPPS is modeled using different cyber-physical interface strategies, the same cyber node may be connect to different physical nodes. If the same cyber nodes fail, the unobservable/uncontrollable physical area is different, and the performance drops of CPPS are certainly different. The two thresholds of CPPS using closeness centrality interface strategy are 5 and 13, while the two thresholds of CPPS using degree-betweenness interface are 5 and 21. Therefore, degree-betweenness interface is better than a closeness centrality interface strategy.

4.4. Additional Cyber-Physical Interconnections Analysis

In the previous analysis, a substation is considered to exchange data only with its own SAS, which means cyber nodes and physical nodes have a one-to-one correspondence. With the development of communication, computer and control technologies, the extra data exchange links from a substation to another substation's SAS through a public network or a wireless network may be both technically and economically possible. The interconnections between cyber nodes and physical node could be extended into "two-to-two".

In this subsection, we assume degree-betweenness interface is used. That is, the physical node with highest node betweenness is connected to the cyber nodes with the highest and second highest degree, the physical node with the second highest node betweenness is connected to the cyber nodes with the second highest and third highest degree and so on. The impacts of additional cyber-physical interconnections under a degree attack strategy are shown in Figure 6.

The result in Figure 6 shows that additional cyber-physical interconnections could effectively decrease the vulnerability of CPPS. The first threshold of "two-to-two" correspondence is 11, which is much bigger than the first threshold of "one-to-one" correspondence. Alse, the ROLL change is more gentle with additional cyber-physical interconnections. When the CPPS suffers a comparatively slight attack, only several cyber nodes fail. Due to the additional interconnections, the whole CPPS structure is more integrated and the cascading failure could be controlled more quickly. However, when the CPPS suffers a heavy attack, even the additional interconnections could not prevent the whole system from collapsing, and the two curves are similar after the first threshold. Therefore, additional interconnections could greatly decrease the vulnerability of CPPS, especially when facing slight threats.

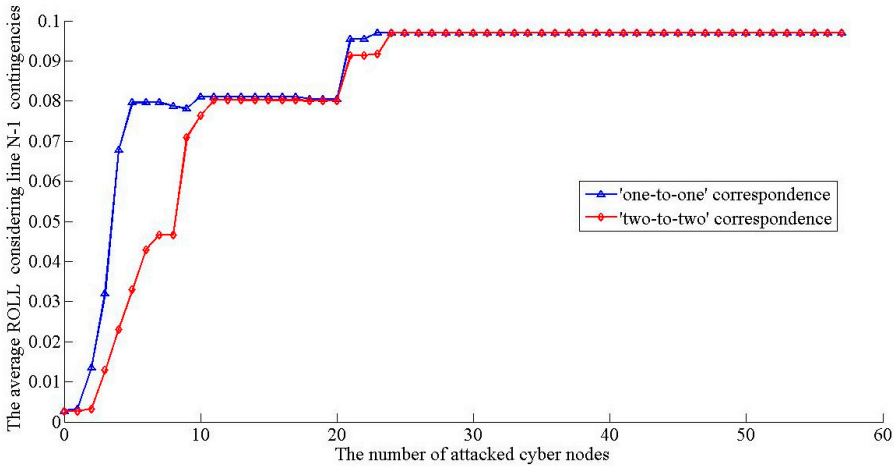


Figure 6. Adding additional cyber-physical interconnections, the average ROLL of CPPS considering line N − 1 contingencies.

5. Conclusions

Due to the interdependencies of the cyber layer and the physical layer, failures in the cyber layer may affect the behavior of the physical layer. During the cascading failure process, the lack of observations and control will accelerate the failure propagation and lead to greater losses. Therefore, it is necessary to analyze the vulnerability of CPPS and reinforce the weak points.

Against this background, this paper proposes a CPPS model which consists of a cyber layer, a physical layer and a cyber-physical interface, based on complex network theory. Considering the power flow properties, the unobservable and uncontrollable consequences of cyber node failure are discussed, and a CPPS vulnerability analysis method is proposed. Vulnerability indices are established from the perspectives of both topological structure and power supply. The initial failure of cyber node transmission lines is set as the disruptive event, and the cascading failure process caused by this disruptive event is simulated using the proposed method. The CPPS performance before and after cascading failures is compared, and the vulnerability of CPPS is analyzed. In the case study, two thresholds are proposed to roughly evaluate the CPPS vulnerability. The results show that CPPS is more vulnerable under malicious attacks, especially a degree attack strategy, and degree-betweenness interface is better in a closeness centrality interface strategy. The results also point out that cyber nodes with high degrees are key nodes. Improving the security of key nodes could reduce the CPPS vulnerability with minimum cost.

The model and method proposed in this paper are valuable to analyze the vulnerability in CPPS. Because of the complexity of CPPS, this paper makes some simplifications during the cascading failure simulation. In future studies, more factors should be taken into consideration, such as multi-level control center strategy, communication congestion, communication delay and hidden failures of the protection systems.

Acknowledgments: The work of Jia Guo, Yuqi Han and Chuangxin Guo was supported in part by the National Basic Research Program (973 Program) (2013CB228206) and in part by the State Key Program of National Natural Science Foundation of China (51537010).

Author Contributions: Jia Guo and Yuqi Han conceived and designed the experiments; Jia Guo performed the experiments, analyzed the data, and wrote the paper. Chuangxin Guo conceived the project; Yuqi Han, Chuangxin Guo, Fengdan Lou and Yanbo Wang reviewed and edited the manuscript. All authors read and approved the manuscript.

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

Appendix A. Parameters of the Test System

Table A1. The power flow limits of transmission lines.

From	To	$T_l^{\max}$ (MVA)	From	To	$T_l^{\max}$ (MVA)	From	To	$T_l^{\max}$ (MVA)
1	2	262.5306	14	15	141.1414	41	42	18.9184
2	3	195.7659	18	19	9.6738	41	43	24.2486
3	4	121.5316	19	20	2.7535	38	44	50.0832
4	5	28.9854	21	20	2.2979	15	45	74.7822
4	6	30.0906	21	22	2.3008	14	46	110.3533
6	7	35.7214	22	23	20.2854	46	47	108.4925
6	8	86.9207	23	24	7.5653	47	48	43.0824
8	9	358.2584	24	25	14.5446	48	49	14.7546
9	10	38.9846	24	25	13.9770	49	50	21.2650
9	11	26.9235	24	26	21.3183	50	51	26.7256
9	12	32.1148	26	27	21.8235	10	51	64.3518
9	13	6.0681	27	28	40.9961	13	49	93.6836
13	14	50.6947	28	29	51.5401	29	52	36.1949
13	15	99.6322	7	29	122.9730	52	53	25.1131
1	15	305.5369	25	30	17.7276	53	54	18.0454
1	16	158.5039	30	31	9.3630	54	55	27.4959
1	17	186.8515	31	32	4.1781	11	43	28.8698
3	15	76.7108	32	33	8.5176	44	45	74.7822
4	18	28.3463	34	32	16.7319	40	56	10.6847
4	18	35.8253	34	35	16.7319	56	41	11.2540
5	6	12.5437	35	36	30.1737	56	42	4.3035
7	8	160.5002	36	37	40.5700	39	57	9.6690
10	12	53.4232	37	38	51.4302	57	56	5.8435
11	13	21.7066	37	39	9.6893	38	49	23.0330
12	13	128.1994	36	40	10.7179	38	48	52.6217
12	16	70.1783	22	38	22.6531	9	55	43.1853
12	17	100.7499	11	41	19.6837	-	-	-

Table A2. The sparse expression of A_c.

i	j	$a_{i,j}$	i	j	$a_{i,j}$	i	j	$a_{i,j}$	i	j	$a_{i,j}$	i	j	$a_{i,j}$
2	1	1	16	4	1	57	10	1	4	22	1	45	39	1
3	1	1	19	4	1	1	11	1	18	22	1	4	40	1
4	1	1	22	4	1	2	11	1	36	22	1	11	40	1
5	1	1	24	4	1	40	11	1	1	23	1	11	41	1
6	1	1	25	4	1	41	11	1	15	23	1	27	41	1
7	1	1	29	4	1	52	11	1	26	23	1	18	42	1
8	1	1	33	4	1	55	11	1	38	23	1	26	42	1
10	1	1	40	4	1	1	12	1	2	24	1	7	43	1
11	1	1	49	4	1	9	12	1	4	24	1	28	43	1
12	1	1	50	4	1	48	12	1	27	24	1	6	44	1
13	1	1	51	4	1	1	13	1	1	25	1	14	44	1
16	1	1	56	4	1	5	13	1	4	25	1	54	44	1
17	1	1	1	5	1	6	14	1	1	26	1	34	45	1
18	1	1	4	5	1	10	14	1	23	26	1	39	45	1
19	1	1	7	5	1	30	14	1	42	26	1	53	45	1
23	1	1	13	5	1	31	14	1	9	27	1	15	46	1
25	1	1	15	5	1	44	14	1	24	27	1	18	46	1
26	1	1	21	5	1	3	15	1	41	27	1	3	47	1
28	1	1	35	5	1	5	15	1	1	28	1	18	47	1
30	1	1	48	5	1	23	15	1	2	28	1	5	48	1
37	1	1	52	5	1	36	15	1	43	28	1	12	48	1

Table A2. *Cont.*

i	j	$a_{i,j}$	i	j	$a_{i,j}$	i	j	$a_{i,j}$	i	j	$a_{i,j}$	i	j	$a_{i,j}$
1	2	1	58	5	1	46	15	1	4	29	1	4	49	1
3	2	1	1	6	1	1	16	1	20	29	1	35	49	1
4	2	1	4	6	1	4	16	1	1	30	1	3	50	1
8	2	1	9	6	1	20	16	1	14	30	1	4	50	1
11	2	1	14	6	1	1	17	1	14	31	1	3	51	1
17	2	1	32	6	1	2	17	1	18	31	1	4	51	1
18	2	1	44	6	1	34	17	1	6	32	1	5	52	1
24	2	1	1	7	1	1	18	1	10	32	1	11	52	1
28	2	1	5	7	1	2	18	1	37	32	1	55	52	1
34	2	1	43	7	1	20	18	1	4	33	1	10	53	1
35	2	1	1	8	1	22	18	1	18	33	1	45	53	1
56	2	1	2	8	1	31	18	1	2	34	1	3	54	1
1	3	1	10	8	1	33	18	1	17	34	1	44	54	1
2	3	1	39	8	1	42	18	1	45	34	1	11	55	1
9	3	1	3	9	1	46	18	1	2	35	1	52	55	1
15	3	1	6	9	1	47	18	1	5	35	1	2	56	1
21	3	1	12	9	1	1	19	1	49	35	1	4	56	1
47	3	1	27	9	1	4	19	1	15	36	1	10	57	1
50	3	1	39	9	1	16	20	1	22	36	1	20	57	1
51	3	1	1	10	1	18	20	1	1	37	1	5	58	1
54	3	1	8	10	1	29	20	1	32	37	1	20	58	1
1	4	1	14	10	1	57	20	1	10	38	1	-	-	-
2	4	1	32	10	1	58	20	1	23	38	1	-	-	-
5	4	1	38	10	1	3	21	1	8	39	1	-	-	-
6	4	1	53	10	1	5	21	1	9	39	1	-	-	-

Table A3. The degrees and closeness centralities of cyber nodes.

i	k_i	$C_c(i)$	i	k_i	$C_c(i)$	i	k_i	$C_c(i)$
1	21	0.0104	21	2	0.0062	41	2	0.0054
2	12	0.0090	22	3	0.0066	42	2	0.0057
3	9	0.0080	23	4	0.0070	43	2	0.0053
4	16	0.0090	24	3	0.0069	44	3	0.0059
5	10	0.0083	25	2	0.0071	45	3	0.0051
6	6	0.0079	26	3	0.0068	46	2	0.0060
7	3	0.0070	27	3	0.0056	47	2	0.0061
8	4	0.0074	28	3	0.0070	48	2	0.0059
9	5	0.0066	29	2	0.0064	49	2	0.0061
10	7	0.0074	30	2	0.0068	50	2	0.0064
11	6	0.0074	31	2	0.0060	51	2	0.0064
12	3	0.0069	32	3	0.0059	52	3	0.0060
13	2	0.0069	33	2	0.0065	53	2	0.0054
14	5	0.0062	34	3	0.0062	54	2	0.0057
15	5	0.0068	35	3	0.0065	55	2	0.0054
16	3	0.0074	36	2	0.0054	56	2	0.0068
17	3	0.0070	37	2	0.0067	57	2	0.0056
18	9	0.0081	38	2	0.0055	58	2	0.0060
19	2	0.0071	39	3	0.0059	-	-	-
20	5	0.0063	40	2	0.0063	-	-	-

Table A4. The betweennesses and closeness centralities of physical nodes.

i	s_i	$C_c(i)$	i	s_i	$C_c(i)$	i	s_i	$C_c(i)$
1	0.0067	0.0036	21	0.0146	0.0035	41	0.0258	0.0040
2	0.0014	0.0033	22	0.0470	0.0042	42	0	0.0034
3	0.0169	0.0039	23	0.0253	0.0037	43	0	0.0038
4	0.0181	0.0036	24	0.0292	0.0034	44	0.0098	0.0041
5	0	0.0033	25	0.0122	0.0027	45	0.0091	0.0041
6	0.0167	0.0038	26	0.0145	0.0031	46	0.0029	0.0037
7	0.0239	0.0038	27	0.0134	0.0031	47	0.0035	0.0036
8	0.0300	0.0042	28	0.0149	0.0032	48	0.0090	0.0043
9	0.0600	0.0047	29	0.0240	0.0034	49	0.0552	0.0049
10	0.0056	0.0039	30	0.0073	0.0025	50	0.0049	0.0039
11	0.0350	0.0045	31	0.0066	0.0024	51	0.0022	0.0037
12	0.0172	0.0043	32	0.0178	0.0026	52	0.0043	0.0029
13	0.0696	0.0051	33	0	0.0023	53	0.0041	0.0030
14	0.0078	0.0042	34	0.0216	0.0028	54	0.0085	0.0033
15	0.0320	0.0044	35	0.0280	0.0032	55	0.0150	0.0038
16	0.0011	0.0036	36	0.0392	0.0037	56	0.0204	0.0037
17	0.0011	0.0036	37	0.0437	0.0042	57	0.0032	0.0034
18	0.0063	0.0030	38	0.0819	0.0048	-	-	-
19	0.0059	0.0029	39	0.0051	0.0035	-	-	-
20	0.0088	0.0031	40	0.0117	0.0036	-	-	-

Table A5. The sparse expression of A_{c-p} with degree-betweenness interface strategy.

i	j	$a_{i,j}$	i	j	$a_{i,j}$	i	j	$a_{i,j}$	i	j	$a_{i,j}$
33	1	1	53	16	1	36	31	1	49	46	1
51	2	1	54	17	1	24	32	1	47	47	1
27	3	1	37	18	1	56	33	1	21	48	1
22	4	1	38	19	1	16	34	1	3	49	1
55	5	1	25	20	1	20	35	1	42	50	1
28	6	1	35	21	1	6	36	1	50	51	1
12	7	1	18	22	1	10	37	1	43	52	1
14	8	1	23	23	1	4	38	1	46	53	1
5	9	1	15	24	1	41	39	1	29	54	1
40	10	1	45	25	1	52	40	1	32	55	1
11	11	1	39	26	1	8	41	1	17	56	1
26	12	1	44	27	1	57	42	1	48	57	1
2	13	1	34	28	1	58	43	1	-	-	-
30	14	1	7	29	1	13	44	1	-	-	-
9	15	1	31	30	1	19	45	1	-	-	-

Table A6. The sparse expression of A_{c-p} with closeness centrality interface strategy.

i	j	$a_{i,j}$	i	j	$a_{i,j}$	i	j	$a_{i,j}$	i	j	$a_{i,j}$
33	1	1	50	16	1	43	31	1	35	46	1
58	2	1	51	17	1	55	32	1	29	47	1
12	3	1	27	18	1	45	33	1	10	48	1
20	4	1	57	19	1	36	34	1	4	49	1
31	5	1	44	20	1	32	35	1	28	50	1
15	6	1	21	21	1	56	36	1	37	51	1
30	7	1	11	22	1	19	37	1	38	52	1
25	8	1	22	23	1	5	38	1	42	53	1

Table A6. *Cont.*

i	j	$a_{i,j}$	i	j	$a_{i,j}$	i	j	$a_{i,j}$	i	j	$a_{i,j}$
18	9	1	46	24	1	34	39	1	52	54	1
13	10	1	53	25	1	40	40	1	26	55	1
3	11	1	48	26	1	23	41	1	9	56	1
8	12	1	54	27	1	14	42	1	49	57	1
2	13	1	39	28	1	24	43	1	-	-	-
16	14	1	47	29	1	17	44	1	-	-	-
6	15	1	41	30	1	7	45	1	-	-	-

References

1. Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **2010**, *464*, 1025–1028. [CrossRef] [PubMed]
2. US-Canada Power System Outage Task Force. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. 2004. Available online: https://www.ferc.gov/industries/electric/indus-act/reliability/blackout/ch1-3.pdf (accessed on 6 January 2017).
3. Guo, Q.L.; Xin, S.J.; Wang, J.H.; Sun, H.B. Comprehensive security assessment for a cyber physical energy system: A lesson from Ukraine's blackout. *Autom. Electr. Power Syst.* **2016**, *40*, 145–147.
4. Albert, R.; Albert, I.; Nakarado, G.L. Structural vulnerability of the North American power grid. *Phys. Rev. E* **2004**, *69*, 292–313. [CrossRef] [PubMed]
5. Bompard, E.; Napoli, R.; Xue, F. Extended topological approach for the assessment of structural vulnerability in transmission networks. *IET Gener. Transm. Distrib.* **2010**, *4*, 716–724. [CrossRef]
6. Yan, J.; Zhu, Y.; He, H.; Sun, Y. Multi-contingency cascading analysis of smart grid based on self-organizing map. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 646–656. [CrossRef]
7. Doorman, G.L.; Uhlen, K.; Kjolle, G.H.; Huse, E.S. Vulnerability analysis of the Nordic power system. *IEEE Trans. Power Syst.* **2006**, *21*, 402–410. [CrossRef]
8. Wangdee, W.; Billinton, R. Bulk electric system well-being analysis using sequential Monte Carlo simulation. *IEEE Trans. Power Syst.* **2006**, *21*, 188–193. [CrossRef]
9. Fouad, A.A.; Zhou, Q.; Vittal, V. System vulnerability as a concept to assess power system dynamic security. *IEEE Trans. Power Syst.* **1994**, *9*, 1009–1015. [CrossRef]
10. Kamwa, I.; Pradhan, A.K.; Joos, G. Automatic segmentation of large power systems into fuzzy coherent areas for dynamic vulnerability assessment. *IEEE Trans. Power Syst.* **2007**, *22*, 1974–1985. [CrossRef]
11. Rocco, C.M.; Ramirez-Marquez, J.E.; Salazar, D.E.; Yajure, C. Assessing the vulnerability of a power system through a multiple objective contingency screening approach. *IEEE Trans. Reliab.* **2011**, *60*, 394–403. [CrossRef]
12. Ilic, M.D.; Xie, L.; Khan, U.A.; Moura, J.M. Modeling of future cyber-physical energy systems for distributed sensing and control. *IEEE Trans. Syst. Man Cybern. A Syst. Hum.* **2010**, *40*, 825–838. [CrossRef]
13. Xin, S.; Guo, Q.; Sun, H.; Zhang, B.; Wang, J.; Chen, C. Cyber-Physical modeling and cyber-contingency assessment of hierarchical control systems. *IEEE Trans. Smart Grid* **2015**, *6*, 2375–2385. [CrossRef]
14. Falahati, B.; Fu, Y.; Wu, L. Reliability assessment of smart grid considering direct cyber-power interdependencies. *IEEE Trans. Smart Grid* **2012**, *3*, 1513–1524. [CrossRef]
15. Falahati, B.; Fu, Y. Reliability Assessment of smart grids considering indirect cyber-power interdependencies. *IEEE Trans. Smart Grid* **2014**, *5*, 1677–1685. [CrossRef]
16. Hashemi-Dezaki, H.; Askarian-Abyaneh, H.; Haeri-Khiavi, H. Impacts of direct cyber-power interdependencies on smart grid reliability under various penetration levels of micro-turbine/wind/solar distributed generations. *IET Gener. Trans. Distrib.* **2016**, *10*, 928–937. [CrossRef]
17. Aminifar, F.; Fotuhi-Firuzabad, M.; Shahidehpour, M.; Safdarian, A. Impact of WAMS malfunction on power system reliability assessment. *IEEE Trans. Smart Grid* **2012**, *3*, 1302–1309. [CrossRef]
18. Lei, H.T.; Singh, C.; Sprintson, A. Reliability modeling and analysis of IEC 61850 based substation protection systems. *IEEE Trans. Smart Grid* **2014**, *3*, 2194–2202. [CrossRef]

19. Lei, H.T.; Singh, C. Power system reliability evaluation considering cyber-malfunctions in substations. *Electr. Power Syst. Res.* **2015**, *129*, 160–169. [CrossRef]
20. Zonouz, S.; Davis, C.M.; Davis, K.R.; Berthier, R.; Bobba, R.B.; Sanders, W.H. SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures. *IEEE Trans. Smart Grid* **2014**, *5*, 3–13. [CrossRef]
21. Ten, C.W.; Liu, C.C.; Manimaran, G. Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Trans. Power Syst.* **2008**, *23*, 1836–1846. [CrossRef]
22. Yagan, O.; Qian, D.; Zhang, J.; Cochran, D. Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading Failures, and robustness. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 1708–1720. [CrossRef]
23. Chen, W.H.; Jiang, Q.Y.; Cao, Y.J. Risk assessment of power system cascading failure considering hidden failures of protective relayings. *Power Syst. Technol.* **2006**, *30*, 14–18.
24. Vellaithurai, C.; Srivastava, A.; Zonouz, S.; Berthier, R. CPINDEX: Cyber-physical vulnerability assessment for power-grid Infrastructures. *IEEE Trans. Smart Grid* **2015**, *6*, 566–575. [CrossRef]
25. Huang, Z.; Wang, C.; Stojmenovic, M.; Nayak, A. Characterization of cascading failures in interdependent cyber-physical systems. *IEEE Trans. Comput.* **2015**, *64*, 2158–2168. [CrossRef]
26. Huang, Z.; Wang, C.; Ruj, S.; Stojmenovic, M.; Nayak, A. Modeling Cascading Failures in Smart Power Grid Using Interdependent Complex Networks and Percolation Theory. In Proceedings of the Industrial Electronics and Applications (ICIEA), Melbourne, Australia, 19–21 June 2013.
27. Barabasi, A.L.; Albert, R. Emergence of scaling in random networks. *Science* **1999**, *286*, 509–512. [PubMed]
28. Hu, J.; Li, Z.H.; Duan, X.Z. Structural Feature Analysis of the Electric Power Dispatching Data Network. *Proc. CSEE* **2009**, *29*, 53–59.
29. Parshani, R.; Rozenblat, C.; Ietri, D.; Ducruet, C.; Havlin, S. Inter-similarity between coupled networks. *Europhys. Lett.* **2011**, *92*, 2470–2484. [CrossRef]
30. Cao, Y.J.; Zhang, Y.D.; Bao, Z.J. Analysis of cascading failures under interactions between power grid and communication network. *Electr. Power Autom. Equip.* **2013**, *33*, 7–11.
31. Freeman, L.C. Centrality in social networks conceptual clarification. *Soc. Netw.* **2012**, *1*, 215–239. [CrossRef]
32. Li, W.Y. *Risk Assessment of Power System: Model, Method and Application*, 1st ed.; Science Press: Beijing, China, 2006; pp. 105–109.
33. Cuadra, L.; Salcedo-Sanz, S.; Del Ser, J.; Jiménez-Fernández, S.; Geem, Z.W. A critical review of robustness in power grids using complex networks concepts. *Energies* **2015**, *8*, 9211–9265. [CrossRef]