

Article

Impact of Communication Link Overload on Power Flow and Data Transmission in Cyber–Physical Power Systems

Xinyu Liu ^{1,2,3} , Yan Li ^{1,2,3,*}  and Tianqi Xu ^{1,2,3} 

¹ School of Electrical and Information Technology, Yunnan Minzu University, Kunming 650504, China; xyliu7918@gmail.com (X.L.); xu.tianqi@ymu.edu.cn (T.X.)

² Yunnan Key Laboratory of Unmanned Autonomous System, Kunming 650504, China

³ Key Laboratory of Cyber–Physical Power System of Yunnan Colleges and Universities, Kunming 650504, China

* Correspondence: yan.li@ymu.edu.cn

Abstract: The volume of flow demand in cyber-physical power systems (CPPSs) fluctuates unevenly across coupled networks and is susceptible to congestion or overload due to consumers' energy demand or extreme disasters. Therefore, considering the elasticity of real networks, communication links with excessive information flow do not immediately disconnect but have a certain degree of redundancy. This paper proposes a dynamic cascading failure iterating model based on the distribution of information flow overload in a communication network and power flow betweenness in the physical power grid. First, a nonlinear load capacity model of a communication network with overload and weighted edges is introduced, fully considering the three link states: normal, failure, and overload. Then, flow betweenness substitutes for branch flows in the physical power network, and power flow on failed lines is redistributed using the load capacity model, simplifying the calculations. Third, under the influence of coupling relations, a comprehensive model based on improved percolation theory is constructed, with attack strategies formulated to more accurately assess the coupled networks. Simulations on the IEEE-39 bus system demonstrate that considering the overload capacity of communication links on a small scale enhances the robustness of coupled networks. Furthermore, deliberate link attacks cause more rapid and extensive damage compared to random attacks.



Citation: Liu, X.; Li, Y.; Xu, T. Impact of Communication Link Overload on Power Flow and Data Transmission in Cyber–Physical Power Systems.

Electronics **2024**, *13*, 3065. <https://doi.org/10.3390/electronics13153065>

Academic Editor: Christos J. Bouras

Received: 8 July 2024

Revised: 30 July 2024

Accepted: 31 July 2024

Published: 2 August 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: overloaded edges; information flow; power flow; cascading failures; improved percolation theory; cyber–physical power systems

1. Introduction

1.1. Background

With the development of the smart grid and the energy internet, the power system has become deeply coupled with the information system. The power system on the physical side and the communication system on the information side have gradually evolved into the cyber–physical power system (CPPS) [1]. While the coupled system has brought numerous benefits, it has also increased the risk of cascading failures across space. Vulnerabilities in the two systems through an overlapping network will increase the risk of fault propagation, such that even a single edge or node failure can impact the entire network, often leading to a global collapse [2,3]. For instance, the massive blackout in the western United States in 2003, the blackout in Ukraine in 2015, and the 815 blackout in Brazil in 2023 [4,5] were all caused by the failure of specific edges in the information network. These failures propagated to the power grid through functional coupling, ultimately resulting in the simultaneous paralysis of both systems.

1.2. Related Works

The analysis of past cases shows that when the communication system fails or is attacked, data packets can be lost or manipulated, preventing closed-loop control. Due to the cyber–physical coupling connection, the failure will propagate to affect power nodes in the physical network with a certain probability. Then, the failure continues spreading in the physical network, ultimately causing serious damage to the system [6–8]. Therefore, modeling the physical power grid, communication network, and its coupling connection is essential for understanding the propagation process of cascading failure across space.

In [9], a one-to-one coupling model between power and communication nodes was proposed, analyzing the robustness of the cascading failure system after the removal of a small fraction of nodes based on its topological model. In [10], the authors studied the robustness of a dual-layer scale-free communication network based on percolation theory. Based on [10], Ref. [11] considered the interactions among nodes in different layers as heterogeneous, studying a type of cascading dynamics in dual-layer networks that exhibit both interdependence and connectivity. Based on [9,10], Chen et al. [12] differentiated the nodes in the physical power grid into generator and load nodes, proposing a new interactive mechanism for cascading failures. In [13], the operational characteristics and topological structure of the transmission network were integrated to establish a cascade failure model for random faults in transmission lines under different coupling strategies, aiming to obtain an optimal robust coupled network. However, the coupling models established in these studies focus solely on topological structures, neglecting the operational characteristics of both sides of the coupled networks. In [14,15], power flow optimization in the physical power network was considered and the results of vulnerability under different strategies and information network topologies were compared, but the operational characteristics of the information network were not considered. In [16], the dynamic propagation of cascade failures between the power grid and the communication network was studied, considering the characteristics of power flow and data flow in two different systems, but the impact of data overload in the communication network on the coupled network was not considered. In [17], the recovery characteristics of different coupling strengths and network topologies based on a load-related cascade model were studied. Although the overload state of nodes was considered in this model, the extra load was not redistributed. Based on [16,17], Ding et al. [18] proposed an improved cascading failures model. This model considers the overload state and recovery process of cyber nodes, as well as the optimization of power flow in the physical layer and the redistribution of information flow during fault propagation. Building on this, Wang et al. [19] employed an AC power flow model to characterize the operational characteristics of the power grid, enhancing the accuracy of the power grid model. Simultaneously, it constructed a weighted communication network with control centers and applied a flow redistribution model. In [20], the authors proposed two types of strong and weak dependency models and analyzed the robustness changes of the coupling network using a congestion-aware load balancing scheme under initial random faults in the power layer. However, data flows in the communication layer were not considered. The authors of [21,22] considered communication node failures and established an improved cascade failure model based on the physical layer load distribution. In [23], the authors' proposed model considered the practical differences between a communication network and a power network in terms of network structure, physical operation, and dynamic behavior, focusing on analyzing faults occurring on the power grid side. From these studies, it is evident that most scholars have paid less attention to transmission delays caused by traffic overloads in communication networks and the establishment of coupled models that incorporate the operational characteristics of both networks.

1.3. Motivation

In fact, many connected edges often possess redundant capacity. For example, Figure 1a illustrates a communication network with five nodes. The matrix F represents the information flow transmission demand matrix, where elements F_{ij} indicate the information flow

demand that needs to be transmitted from the source to the destination. Each link e_{ij} is associated with its quality attribute q_{ij} [24,25], where the operational level of a link e_{ij} is defined as the ratio of link capacity to link load. Assuming the failure threshold of the link is ρ , if the initial faults in the communication network are links with $\rho < 0.5$, these links will be removed from the original network (e.g., remove $1 \rightarrow 2$, $2 \rightarrow 3$). At this point, the information flow transmission on the communication link is not affected (links $1 \rightarrow 4 \rightarrow 2$ and $2 \rightarrow 1 \rightarrow 3$ still exist), but links $1 \rightarrow 4$ and $2 \rightarrow 1$ are in an overloaded state. The information flow demand on the original link $1 \rightarrow 2$ will be redistributed to the link $1 \rightarrow 4 \rightarrow 2$. Although the network is not immediately affected and the overloaded links do not fail, the transmission quality will continue to decrease. When increasing the threshold to $\rho = 0.7$, the operating efficiency of link $1 \rightarrow 4$ drops below the critical threshold, causing the edge's state to change from overloaded to failed, and it is removed from the original network. At this point, 25 information flow transmission demands are affected (highlighted in red in the figure). When the threshold is further increased to $\rho = 0.9$, links with $q_{ij} < 0.9$ are removed. As shown in Figure 1d, only eleven units of traffic demand can be effectively transmitted to the control center. It can be seen that during the process of changing the threshold and removing links, if the overloaded state and the transmission flow demand of the links are not considered, the network will collapse prematurely, leading to significant losses in the power grid.

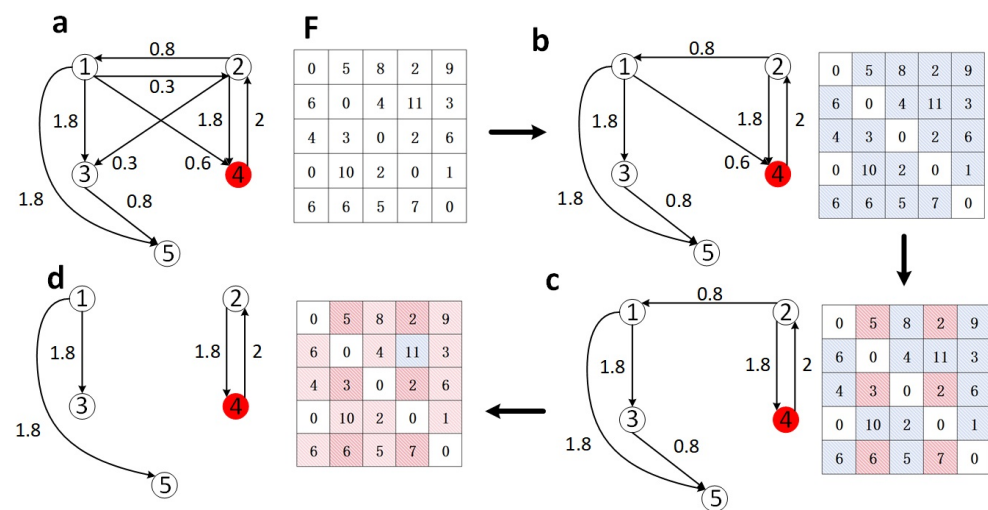


Figure 1. Power communication network diagram of link failure based on information flow demand. (a) Communication network G with size $n = 5$, where node four is the control center and the others are regular transmission nodes. The quality q_{ij} of each line e_{ij} is marked beside the link. The matrix F represents the information flow transmission demand. (b) Assuming the initial faults in the communication network are links with $\rho < 0.5$. (c) Increasing the threshold to $\rho = 0.7$, while removing links with $q_{ij} < 0.7$. (d) When the threshold is further increased to $\rho = 0.9$, links with $q_{ij} < 0.9$ are removed and only eleven units of traffic demand can be effectively transmitted to the control center.

Typically, when an N-1 failure occurs in the power grid, flow convergence must be recomputed for each scenario. If the flow converges, it must be determined whether the flow on each line exceeds its limits; if so, the affected line should be cut. If it does not converge, load shedding or generator output adjustments are typically implemented to balance the power flows. Enumerating all scenarios can be both complex and time-consuming. Therefore, this paper proposes applying line flow betweenness [26] to the load–capacity model of the power system, utilizing it as the power load on the line. This approach effectively reflects and quantifies the role of lines in transmitting power from generators to loads, also considering the impact of the maximum available transmission power between generators and loads on the critical lines. This physical background aligns more closely with

the actual operation of power systems and better reflects their operational characteristics. When modeling the information flow transmission process, distinguishing it from the power network is crucial. Information layer links will not disconnect due to information flow overload but will cause congestion if the flow is excessive. It is necessary to account for the overloaded state when redistributing information flow from non-operational links to neighboring links to develop a more realistic power–communication network flow model. Therefore, this paper, considering link interruptions in the communication system, proposes a load–capacity cascading failure model based on improved percolation theory, integrating information flow overload and power system operational characteristics. This model analyzes the impact of overloaded links on the system’s robustness.

1.4. Contributions

The contributions of this paper are summarized as follows:

- Considering the congestion state of communication network links, a dynamic transmission allocation model for information flow under three link states—normal, overload, and failure—is established. Metrics for communication system topology integrity and operational characteristics are proposed to assess system vulnerability in the event of faults.
- Considering the topology generation characteristics of actual power communication networks, an improved percolation theory is proposed. Communication nodes that are initially outside the largest connected component but have communication links to the control center are considered effective nodes. Power nodes that lose coupling with the communication network but remain self-consistent are also regarded as effective nodes.
- Considering the physical characteristics of coupled networks, the line flow betweenness indicator is utilized to measure the electrical characteristics of line power flows. A load–capacity distribution model based on flow betweenness is proposed for transferring the load of failed lines.

The rest of the paper is organized as follows. In Section 2, we construct the unidirectional dependency model of CPPS and provide a detailed description of the fault propagation process across the space considering communication link overload conditions within the coupled model. In Section 3, we propose two metrics of system robustness assessment to measure the cascading failure results. In Section 4, the numerical simulation is conducted to analyze the cascading failure and presents related discussions. Section 5 concludes the paper.

2. Methods

2.1. Modeling of Power–Communication Coupled Networks Based on Unidirectional Dependency

CPPS includes the modeling of the information network, power network, and coupling layer. The information network comprises the access layer, backbone layer, and core layer. The interdependent edges between power nodes and information nodes form the coupling network [27]. In the coupling network, the power network provides power support for the communication network, while the communication network offers 3C support for the power network. However, since communication nodes are widely equipped with backup power sources, the failure of coupled power nodes does not cause the failure of communication nodes due to power outage. The normal operation of power nodes relies on the monitoring and control of communication nodes. The failure of communication links will result in the control center being unable to receive the fault information of the power system in a timely manner, leading to the failure to promptly deal with power failures and expanding the scope of fault impact. Therefore, this paper primarily studies the model of the power network’s dependence on the information network. Referring to the flowchart in Figure 2, the modeling process is detailed as follows:

- (1) The physical power grid is abstracted as a graph $G_p(V_p, E_p)$ composed of power nodes V_p and transmission lines E_p . The set V_p includes physical equipment in the power grid such as power plants, substations, and loads.
- (2) Divide the power grid into regions [28].
 - a. The partitioning of communities is applied to the division of power network regions. In the power grid, the closer the distance between two buses, the smaller the line reactance and the larger its reciprocal (i.e., higher weight), indicating higher intimacy between the node pair. Thus, such nodes are more likely to be partitioned into the same region. The reciprocal of the line reactance is used as the weight for the non-zero elements of the power network adjacency matrix E .
 - b. Using the Fast Newman method, the modified matrix E from the above steps is substituted for the original matrix E to calculate the modularity Q for the initial partitioning of the power network. The partitioning process must satisfy the following conditions: each region must contain at least one generator and one load; the number of regions must be less than the minimum of the number of generators and loads; and the subregions must achieve power balance.
 - c. To achieve power balance within regions, the system's power flows on the lines are used as weight values based on the Prim algorithm. These weight values are used to determine the flow paths from generators to loads. Regions are then merged according to these paths and combined with the initial partitioning results to form the final zones.
- (3) The number of nodes for each layer is determined: the access layer, backbone layer, and core layer. The access layer nodes are information collection nodes, with the number of communication nodes equal to the number of power nodes; the backbone layer nodes are routing equipment nodes, also considered as control nodes, with the number of nodes equal to the number of power grid partitions; and the core layer nodes are two control nodes representing the main and backup dispatch.
- (4) The modeling of the information network:
 - a. The connection between the power grid and the access layer: according to the abstract diagram of the power grid G_p , access layer nodes are connected in a one-to-one corresponding manner to make the topology diagram of the access layer consistent with the topology diagram of the power grid.
 - b. The connection between the access layer and the backbone layer: the highest-degree nodes in each region of the access layer and the generator nodes are connected to the corresponding nodes in the backbone layer.
 - c. The backbone layer nodes are connected internally according to the connection relationship of the power grid partitions.
 - d. The connection between the access layer and the core layer: calculate the proportion q_i of the generator G_i output to the total system output, and connect it to the main and backup calls with a probability of q_i .
 - e. All routing nodes are connected to the main and backup scheduling center nodes.
 - f. The main and backup scheduling centers are connected.
- (5) Abstract the information network to form G_c .
- (6) Connect the access layer nodes with the power nodes to form unidirectional dependent edges.

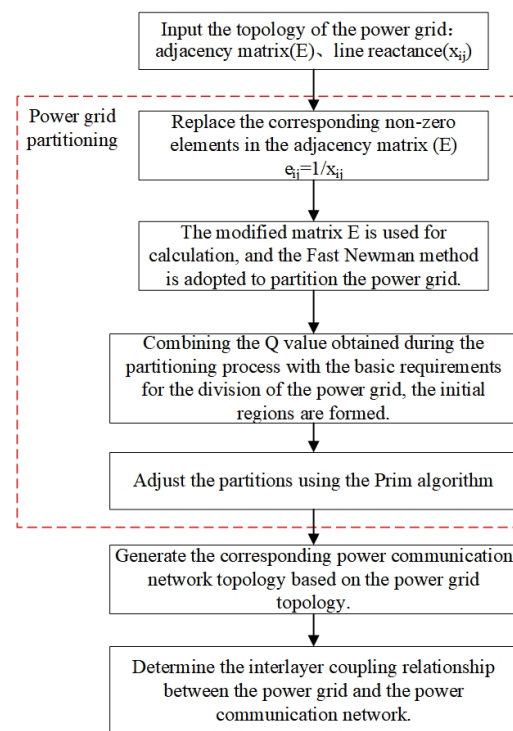


Figure 2. Flowchart of cyber-physical power system modeling.

Thus, the coupled networks are shown in Figure 3.

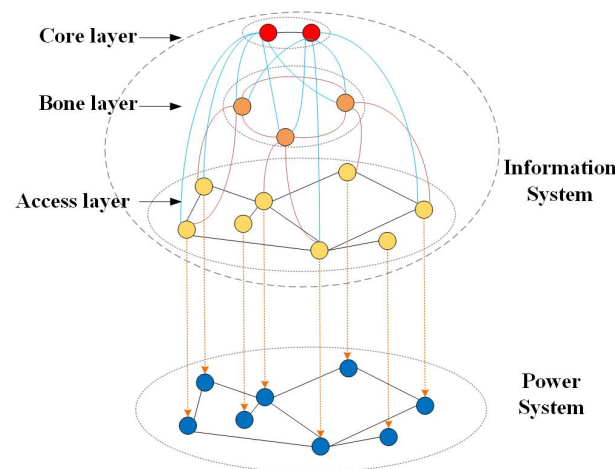


Figure 3. Topology diagram of the power grid dependent on the information network.

2.2. Cascade Failure Model Based on Percolation Theory Considering Communication Link Overloads

2.2.1. Nonlinear Flow Model for Links

The communication network's link information flow model employs a nonlinear capacity-load model that accounts for the overload state [29]. In complex networks, a higher node degree indicates more connections with other nodes. Therefore, the degree values of the endpoints are utilized to calculate the information flow of each access layer link. The higher the degree value of a link, the greater the information flow through it. The information flow ratio of a link is used as the link weight, and the overload coefficient δ describes the edge's capacity to handle additional information flow, as follows:

$$C_{c,ij} = L_{c,ij} + \beta L_{c,ij}^{\alpha} \quad (1)$$

$$C_{c,ij}^{\max} = \delta C_{c,ij} \quad (2)$$

$$W_{c,ij} = \begin{cases} \frac{L_{c,ij}}{C_{c,ij}^{\max}} & e_{ij} \in E_C \\ 0 & e_{ij} \notin E_C \end{cases} \quad (3)$$

where

$$L_{c,ij} = w_{ij} = (k_i k_j)^\theta \quad (4)$$

where $L_{c,ij}$ represents the amount of information transmitted by the link and k_i and k_j denote the degrees of nodes i and j , respectively. θ is a parameter that adjusts the information flow. $C_{c,ij}$ is the capacity of the link, $C_{c,ij}^{\max}$ represents the maximum flow that the line can bear, and $W_{c,ij}$ is the weight of the edge e_{ij} . α and β are capacity coefficients. When $\alpha = 1$, the model is linear.

2.2.2. Improved Percolation Theory

Traditional percolation theory [30] is widely used to describe the structure, function, and resilience of network systems. Percolation models simulate link failure scenarios by gradually removing links from the network. As links are progressively removed, the reduction in the size of the largest connected subgraph can be used to measure the consequences of link failures. Thus, percolation theory is applicable to modeling cascading failures in cyber–physical power systems. However, traditional percolation theory only considers the largest connected subset in a single-layer network when determining the working node subset, without considering other scenarios. Directly applying it to model cascading failures in cyber–physical power systems makes it difficult to accurately simulate the failure process. Considering the information flow transmission characteristics of the information network, where the core layer and backbone layer do not directly correspond to the access layer, and the link status considers the overload situation, it is necessary to improve the classical percolation theory model. The failure model of the cyber–physical power system established in this paper is as follows:

- Communication system. For the links in the access layer, edges with weights greater than the overload coefficient are considered failed. For the information nodes in the access layer, nodes that cannot establish a path to control nodes are considered failed.
- Power system. A power load node must be connected to at least one generator node; otherwise, it is considered failed. Similarly, a generator node must be connected to at least one power load node; otherwise, it is considered failed. Nodes functioning as both generators and loads are considered self-consistent nodes.
- Interaction. Power nodes coupled with failed communication nodes will also fail. Additionally, power nodes coupled with communication nodes exiting transmission delays will fail with a certain probability P_{di} .

2.2.3. Load–Capacity Model of Power Network Based on Flow Betweenness

In previous studies, the shortest path propagation principle has commonly been used to investigate power transmission between buses in a power network. However, in reality, power flow in a power network does not follow only the path with the lowest impedance but rather propagates along all possible paths, adhering to Kirchhoff's Law.

To accurately reflect the role of each transmission line in power propagation and the varying impact of different generator–load pairs on each line, consider that in a given power network, each transmission line carries a varying proportion of transmission power $P(m, n)$ from generator m to load n . Consequently, each line plays a distinct role and has varying levels of significance in transmitting power $P(m, n)$. Since the power transmission paths for generator–load pairs that traverse each line differ, the line's significance within the entire

network is quantified using the flow betweenness index [26]. This index is computed by considering all generator–load pairs utilizing the line. The calculation formula is as follows:

$$F_{Bij} = \sum_{m \in G} \sum_{n \in L} \min(S_m, S_n) \frac{P_{ij,m} P_{ij,n} P_n}{P_{ij} P_{Ln} A_{unm}^{-1} P_{Gm}} \quad (5)$$

where G is the assembly of generation nodes and L is the assembly of consumer nodes. $\min(S_m, S_n)$ is the weight of a single line's flow betweenness, which depends on the minimum value between the actual output of the generator m and the actual load n , reflecting the maximum available transmission power between m and n . $P_{ij,m}$ is the portion of the power flow on line e_{ij} originating from generator m . $P_{ij,n}$ is the portion of the power flow on line e_{ij} directed towards load n . P_n is the node power flow of n . P_{ij} is the active power through line e_{ij} . P_{Ln} is the active load at load node n . A_{unm}^{-1} contains the inverse-order distribution matrix elements. P_{Gm} is the active output of the generator node m .

Therefore, the power load $L_p(ij)$ on edge e_{ij} can be calculated as

$$L_p(ij) = F_{Bij} \quad (6)$$

Considering the capacity of links to handle power loads, we employ the load–capacity model proposed by Motter and Lai [31]. According to this model, the link capacity is directly proportional to its initial power load, as follows:

$$C_p(ij) = (1 + \gamma)L_p(ij) \quad (7)$$

where γ is the tolerance parameter.

2.2.4. Process of Cascading Failure

The information network has the capability to control power nodes. Consequently, faults occurring within the information network can propagate to the interconnected power network. This section details the dynamic process of cascading failures triggered by certain faulty communication links.

Based on the magnitude of information flow transmission in the communication network, the operational states of links are categorized into three types: normal, overloaded, and failed. To analyze cascading failures between coupled networks, some links in the communication network are randomly removed as initial faults. Referring to the flowchart in Figure 4, the detailed dynamic process of cascading failures triggered by specific damaged links is described as follows:

- Step 1: The set of failed links in the access layer communication network due to accidental failures or attacks is denoted as e_{ij} . The information flow on these failed links will be borne by the edges connected to the nodes of the failed links.
- Step 2: The process of distributing information flow on failed branches. This paper utilizes the principle of local redistribution of information flow, with the calculation formula provided as follows.

$$\Delta L_{c,ia} = L_{c,ij} \frac{L_{c,ia}}{\sum_{m \in \Omega_1} L_{c,im} + \sum_{n \in \Omega_2} L_{c,jn}} \quad (8)$$

where $L_{c,ij}$ is the initial information flow on a branch e_{ij} , $L_{c,ia}$ is the initial information flow on a branch e_{ia} , Ω_1 is the set of neighboring nodes of node i , and Ω_2 is the set of neighboring nodes of node j .

- Step 3: The process for determining the overloaded and failed states is as follows.

$$\begin{cases} W_{c,im} > \delta & \text{fail} \\ 1 < W_{c,im} < \delta \text{ and } \text{rand} > p_{im} & \text{overload} \\ 1 < W_{c,im} < \delta \text{ and } \text{rand} \leq p_{im} & \text{fail} \\ W_{c,im} \leq 1 & \text{normal} \end{cases} \quad (9)$$

where $\text{rand} \in (0, 1)$.

Since each branch has different capacities to handle additional information flow, a distribution coefficient ω is introduced to characterize this property.

$$p_{ia} = \left(\frac{W_{c,ia} - 1}{\delta - 1} \right)^\omega \quad (10)$$

- Step 4: Distribution process for information flow on overloaded branches:

$$\Delta_{ak} = (L_{c,ia} - C_{c,ia})T_{ak} \quad (11)$$

$$T_{ak} = \frac{C_{c,ak} - L_{c,ak}}{\sum_{e \in \Omega_i} (C_{c,ie} - L_{c,ie}) + \sum_{f \in \Omega_a} (C_{c,af} - L_{c,af})} \quad (12)$$

where Δ_{ak} is the distribution strategy for the overloaded branch, Ω_i is the set of neighboring nodes of node i with branches in a normal state, and Ω_a is the set of neighboring nodes of the node a with branches in a normal state.

- Step 5: Determine whether there are new failed branches. If new failed branches are detected, proceed to Step 2; otherwise, proceed to Step 6.
- Step 6: Count the sets of failed and overloaded links within the communication network. Update the effective set of communication links, and calculate the transmission delay increments for each communication node. Assess the failure conditions of communication nodes, remove nodes that cannot form a path to the control center, and update the set of effective communication nodes.
- Step 7: Control dependency analysis: Due to the one-to-one coupling between access layer communication nodes and power nodes, the failed communication nodes identified in Step 6 will cause corresponding power nodes to fail through dependent edges. Nodes are selected based on the delay probability of each communication node. If information from these nodes is not transmitted to the control center in a timely manner, their corresponding power nodes are considered failed. Mark the power nodes that have failed in this step.
- Step 8: Physical failure: First, remove the failed nodes in the power network. Next, based on the failure conditions for power system nodes, check if there are additional failed nodes among the remaining nodes and remove them if necessary. Recalculate the power load on the lines; if the redistributed load exceeds the capacity of any line, mark that line as faulty. Repeat this process until no more faulty nodes remain in the power network.
- Step 9: Output: Single cascading failure simulation ends. Output the data for both the power network and the communication network.

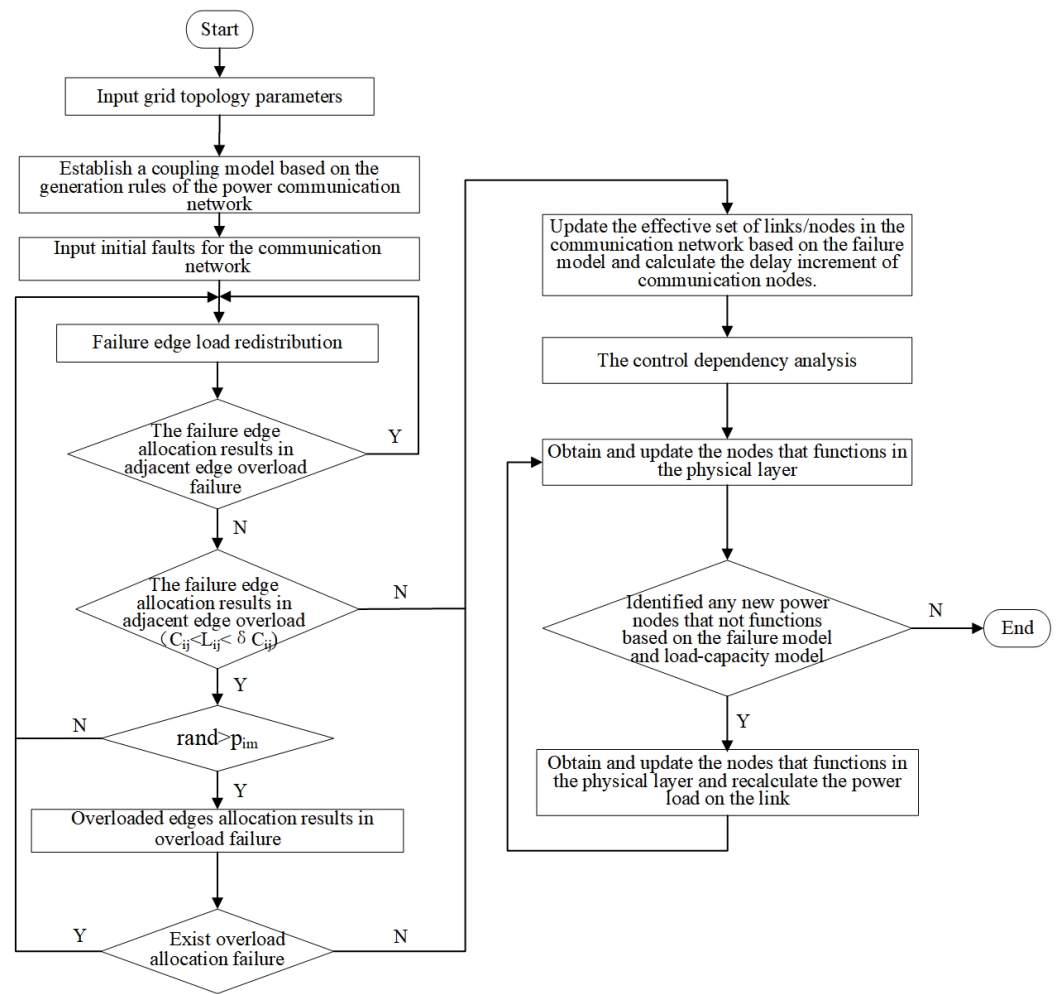


Figure 4. Flowchart of cascading failure process in cyber-physical power systems.

3. Evaluation Metrics of System Robustness to Cascading Failures

In CPPS, any faulty link has the potential to propagate through coupling relationships and evolve into cascading failures. To analyze the impact of initial failures on the system, we define evaluation metrics for both coupled networks based on network topology integrity and operational characteristics.

3.1. Metrics of Communication Network

In the communication network, we employ adjusted node/link survival rates to evaluate the communication network's topology integrity. Considering that communication links in an overloaded state have information flow exceeding their capacity—contrary to normal conditions—these links operate inefficiently and have a certain probability of transitioning to a failed state. Therefore, to distinguish between normal and overloaded links and more accurately represent the impact of the overloaded state on the system, the relative size of the largest connected component G_c is used to evaluate the communication links after adjustment [29]. The survival rate of nodes/links following failure is used to assess the topological integrity, as detailed below:

$$G_c = \frac{\sum_{h \in \Psi} s_h}{N_c} \quad (13)$$

where N_c is the number of nodes in the communication network's access layer. Ψ denotes the set of non-failed nodes. When the information links are in a normal state, $s_h = 1$.

However, when the information links are under overload conditions, s_h is calculated as follows:

$$s_h = \frac{\delta C_h - L_h}{\delta C_h - C_h} \quad (14)$$

Then, the adjusted node/link survival rate is

$$F_c = \frac{1}{2} * (\frac{V'_c}{V_c} + G_c) \quad (15)$$

Due to the disconnection of information links, the path from the access layer nodes of the communication network to the control center may change, resulting in communication delays. In this paper, the data communication delay is simplified and calculated as follows [32]: Data transmission in the communication network follows the shortest path principle, and each time it passes through a data node, the delay increases by one time unit τ . The delay time unit reflects the delay caused by data transmission and processing from the source node to the destination node in the communication network, including passing through each information node and the communication path to the next information node. Therefore, the transmission delay increment T caused by the communication network is calculated as follows:

$$T = \sum_{k \in L_c} T'_{\pi_c} + \sum_{k \in L_c} T_{\pi_c} \quad (16)$$

where T'_{π_c} and T_{π_c} are the delay of the transmission path of the same source–destination pairs after and before the cascading failure. L_c denotes the set of the shortest transmission paths for all source–destination pairs in the communication network.

3.2. Metrics of Power Network

In the physical power network, we use failure impact F_p to evaluate the influence of cascading failure [12], expressed as

$$F_p = \frac{1}{2} * (\frac{V'_p}{V_p} + \frac{E'_p}{E_p}) \quad (17)$$

where V'_p and E'_p , respectively, are the number of failed nodes and links in the power network. V_p and E_p , respectively, are the total number of nodes and links in the physical power network.

4. Case Study and Discussion

In this section, taking the IEEE 39-bus system as an example, the power network topology is shown in Figure 5 and the original topology is divided into four regions based on zoning principles. Correspondingly, the power communication network, generated according to the aforementioned rules, is depicted in Figure 6. In this network, the access layer consists of 39 communication nodes, each corresponding to one of the 39 power nodes, which are used for uploading fault information and issuing dispatch instructions. The backbone layer includes four control nodes, each corresponding to its respective access layer region. The dispatch center is equipped with two control nodes.

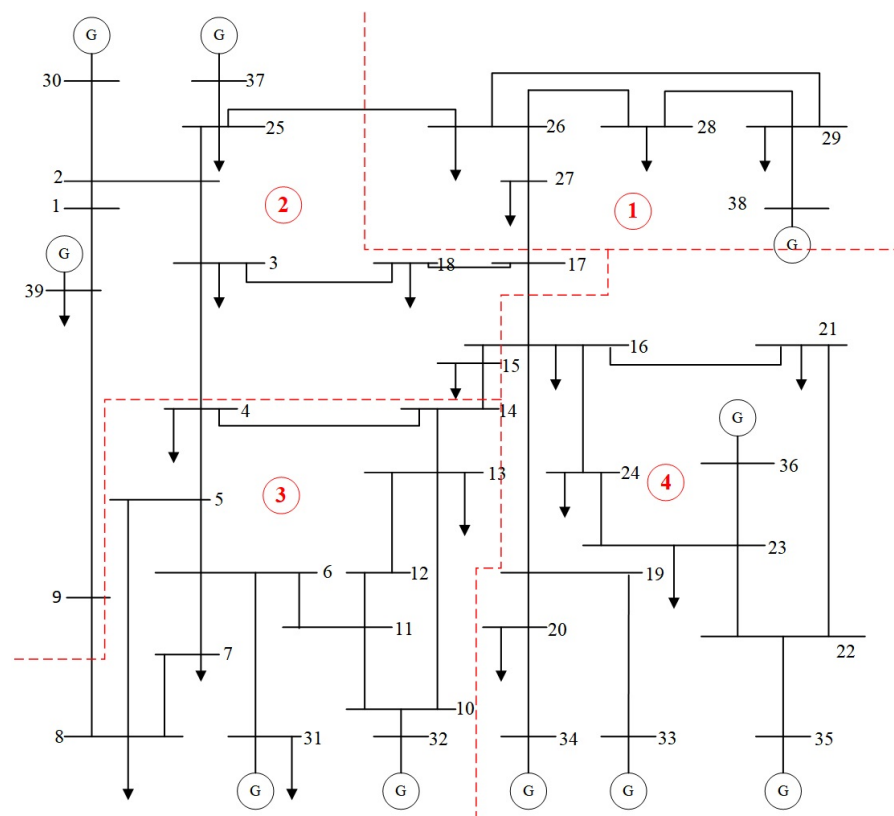


Figure 5. Partition diagram of IEEE 39-bus system.

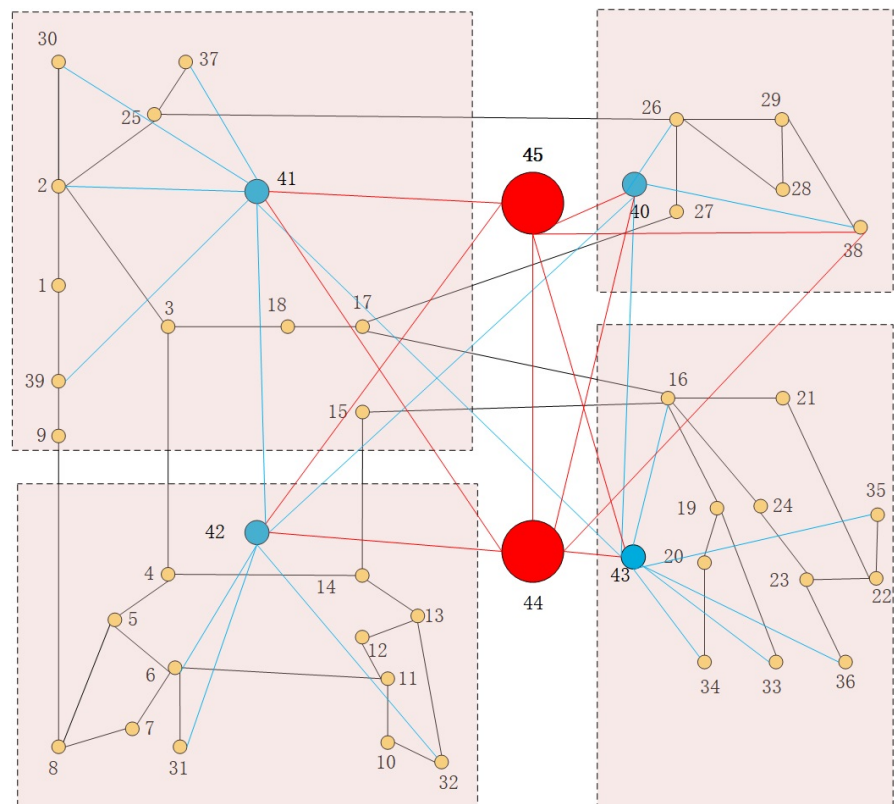


Figure 6. Topology diagram of information network generated by IEEE 39-bus system.

4.1. Impact of Overload Coefficient

To explore the impact of the overload coefficient on the robustness of the network, the number of initial link faults was varied, with each set of faulty links generated randomly. The simulations were independently run 50 times, and the average value was taken as the communication network metric. For clarity of presentation in charts, textual descriptions were used when the communication system completely failed, and the data set with the highest number of failed links that caused the complete failure of the communication system is selected for textual explanation. According to Figure 7a, as the number of initial faulty links increases, the survival rate of nodes/links in the communication network gradually decreases. When the overload capacity of links is not considered, the survival rate of nodes/links in the network is the lowest. When the overload coefficient is 1.2, the survival rate of nodes/links in the communication network significantly improves. However, it can be observed that when the overload coefficients are 1.3 and 1.5, the survival rate of nodes/links does not improve significantly.

Figure 7b shows that the CPPS under different overload coefficients exhibits a first-order percolation transition, with a similar overall trend. As the number of failed lines increases, the topology of the information layer is disrupted, and some nodes lose their data transmission paths. Changing the transmission path increases the system delay. When the overload coefficient is 1.5, the number of failed links that the communication network can withstand before complete collapse is the highest. As seen in Figure 7b and Table 1, there is a threshold for the initial number of failed links, near which the cascading failure effect expands to all communication links, leaving no transmission path between communication nodes and the control center. At this point, the communication system completely fails, making it impossible to control the power grid. Table 1 shows the specific thresholds for different overload coefficients.

Therefore, considering network construction costs, the overload coefficient is set to 1.3 according to Figure 7 and Table 1.

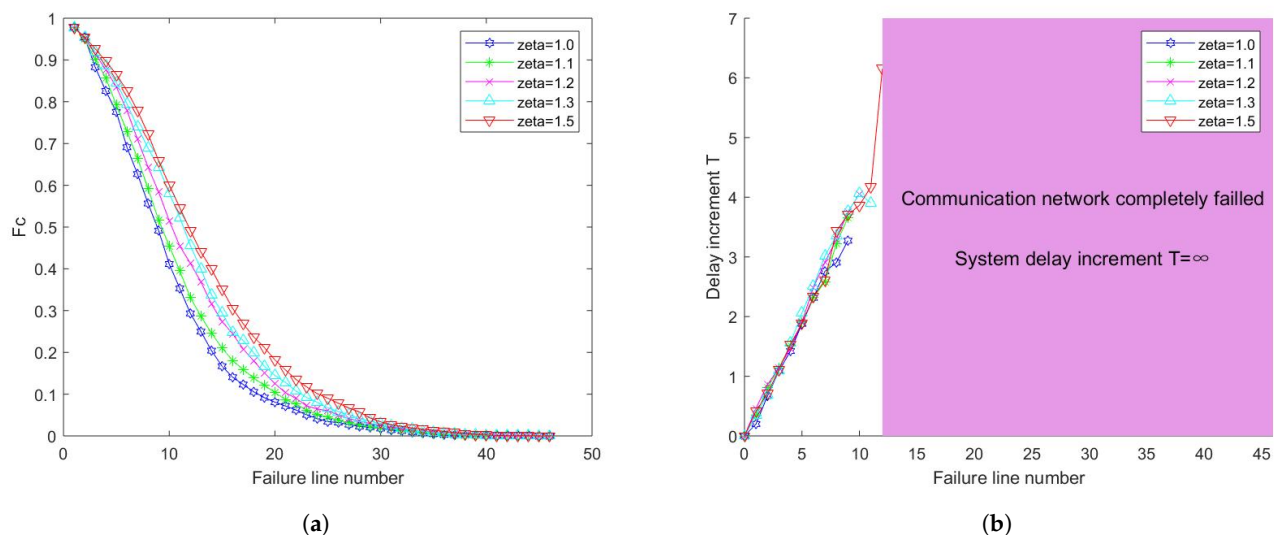


Figure 7. The robustness of the communication network and the increment in communication delay under different overload coefficients. (a,b) respectively show the relationship between the robustness of the communication network and the system delay with the increase in the number of communication link failures under different overload coefficients, while other parameters remain constant.

Table 1. The thresholds of the system under different overload coefficients.

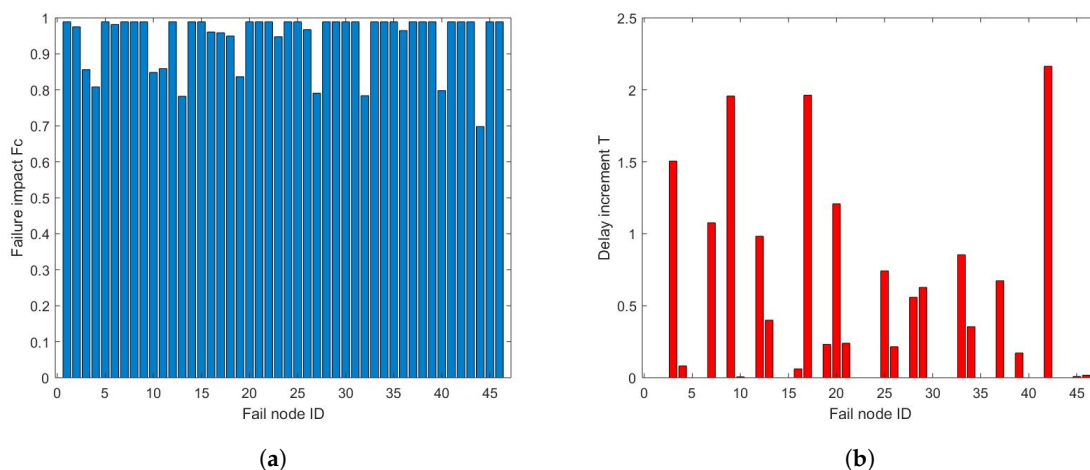
Overload Coefficient	The Threshold of Initial Failed Lines	Threshold Percentage %
1.0	9	19.56
1.1	9	19.56
1.2	10	21.74
1.3	11	23.91
1.5	12	26.09

4.2. Impact of Failed Links

In this section, we will analyze the impact on data transmission within the power and communication networks by sequentially removing each communication network link.

As shown in Figure 8, most of the faulty communication links have varying impacts on the topological integrity and operational characteristics of the CPPS. Links that cause significant system disruption are identified as critical links. Under N-1 fault conditions, all possible scenarios of system attacks are enumerated.

As shown in Figure 8, it can be observed that the failure of a single communication link can reduce the node and link survival rate in the communication network to as low as 69.69%, induce a system delay increment of 2.1635, and cause a 35.07% paralysis in the nodes and links of the power network. It is also noted that some link failures do not affect the rest of the communication and power networks beyond the faulty link. This is because, in cascading failures, the communication network considers the congested state of the links, redistributing the traffic on failed and overloaded links. Moreover, overloaded links can sustain operation for a short period before failing, thereby enhancing the system's robustness to some extent. Furthermore, the communication link that causes the maximum delay increment may not necessarily result in the lowest node/link survival rate in the communication network or the highest failure rate in the power network nodes/links. However, the failure rates of nodes/links in the communication and power networks are notably similar. For example, when link 42 fails, the highest delay increment of 2.1635 occurs. At this point, the survival rate of communication nodes/links is 98.91%, and the failure rate of power nodes/links is 3.46%. This is because the failure of link 42 changes the path from communication node 27 to the control center, from the original path 27→26→40→44 to 27→17→16→43→44, resulting in communication delay. The failure rate of communication node 27 is 36.06%. However, removing link 42 does not cause failure or overload in other links, so there are 45 operational links, and the number of effective communication nodes remains unchanged compared to before the fault. Due to the coupling relationship, the failure rate of power node 27 is also 36.06%, ultimately leading to the failure of power node 27.

**Figure 8.** Cont.

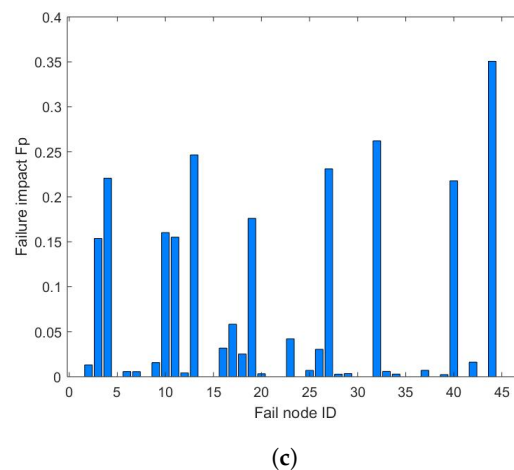


Figure 8. The impact of initial faults on the cyber–physical system. (a,b) show the impact of each communication link failure on the robustness and delay increment of the communication system, while (c) shows the impact of each communication link failure on the physical power grid.

4.3. Impact of Attack Strategies

The previous section analyzed the N-1 impact caused by the failure of a single communication link. As the number of faulty lines increases, different initial sets of faulty lines will have varying effects on the system. Therefore, based on structural and electrical characteristics, we employ both random line attack and critical line attack to remove communication network links one by one, analyzing the impact of different attack strategies on power and communication network data transmission.

The critical line attack strategy is derived from the initial power betweenness centrality importance ranking of the power network. Due to the uncertainty of the random line attack strategy, each faulty line in the random attack strategy is randomly generated, and the results are averaged after 50 independent runs.

As shown in Figure 9, compared to random attacks, the CPPS exhibits high vulnerability under attacks on critical lines. Under critical line attacks, even with the prior consideration of information flow redistribution due to link overload, the network still suffers significant damage. This is because the failure of critical lines disrupts the paths that transmit information to the control center, preventing the upload of power fault information. Consequently, the control center cannot respond, and the source nodes transmitting information in the communication network will cause the failure of coupled power nodes, thus expanding the fault scale and accelerating the propagation of cascading failures and system collapse.

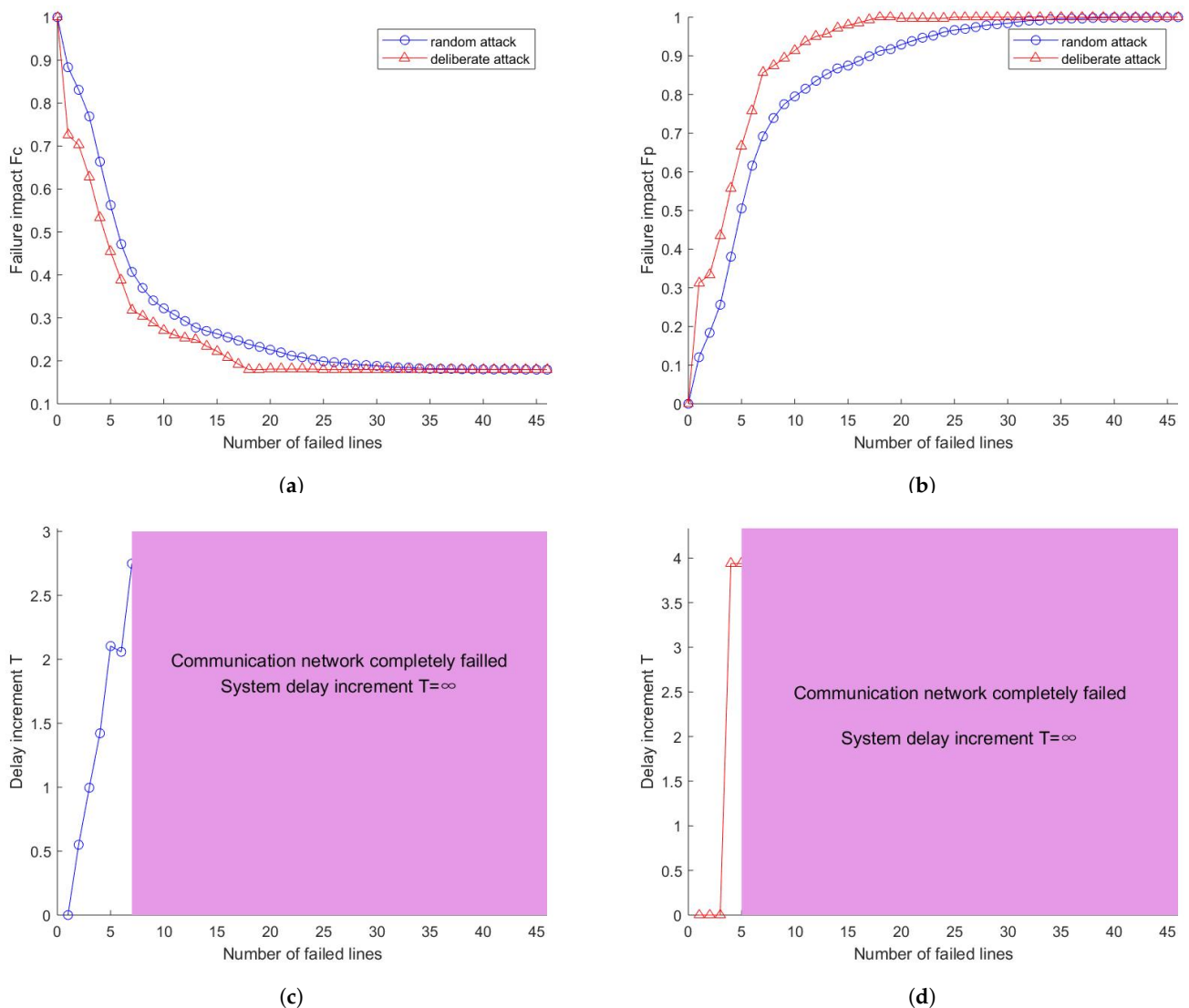


Figure 9. Impact of attack strategies on cyber-physical system. (a–d) illustrate the relationship between the evaluation metrics of the coupled network and the number of failed communication links under two different attack strategies (random attack and deliberate attack). Specifically, (a) shows the relationship between the survival rate of nodes/links in the power communication network and the number of failed communication links, (b) shows the relationship between the failure rate of nodes/links in the power communication network and the number of failed communication links. (c,d) respectively depict the trend of delay increment in the system under random attack and deliberate attack.

5. Conclusions

This paper investigates the dynamic propagation of cascading failures in CPPS. First, the coupling relationship between the communication network and the physical power network is analyzed, and the corresponding communication system's topology structure is generated based on the power network. Next, an overload distribution model for information flow is established within the communication network to address overloads resulting from failures. In the power network, a load–capacity distribution model based on power flow betweenness is established to handle the complexity of power flow calculations due to failures. To more accurately describe the node/line failures caused by power flow transfers due to faults, traditional percolation theory is improved to establish a failure propagation model for coupled networks.

Overall, this paper comprehensively considers both the electrical characteristics of the physical power grid and the information transmission characteristics of the power communication network when establishing the coupling model. It improves the coupled network model from both the topological structure and functional characteristics and constructs a cascading failure model that more accurately reflects real-world scenarios. Most existing studies are based on percolation theory and only analyze the cascading failure process of CPPS from the perspective of network topological integrity. This approach fails to realistically capture islanding phenomena in power system operations, thus necessitating an enhancement of percolation theory.

The simulations analyze the impact of faulty lines on the overload capacity of communication network links, data transmission, network survivability, and physical power network fault rates. The results indicate that even a small increase in link capacity can significantly enhance network robustness. Additionally, the system performance degrades when links at critical topological positions in the communication network are attacked, leading to increased system delay increments compared to random attacks and causing the information layer network to collapse earlier.

In summary, these findings offer valuable insights for future power network planning. However, these studies are based on post-fault conditions, considering only the interactions between nodes as either normal or complete failure to achieve power flow dispatch by the control center. In reality, the interaction process between power nodes and information nodes is extremely complex and often only qualitatively analyzed. Moreover, compared to power flow dispatch, scheduling information flow is relatively simple. Reducing the occurrence of faults from the source of the cyber side is a more efficient and reliable solution instead of establishing a cascading failure resistance mechanism on the power grid side. Therefore, our future research will focus on allocating critical information flows to reliable paths under conditions of communication link overload to ensure accessibility and reduce the probability of cascading failures caused by communication interruptions.

Author Contributions: Conceptualization, X.L. and Y.L.; Methodology, X.L. and Y.L.; Writing—original draft, X.L.; Writing—review and editing, Y.L. and T.X. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China under Grant 62062068 and Young Academic and Technical Leaders Program of Yunnan Province under Grant 202305AC160077.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Acknowledgments: Thanks for the help of Kunming AI Computing Center.

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

Abbreviations and Nomenclature

CPPS	Cyber–physical power system;
E_{ij}	Information flow demand on link e_{ij} ;
q_{ij}	The ratio of link capacity to link load;
ρ	The failure threshold of the link;
V_p	The sets of power nodes;
E_p	The sets of power transmission lines;
Q	The modularity value of the combined union of two communities;
q_i	The proportion of the generator i output to the total system output;
δ	The link's capacity to handle additional information flow;
k_i	The degrees of node i ;
θ	The parameter that adjusts the information flow;
$L_{c,ij}$	The amount of information transmitted by the link e_{ij} ;
$C_{c,ij}$	The capacity of the link e_{ij} ;

$C_{c,ij}^{\max}$	The maximum flow that the link e_{ij} can bear;
$W_{c,ij}$	The weight of the link e_{ij} ;
α	The capacity coefficient;
β	The capacity coefficient;
$\min(S_m, S_n)$	The weight of a single line's flow betweenness;
$P_{ij,m}$	The portion of the power flow on line e_{ij} originating from generator m ;
$P_{ij,n}$	The portion of the power flow on line e_{ij} directed towards load n ;
P_{ij}	The active power through line e_{ij} ;
P_{Ln}	The active load at load node n ;
A_{unm}^{-1}	The inverse-order distribution matrix elements;
P_{Gm}	The active output of the generator node m ;
F_{Bij}	The flow betweenness of edge e_{ij} in the power network;
$L_p(ij)$	The power load on edge e_{ij} in the power network;
$C_p(ij)$	The capacity of edge e_{ij} in the power network;
γ	The tolerance parameter;
Δ_{ak}	The distribution strategy for the overloaded branch;
F_c	The adjusted node/link survival rate following failure in the communication network;
T	The transmission delay increment;
F_p	The failed node/link rate following failure in the power network.

References

- Abdelmalak, M.; Venkataramanan, V.; Macwan, R. A survey of cyber-physical power system modeling methods for future energy systems. *IEEE Access* **2022**, *10*, 99875–99896. [\[CrossRef\]](#)
- Li, Y.; Wang, B.; Wang, H.; Ma, F.; Ma, H.; Zhang, J.; Zhang, Y.; Mohamed, M.A. An Effective Node-to-Edge Interdependent Network and Vulnerability Analysis for Digital Coupled Power Grids. *Int. Trans. Electr. Energy Syst.* **2022**, *2022*, 5820126. [\[CrossRef\]](#)
- Gao, X.; Peng, M.; Chi, K.T.; Zhang, H. A stochastic model of cascading failure dynamics in cyber-physical power systems. *IEEE Syst. J.* **2020**, *14*, 4626–4637. [\[CrossRef\]](#)
- Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Trans. Power Syst.* **2016**, *32*, 3317–3318. [\[CrossRef\]](#)
- Zhao, Q.; Qi, X.; Hua, M.; Liu, J.; Tian, H. Review of the recent blackouts and the enlightenment. In Proceedings of the CIRED 2020 Berlin Workshop (CIRED 2020), Online Conference, 22–23 September 2020; IET: Stevenage, UK, 2020; Volume 2020; pp. 312–314.
- Wu, J.; Chen, Z.; Zhang, Y.; Xia, Y.; Chen, X. Sequential recovery of complex networks suffering from cascading failure blackouts. *IEEE Trans. Netw. Sci. Eng.* **2020**, *7*, 2997–3007. [\[CrossRef\]](#)
- Peng, C.; Wu, J.; Tian, E. Stochastic event-triggered H_∞ control for networked systems under denial of service attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *52*, 4200–4210. [\[CrossRef\]](#)
- Hu, S.; Yue, D.; Han, Q.L.; Xie, X.; Chen, X.; Dou, C. Observer-Based Event-Triggered Control for Networked Linear Systems Subject to Denial-of-Service Attacks. *IEEE Trans. Cybern.* **2020**, *50*, 1952–1964. [\[CrossRef\]](#)
- Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **2010**, *464*, 1025–1028. [\[CrossRef\]](#)
- Huang, X.; Gao, J.; Buldyrev, S.V.; Havlin, S.; Stanley, H.E. Robustness of interdependent networks under targeted attack. *Phys. Rev. E—Stat. Nonlinear Soft Matter Phys.* **2011**, *83*, 065101. [\[CrossRef\]](#) [\[PubMed\]](#)
- Cao, Y.Y.; Liu, R.R.; Jia, C.X.; Wang, B.H. Percolation in multilayer complex networks with connectivity and interdependency topological structures. *Commun. Nonlinear Sci. Numer. Simul.* **2021**, *92*, 105492. [\[CrossRef\]](#)
- Chen, L.; Yue, D.; Dou, C.; Cheng, Z.; Chen, J. Robustness of cyber-physical power systems in cascading failure: Survival of interdependent clusters. *Int. J. Electr. Power Energy Syst.* **2020**, *114*, 105374. [\[CrossRef\]](#)
- Pan, H.; Li, X.; Na, C.; Cao, R. Modeling and analysis of cascading failures in cyber-physical power systems under different coupling strategies. *IEEE Access* **2022**, *10*, 108684–108696. [\[CrossRef\]](#)
- Jianfeng, D.; Jian, Q.; Jing, W.; Xuesong, W. A vulnerability assessment method of cyber physical power system considering power-grid infrastructures failure. In Proceedings of the 2019 IEEE Sustainable Power and Energy Conference (iSPEC), Beijing, China, 21–23 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1492–1496.
- Tian, M.; Dong, Z.; Gong, L.; Wang, X. Line hardening strategies for resilient power systems considering cyber-topology interdependence. *Reliab. Eng. Syst. Saf.* **2024**, *241*, 109644. [\[CrossRef\]](#)
- Chen, L.; Yue, D.; Dou, C.; Xie, X.; Li, S.; Zhao, N.; Zhang, T. Impact of cascading failure on power distribution and data transmission in cyber-physical power systems. *IEEE Trans. Netw. Sci. Eng.* **2023**, *11*, 1580–1590. [\[CrossRef\]](#)
- Zhong, J.; Zhang, F.; Yang, S.; Li, D. Restoration of interdependent network against cascading overload failure. *Phys. A Stat. Mech. Its Appl.* **2019**, *514*, 884–891. [\[CrossRef\]](#)

18. Ding, D.; Wu, H.; Yu, X.; Wang, H.; Yang, L.; Wang, H.; Kong, X.; Liu, Q.; Lu, Z. Vulnerability Assessment of Cyber Physical Power System Based on Improved Cascading Failure Model. *J. Electr. Eng. Technol.* **2024**, 1–12. [\[CrossRef\]](#)
19. Wang, S.; Gu, X.; Chen, J.; Chen, C.; Huang, X. Robustness improvement strategy of cyber-physical systems with weak interdependency. *Reliab. Eng. Syst. Saf.* **2023**, 229, 108837. [\[CrossRef\]](#)
20. Ghasemi, A.; de Meer, H. Robustness of interdependent power grid and communication networks to cascading failures. *IEEE Trans. Netw. Sci. Eng.* **2023**, 10, 1919–1930. [\[CrossRef\]](#)
21. Cao, R.; Dong, X.; Wang, B.; Liu, K. Discussion of protection and cascading outages from the viewpoint of communication. In Proceedings of the 2011 International Conference on Advanced Power System Automation and Protection, Beijing, China, 16–20 October 2011; IEEE: Piscataway, NJ, USA, 2011; Volume 3, pp. 2430–2437.
22. Zhang, G.; Shi, J.; Huang, S.; Wang, J.; Jiang, H. A cascading failure model considering operation characteristics of the communication layer. *IEEE Access* **2021**, 9, 9493–9504. [\[CrossRef\]](#)
23. Gao, X.; Peng, M.; Chi, K.T. Robustness analysis of cyber-coupled power systems with considerations of interdependence of structures, operations and dynamic behaviors. *Phys. A Stat. Mech. Its Appl.* **2022**, 596, 127215. [\[CrossRef\]](#)
24. Wang, F.; Li, D.; Xu, X.; Wu, R.; Havlin, S. Percolation properties in a traffic model. *Europhys. Lett.* **2015**, 112, 38001. [\[CrossRef\]](#)
25. Saberli, M.; Hamedmoghadam, H.; Ashfaq, M.; Hosseini, S.A.; Gu, Z.; Shafiei, S.; Nair, D.J.; Dixit, V.; Gardner, L.; Waller, S.T.; et al. A simple contagion process describes spreading of traffic jams in urban networks. *Nat. Commun.* **2020**, 11, 1616. [\[CrossRef\]](#)
26. Liu, W.; Liang, C.; Xu, P.; Dan, Y.; Wang, J.; Wang, W. Identification of critical line in power systems based on flow betweenness. *Proc. CSEE* **2013**, 33, 90–98.
27. Wang, T.; Sun, C.; Gu, X.; Qin, X. Modeling and vulnerability analysis of electric power communication coupled network. *Proc. CSEE* **2018**, 38, 3556–3567.
28. Newman, M.E. Finding community structure in networks using the eigenvectors of matrices. *Phys. Rev. E—Stat. Nonlinear Soft Matter Phys.* **2006**, 74, 036104. [\[CrossRef\]](#)
29. Chen, C.Y.; Zhao, Y.; Gao, J.; Stanley, H.E. Nonlinear model of cascade failure in weighted complex networks considering overloaded edges. *Sci. Rep.* **2020**, 10, 13428. [\[CrossRef\]](#)
30. Stauffer, D.; Aharony, A. *Introduction to Percolation Theory*; Taylor & Francis: Abingdon, UK, 2018.
31. Motter, A.E.; Lai, Y.C. Cascade-based attacks on complex networks. *Phys. Rev. E* **2002**, 66, 065102. [\[CrossRef\]](#)
32. Han, Y.; Guo, C.; Zhu, B.; Xu, L. Model cascading failures in cyber physical power system based on improved percolation theory. *Autom. Electr. Power Syst.* **2016**, 40, 30–37.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.