Hindawi
Mathematical Problems in Engineering
Volume 2019, Article ID 2817586, 15 pages
https://doi.org/10.1155/2019/2817586

Research Article

Survivability Evaluation Method for Cascading Failure of Electric Cyber Physical System Considering Load Optimal Allocation

Zhaoyang Qu,[1,2] **Yunchang Dong**,[3] **Nan Qu**,[4] **Lei Wang**,[1] **Yang Li**,[5,6] **Yu Zhang**,[1] **and Sylvere Mugemanyi**[1]

[1]*College of Information Engineering, Northeast Electric Power University, Jilin 132012, China*
[2]*Jilin Engineering Technology Research Center of Intelligent Electric Power Big Data Processing, Jilin 132012, China*
[3]*NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106, China*
[4]*Maintenance Company of Jiangsu Power Company, Nanjing 210000, China*
[5]*School of Electrical Engineering, Northeast Electric Power University, Jilin 132012, China*
[6]*Energy Systems Division, Argonne National Laboratory, IL 60439, USA*

Correspondence should be addressed to Yunchang Dong; 595245700@qq.com

Received 8 May 2019; Accepted 23 June 2019; Published 15 July 2019

Academic Editor: Ricardo Aguilar-Lopez

The scale of the electric cyber physical system (ECPS) is continuously extending, and the existing cascade failure models ignore both the information flow and power flow transferring characteristics and also lack effective survivability analysis. In this paper, the quantitative evaluation method for cascading failure of ECPS survivability considering optimal load allocation is proposed. Firstly, according to the system topological structure and correlation, the degree-betweenness weighted correlation matrix of ECPS is established by defining the degree function as well as the electric betweenness, and the formal representation of coupled ECPS network model is realized. Secondly, based on the structural connectivity change and risk propagation range of ECPS cascade failure, the survivability evaluation model is designed by taking into account the constraints such as node load capacity limitation, information flow optimal allocation strategy, power flow optimization equation, and system safety operation. Finally, the firefly algorithm with chaotic Lévy flight is proposed to solve the evaluation model efficiently. The case study vividly shows that the evaluation method can effectively quantify the survivability of ECPS and thus enhance the evaluation efficiency of large-scale coupled systems.

1. Introduction

With the rapid development of the energy Internet and smart grid, the power system has gradually evolved into a complex multidimensional and heterogeneous electric power cyber physical fusion system with deep coupling of cyber and physical systems [1–3]. Due to the large-scale integration of uncertain renewable generations [4] and new power electronics such as VSC-HVDC [5], the uncertainty of the electric cyber physical systems has greatly increased. The interaction between the information flow and the energy flow in the coupled system is frequently increased, and thus the ECPS network security risk is also increased while improving the power grid perception, computing, communication, and control capabilities. When the cyber system is attacked, it may cause the physical system components to malfunction or refuse to function. Simultaneously, the failure of the physical system will affect the observability and controllability of the cyber system, induce the cascade failure of the dual network, expand the scope of the security incident, and significantly reduce the survivability of the coupled system [6–8]. When a node or line in electric physical system is severely attacked, the relay protection device will act to cause the power flow to shift. When the system cannot achieve a stable state through the power flow calculation, some nodes of the physical system will fail. Since the working physical

node can provide energy supply for the cyber node, the cyber node coupled with the failed physical node will fail due to loss of energy supply, and the cascade failure occurs [9–11]. ECPS survivability refers to, when the coupled system is subjected to random disturbances or deliberate attacks, the ability of the system to maintain its original topological structure and operating state [12, 13]. Therefore, when the coupled system is subjected to disturbance or attack, it is important to reveal the inherent vulnerability and disturbance immunity of the system to quickly and effectively evaluate the survivability of the ECPS.

To date, scholars have carried out numerous researches related to the survivability evaluation of ECPS. Literature [14–16] constructs an ECPS network model from the perspective of a dependent network, evaluates the structural connectivity vulnerability of the coupled system, and proposes a corresponding protection strategy. In [17–19], the authors simulate the dynamic cascading failure effect of cyber physical double-layer network based on seepage theory and analyze the vulnerability of ECPS under different coupling strategies. Literature [20–22] constructs a cascade failure model for ECPS-dependent network risk propagation, evaluates the robustness of coupled systems subjected to random attacks, and compares network robustness and node thresholds under different connection strengths. Based on the power flow optimization model, the effects of different cyber network topological structure, cyber edge fault scales, and edge failure modes on power system vulnerability are studied in [23–25]. Literature [26, 27] presents an ECPS risk evaluation model based on game theory from the perspective of both offensive and defensive sides and assesses the harm of network attacks to small-scale ECPS. Literature [28] presents a new model to reformulate the microgrid formulation problem in resilient distribution networks. Literature [29] proposes a novel load restoration optimization model to coordinate topology reconfiguration and microgrid while satisfying a variety of operational constraints, which exploits benefits of operational flexibility provided by grid modernization to enable more critical load pickup. Literature [30] presents a bilevel optimization model for the risk assessment of transmission systems, and the lower level model is expected to provide a generation redispatch by minimizing the total load shedding, and the upper-level model is to maximize the severity risk by constructing a binary optimization model to identify the worst *N-k* contingency.

To sum up, the existing ECPS survivability evaluation methods are mainly based on the dependent network, the seepage theory, the power flow optimization cascade failure model, and the game theory to analyze the vulnerability and robustness of the ECPS network. These aforementioned researches exhibit significant limitations: (1) Structural vulnerability and robustness analysis based on dependent network and seepage theory ignores the difference in properties of cyber nodes and physical nodes (power generation nodes, contact nodes, and load nodes) and also simplifies the cascade failure process into direct node dependence failure. The actual ECPS node has load capacity; the failure node load will be redistributed and will fail when the load exceeds the capacity. Therefore, this simplification will render the evaluation results. (2) The cascading failure model based on power flow optimization focuses on physical network power flow optimization, without considering communication optimal routing and information flow optimization process, and hence it is difficult to truly reflect the survivability change of ECPS failure dynamic process. (3) The ECPS vulnerability evaluation based on game theory is mainly applicable to small-scale case systems. Nowadays, the system of cyber physical fusion is larger and the operation constraints are numerous and complex. For this reason, it is necessary to introduce an efficient intelligent solution algorithm to improve the evaluation efficiency of large-scale ECPS.

Based on the topological structure analysis, this paper firstly formalizes the coupled ECPS by constructing the degree-betweenness ECPS correlation matrix. It also considers the multiconstraint conditions of the ECPS cascade failure load optimization allocation strategy; thereafter a survivability evaluation model for comprehensive structure and state is designed based on the optimal target of load shedding. Finally, the chaotic Lévy flight firefly algorithm is proposed to solve the model.

2. Mathematical Model and Method

2.1. Weighted ECPS Network Model. The ECPS network consists of three parts: the physical network, the cyber network, and the internetwork connection lines [30, 31]. Based on the graph theory, a weighted degree-betweenness matrix is used to formally characterize the coupled system in accordance with the dual-network topological structure and the network connection relationship. The simplified schematic diagram of ECPS network is shown in Figure 1.

The actual power cyber network structure is mostly a star network structure. The experimental data indicate that the node degree allocation of the star network structure is characterized by a power-law allocation without scale-free network [32], so the Barabási-Albert (BA) model with scale of M nodes without scale-free network is a cyber network. Because the dispatching center receives the collected information and issues the irreplaceability of the control command, the node with the largest degree of cyber network is selected as the scheduling center, the other two nodes are selected as the transmitting node, and the remaining M-3 nodes are randomly selected and connected with transmitted nodes. The new j_{th} node is connected to node i with the probability of $p(k_i)$ [32]:

$$p(k_i) = \frac{k_i}{\sum_i k_i} \tag{1}$$

where k_i is the degree of the node i.

According to this rule, it stops the growth to the network size of M nodes.

The cyber system corresponding to the dispatch center and each plant station is abstracted as a cyber node, and the fiber link of the cyber transmission is an edge, ignoring the multiple edges, self-loop, and directionality of the link [33]. The cyber network can be represented as a sparse undirected

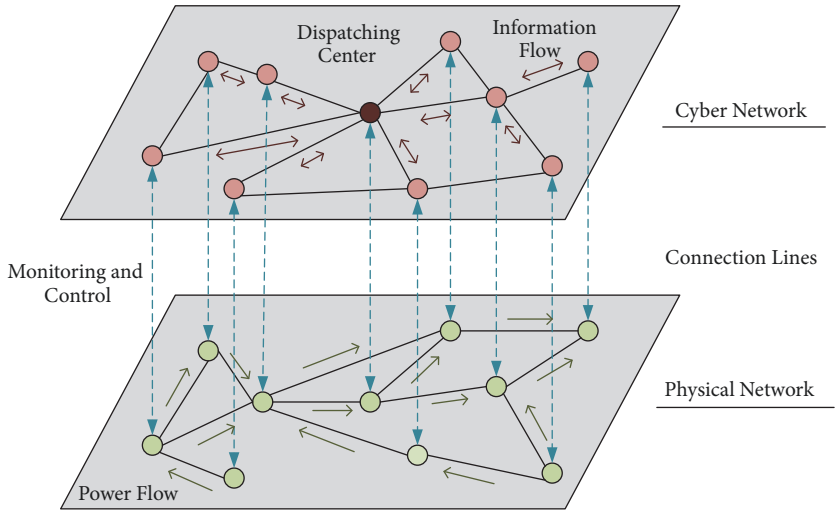


Figure 1: Simplified schematic diagram of ECPS network.

topological structure of m cyber nodes and n communication links: $G_c=(V_c, E_c, \mu)$, node set $V_c = \{v_{c1}, v_{c2} \ldots, v_{cm}\}$, link set $E_c = \{e_{c1}, e_{c2} \ldots, e_{cn}\}$, and μ is the link weight. The edge weight is defined as the degree function that connects the two nodes to the edge:

$$\mu = \left(k_i k_j\right)^{\sigma} \tag{2}$$

where k_j is the degree of the node j, and σ is the weight coefficient ($0 \le \sigma \le 1$). The weight coefficient σ determines the difference of the edges in the cyber network and also determines the weighting of the network. The larger the σ, the larger the difference between the edges. When σ=0, the weights of all edges are μ=1. There is no difference between the edges, and the cyber network belongs to the unprivileged network; the μ can be regarded as an exponential function about σ. When $\sigma \neq 0$ and σ changes from 0 to 1, the μ will change exponentially, and the larger the σ, the greater the difference of the edges; that is, the difference between the edges is changed by changing the coefficient σ, and the weight of the edges is realized by the change of the coefficients. According to the literature [34–36], in general, when the weight coefficient is close to 0, that is, when the edge difference is small, the network survivability is high, and the weight coefficient can be adjusted in conformity with the specific production demand in the actual cyber system. In the simulation of this paper, the weight coefficient σ is smaller. k_i is the degree of the node i, and k_j is the degree of the node j.

The physical system is based on the IEEE118 standard model, which abstracts power plants, substations, and loads into power generation, liaison, and load nodes [37]; the transmission lines between nodes are abstracted as edges, regardless of multiloop transmission, and different nodes are distinguished. Based on the difference in nature and the direction of transmission, the transmission edge set is directed. The physical network topological structure can be represented as a graph: $G_p=(V_p, E_p, u)$, m node sets $V_p = \{v_{p1}, v_{p2} \ldots, v_{pm}\}$, n transmission line sets $E_p = \{e_{p1}, e_{p2} \ldots, e_{pn}\}$, and u is line weight. The electrical trend betweenness u can be formulated as follows:

$$u = \frac{\sqrt{w_i w_j} P_{ij}(b)}{P_{ij}} \tag{3}$$

where w_i is the maximum capacity of the power generation node, w_j is the maximum load of the load node, $P_{ij}(b)$ is the component of the active power flowing into the load node from the power generation node on the branch b, and P_{ij} is the power transmitted by the power generation node i to the load node j. According to this, the tidal current flows from the sending end to the receiving end area, and each power transmission branch has different tidal current allocation.

The node association matrix in the dual network is established according to the connection relationship between the cyber network and the physical network. If $(v_i, v_j) \in G_c$, the cyber network association matrix element $e_{ij}^c = \mu_{ij}$; if $(v_i, v_j) \in G_p$, the physical network association matrix element $e_{ij}^p = u_{ij}$; otherwise e_{ij}=0. The physical node provides energy for the cyber node, and the cyber node implements sensing, computing, and communication of the physical node, that is, has both monitoring and control functions. The intrinsic self-similar coupling method has high robustness [38] and is coupled by a one-to-one connection between the physical network high-tech node and the cyber network height node. The connection edge set between G_p and G_c is $E_{pc}(i, j)$ and $E_{cp}(i, j)$, regardless of the internetwork information and the direction of energy flow transmission. When the cyber and the physical network node are connected, the connection edge $e_{pc}(i, j)=e_{cp}(i, j)$=1; otherwise the value is 0. The dual-network association matrix $E_{cp}(i, j)$ is established as follows:

$$E_{cp}(i, j) = \begin{bmatrix} e_{1,1} & \cdots & e_{1,m} \\ \vdots & \ddots & \vdots \\ e_{m,1} & \cdots & e_{m,m} \end{bmatrix} \tag{4}$$

where the number of nodes in G_p and G_c is m.

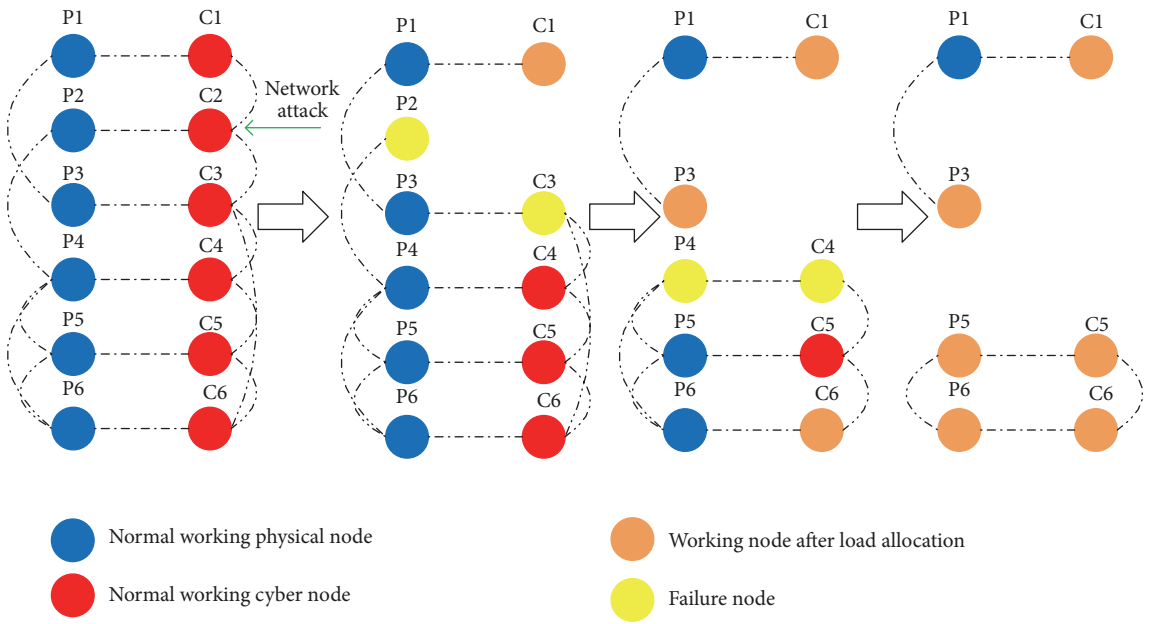


Figure 2: Schematic diagram of ECPS cascade failure.

E_c is weighted according to the degree structure of the cyber network. E_p is based on the power flow allocation for electrical betweenness weighting, and different power branches have different power flow components. So far, the established intranetwork correlation matrices E_c and E_p are integrated into the ECPS structure and power flow allocation characteristics by degree-media weighting, and the node heterogeneity is distinguished. The internetwork correlation matrix E_{cp} represents the dual-network coupling relationship. The information flows in the optimal path between the dispatching center and each cyber station system. The power flow starts from the generator node and is transmitted to each load node via the contact node, and the energy and information interaction between the two networks is realized.

2.2. ECPS Survivability Evaluation Model. This paper primarily discusses the change of ECPS survivability after the cyber network is subjected to attack. In fact, the cascading failure of the alternate domain resulting from the attacks on the cyber network will cause the ECPS to split into several isolated islands or isolated nodes. Thus, the number of failed nodes in the dual network increases and the structural connectivity decreases; the load removal rate increases, the risk scope is expanded, and the survivability is reduced. The survivability evaluation model is designed based on the load allocation optimization constraints of information flow and power flow in the cascade failure process.

2.2.1. Load Allocation Process of Cascading Failure. Researches reveal that cyber system nodes have their own power supply, physical nodes are not the only energy source of cyber nodes, and physical nodes failure does not necessarily cause cyber nodes to fail [38]. Similarly, if the cyber node fails, the coupled physical node cannot be monitored, and the physical node does not necessarily fail. Therefore, the introduction probability ω is used to characterize the probability of failure between networks. It is assumed that the cascading failure process occurs sequentially in the cyber network and the physical network; that is, the physical network state remains unchanged when the cyber network is reloaded, and vice versa. Referring to Figure 2, we describe the load allocation process for ECPS cascade failure as follows:

(1) The initial cyber network node fails: the C2 node starting from the cyber network G_c fails. Due to the load allocation of the information flow, the adjacent node C3 receives the additional load, exceeds its own capacity failure, and updates the matrices E_c and E_{cp} after stabilization.

(2) Failure analysis of physical network: failure of C2 and C3 nodes of G_c will cause the physical node coupled with it to fail with probability ω. At this time, P2 fails, causing optimal allocation of physical network G_p power flow and updating E_p and E_{cp} after stabilization.

(3) Cyber network failure analysis: in the G_p, the failed node in turn causes the G_c information flow to optimize the allocation with the probability ω, causing the cyber network C4 node to fail and updating the matrices E_c and E_{cp} after stabilization.

This reciprocates the above process until there are no more node failures in the two networks.

2.2.2. Survivability Evaluation Model

(1) ECPS Initial Load and Capacity. The traditional load capacity model uses the number of node's degree to define the load. It is necessary to grasp the global information, and the computational complexity is high and difficult to implement.

Here, the initial load $L_{ci}(0)$ of the cyber node v_{ci} is defined as the sum of the adjacent edge weights of the node as follows:

$$L_{ci}(0) = \varepsilon \sum_{j\in\Gamma} \mu^{\tau} = \varepsilon \left(\sum_{j\in\Gamma} \left(k_i k_j\right)^{\sigma} \right)^{\tau} \tag{5}$$

where ε and τ are load-adjustable parameters that control the load strength of different functional nodes (such as communication nodes and routing nodes), neighbor nodes include cyber nodes and coupled physical nodes in the network, and Γ is a set of neighbor nodes of v_{ci}. k_i and k_j can be obtained by E_c. The capacity C_{ci} of the cyber node v_{ci} is proportional to the initial load and is expressed as

$$C_{ci} = \left(1 + \rho_c\right) L_{ci}(0) \tag{6}$$

where ρ_c is the margin coefficient of the cyber node.

The load of the physical network mainly considers the power supply to the area. Each of the lines has power transmission. The power exchange between any pair of power generation and load nodes is restricted by the transmission capability. According to the principle of conservation of power inflow and outflow, the initial load of any node v_{pi} on the network is formulated as

$$L_{pi}(0) = \begin{cases} \dfrac{1}{2}\left(\displaystyle\sum_{b\in F(i)} u + \sum_{k\in L} w_{ik} \right), & i \in G \\ \dfrac{1}{2}\left(\displaystyle\sum_{b\in F(i)} u + \sum_{k\in G} w_{ki} \right), & i \in L \\ \dfrac{1}{2} \displaystyle\sum_{b\in F(i)} u, & others \end{cases} \tag{7}$$

where $F(i)$ is the set of power branches connected to node i.

C_{pi} capacity is proportional to the load as follows:

$$C_{pi} = \left(1 + \rho_p\right) L_{pi}(0) \tag{8}$$

where ρ_p is the margin coefficient of the physical nodes. The node load considers the difference between the nodes of the physical network and considers the transmission power on the arbitrary path (the element sequence of E_p) between the power generation and the load nodes.

The constraints that the cyber node and the physical node do not exceed the capacity limit and are working properly are stated in (9).

$$\begin{aligned} 0 < L_{ci} < C_{ci} \\ 0 < L_{pi} < C_{pi} \end{aligned} \tag{9}$$

(2) Constraints of Dual-Network Load Allocation. In the cyber network, the node failure will replan the route through the load (information flow) of the node, the load it carries will be distributed to the rest of the nodes in the network, and the whole network updates the load allocation [39]. After node i fails, the load increment of node j is given by

$$\Delta L_{cij} = L_{ci} \cdot L_c\left(d_{ij}, \theta, k_j, \xi\right) \tag{10}$$

where L_{ci} is the load of node i; d_{ij} is the path length between nodes i and j, which can be solved by Floyd algorithm [39] in accordance with the cyber network association matrix E_c; θ and ξ are load allocation strategy coefficients, where θ is the range strategy coefficient, which controls the range of load allocation, and the uniformity strategy coefficient, which controls the uniformity of load allocation; k_j is the degree of node j; $L_c(d_{ij}, \theta, k_j, \xi)$ is the scale coefficient expressed as

$$L_c\left(d_{ij}, \theta, k_j, \xi\right) = \frac{d_{ij}^{-\theta} k_j^{\xi}}{\sum_{m\in\Omega} d_{ij}^{-\theta} k_m^{\xi}} \tag{11}$$

where Ω is the set of normal working nodes of the cyber network.

The information flow preferential allocation strategy takes into account the constraints such as the shortest path length, load allocation range, and uniformity. It is described as follows:

$$\begin{aligned} &\min d_{ij} \\ &0 \le \theta < \infty \\ &0 \le \xi < \infty \end{aligned} \tag{12}$$

where $\min d_{ij}$ is the shortest path length between node i and j; when $\theta \longrightarrow 0$, the load allocation follows the global preference allocation strategy, and ξ=0 is the global uniform allocation strategy; when $\theta \longrightarrow \infty$, it is the nearest neighbor optimal allocation strategy, and ξ=0 is the nearest neighbor uniform allocation strategy; ξ>0 is a high-load preference allocation strategy. Considering the actual cyber network load allocation rules, this paper chooses the high-load preference allocation strategy between the global and the nearest neighbors, namely, $0<\theta<\infty$, $0<\xi<\infty$. When some cyber nodes fail, the load increment of the node j is given by

$$\Delta L_{cj} = \sum_{i\in\Lambda} \Delta L_{cij} = \sum_{i\in\Lambda} L_{ci} \cdot L_c\left(d_{ij}, \theta, k_j, \xi\right) \tag{13}$$

where Λ is the set of failure cyber nodes, and the load of the node j after load allocation can be written as follows.

$$L'_{cj} = L_{cj} + \Delta L_{cj} \tag{14}$$

When $L'_{cj} > C_{cj}$, that is, the node j after the load allocation exceeds the capacity, the cyber node j fails and causes a new load allocation.

When the cyber network node fails, the corresponding element e_{ij}=0 is modified by the probability ω, and the element e_{ij}^{p} value in the physical network association matrix E_p coupled with it is modified, so that the corresponding physical node is invalid, causing the physical network load allocation. The failure of the cyber network node will invalidate the physical node coupled with it with a certain probability ω, causing the physical network load allocation. When the physical network transformer node is overloaded, the transmission line is overloaded or the output of the generator exceeds the capacity limit, and the dispatch center

receives the information and issues control optimization instructions. The system optimizes the allocation according to the real-time network topological structure and operating state parameters, adjusts the generator, and cuts off part of the overload capacity to power flow convergence. If the power flow does not converge, indicating that the generator in the system cannot meet the load demand, then the part of the power load is removed. The objective function of load shedding optimization is given by the following.

$$\min \sum_{i}^{N_p} L_{pi\_cut} \tag{15}$$

The constraints to be met by the power flow balance equation are expressed as follows.

$$\begin{aligned} P_i(U,\delta) - P_{Di} + L_{pi_{cut}} &= 0 \\ Q_i(U,\delta) - Q_{Di} &= 0 \end{aligned} \tag{16}$$

The safe operation and optimization constraints are given as

$$\begin{aligned} P_{Gi,min} \le P_i(U,\delta) \le P_{Gi,max} \\ Q_{Gi,min} \le Q_i(U,\delta) \le Q_{Gi,max} \\ 0 \le L_{pi\_cut} \le P_{Di} \\ T_k(U,\delta) \le T_{k,max} \\ U_{i,min} \le U_i \le U_{i,max} \end{aligned} \tag{17}$$

where L_{pi_cut} is the load shedding amount of node i; $P_i(U,\delta)$ is the active power of node i; $Q_i(U,\delta)$ is the reactive power of node i; $P_{Gi,min}$, $P_{Gi,\max}$, $Q_{Gi,\min}$, $Q_{Gi,max}$ are the lower and upper limits of the active and reactive power of the generator node i, respectively; P_{Di} and Q_{Di} are the active and reactive loads of the node, respectively; T_k and $T_{k,max}$ are the power flow and the upper limit of the power flow of the branch k, respectively; $U_{i,min}$ and $U_{i,max}$ are the lower and upper voltage limits of node i, respectively.

(3) ECPS Survivability Evaluation Model. In an effort to quantitatively evaluate the survivability of the coupled system after cascading failure, we comprehensively consider the topological structure and operating conditions to define the ECPS survivability evaluation indicators such as node survival rate of R_{ns} and power load survival rate of R_{pls}.

(1) R_{ns}: R_{ns} is the ratio of the number of remaining working nodes of the coupled ECPS to the number of initial normal working nodes after the cascading failure is terminated. The transmission of information and electrical energy depends on a reliable connected topological structure. R_{ns} is used to measure the structural connectivity change of ECPS: the larger the R_{ns}, the better the structural connectivity and the higher the survivability as follows:

$$R_{ns} = \frac{N'}{N} \tag{18}$$

$$N' = N_c' + N_p', \quad N = N_c + N_p \tag{19}$$

where $N_c^{'}$ is the number of remaining nodes of the cyber network, $N_p^{'}$ is the number of remaining nodes of the physical network, $N^{'}$ is the number of remaining nodes of the cyber network and the physical network, N_c is the initial number of normal nodes of the cyber network, and N_p is the initial number of physical networks. The number of normal nodes, N, is the number of initial normal working nodes.

(2) R_{pls}: R_{pls} is the ratio of the residual power load of the coupled ECPS to the initial total power load after the cascading failure is terminated. When the power flow convergence fails, the safety risk is eliminated by removing the load. R_{pls} is used to measure the risk spread range of the ECPS: the larger the R_{pls}, the smaller the risk spread range and the higher the survivability as follows.

$$R_{pls} = 1 - \frac{\sum_i^{N_p} L_{pi\_cut}}{\sum_i^{N_p} L_{pi}(0)} \tag{20}$$

The ECPS survivability is related to the real-time topological structure and operating state. By calculating the square root, the R_{ns} and R_{pls} indicators are combined to establish an ECPS survivability evaluation model, and the comprehensive survivability value (V_{cs}) is calculated. The expression is mathematically expressed as follows.

$$V_{cs} = \sqrt{R_{ns} \cdot R_{pls}} \tag{21}$$

2.2.3. Model Simulation Process. Based on the previous analysis, and by considering the information flow and power flow optimization control of the dispatch center, the simulation process for designing the ECPS cascade failure survivability evaluation consists of the following steps.

Step 1. According to the topological structure and association relationship of the coupled system, establish an ECPS weighted correlation matrix, initialize node load and capacity, and all nodes in the dual network work normally.

Step 2. Set the cyber network node attack mode: (1) random attack mode: A_{random}, (2) deliberate attack mode: A_{sdr} (static degree ranking attack), A_{slr} (static load ranking attack), and A_{dlr} (dynamic load ranking attack). A_{random} refers to a random attack on a certain proportion of cyber network nodes; A_{sdr} refers to the network structure and parameters in advance and attacks the initial high-degree node of the cyber network in turn, and the attack strategy does not change in the process; A_{slr} refers to successively attacking the high-load nodes determined by the initial cyber network structure and parameters, and the attack process strategy does not change; A_{dlr} refers to attackers attacking the real-time high-load nodes updated by the load allocation in conformity with the cyber network structure and operation status after each attack. The attack mode is selected to remove the number of nodes in the cyber network with a ratio of p% ($0 \le p \le 30$), and the analog cyber network is subjected to network attacks.

Step 3. The information flow is optimized and redistributed. Furthermore, the topology structure after load allocation in

the cyber network is analyzed, and the remaining nodes of the statistical cyber network are collected.

Step 4. The physical node coupled with the failure cyber node will fail with the probability ω and disconnect the coupling edge, calculate the physical network flow at this time, and then upload the physical network topological structure as well as the power flow information to the dispatch center.

Step 5. The information received by the dispatching center will check whether the power flow exceeds the limit in accordance with the power flow status of the physical network. If a situation exceeds the limit, a control command is issued to enable the physical network to optimize the power flow allocation and go to Step 6. Otherwise, it goes to Step 7.

Step 6. If the optimization result converges, the physical network adjusts the generator output or activates the protection action device to cut off the capacity overload line; if the optimization result does not converge, the load optimization is performed to cut off part of the power load (see Section 2.2.4 for the optimization algorithm).

Step 7. The physical node fails to cause the cyber node coupled with it to fail with probability ω, the bearer load of the failed node is allocated according to the information flow optimization strategy, and the statistical cyber network and the remaining nodes of the physical network are collected.

Step 8. If the number of iterative dual-network nodes no longer changes, the single simulation ends, and the R_{ns}, R_{pls}, and V_{cs} of the coupled network are calculated.

2.2.4. Model Solving Algorithm. The load optimal allocation in the evaluation model is an optimization problem that attempts to minimize the coupled ECPS power load under the constraints of the node load capacity limit, the information flow preferential allocation strategy, the power flow optimization equation, and the system safety operation. There are numerous constraints, nonlinearity and high computational complexity. Therefore, it is easy for the bionics firefly optimization algorithm with simple structure and parameters to jump out of the local optimal solution and reduce the computational complexity [39]. However, the standard firefly algorithm has a relatively slow convergence rate in the initial stage. To solve this problem, this paper proposes a chaotic Lévy flight firefly algorithm to solve the model. Based on the standard firefly algorithm, chaotic optimization and Lévy flight search are introduced to improve the random step size as well as the efficiency of the solution.

(1) Chaotic Lévy Flight Firefly Algorithm. In the early stage of optimization, the firefly's position allocation is relatively scattered, the relative distance is long, the attraction is weak, and it is easy to prematurely converge when the solution domain is large. Thus, the following improvements are made:

(1) Chaos optimization relative attraction dynamically updates the value of the attraction coefficient γ by chaos optimization method to improve the mutual attraction ability of long-range fireflies and improves the convergence speed of the initial stage of the algorithm as presented in

$$\gamma_{k+1} = \chi\gamma_k\left(1-\gamma_k\right) \tag{22}$$

where k is the number of iterations, γ is in the range of 0.01 to 100, and χ is chaotic control coefficient.

(2) Lévy flight for random items: based on the idea of heuristic search, Lévy flight is used as a random step size in each local search process, and its expression is given by

$$\begin{aligned} x_i(k+1) = x_i(k) + \beta_{ij}\left(r_{ij}\right)\left(x_j(k) - x_i(k)\right) \\ + \alpha\left(r_1 - 0.5\right) \oplus Lévy \cdot X_M \end{aligned} \tag{23}$$

where x_i, x_j are the spatial position coordinates of fireflies i and j, respectively; β_{ij} is the attraction function; r_{ij} is the Cartesian distance between fireflies i and j; and r_1 is a random number uniformly distributed in the interval $[0, 1]$. $\oplus$ is the interpoint multiplication; r_1 is the distance between fireflies; X_M is the upper and lower limit of the search space of the objective function; Lévy is the random step size satisfying the random search path of the Lévy allocation, and its random step size is expressed as

$$Lévy\text{: } s = t^{-\lambda}, \quad 1 < \lambda \le 3 \tag{24}$$

where s is the Lévy random step size and $t^{-\lambda}$ is the Lévy allocation.

(2) Algorithm Flowchart of Model Solving. Based on the chaotic Lévy flight firefly algorithm, the model solution flow is given, as shown in Figure 3.

3. Case Studies

3.1. Experimental Data. The physical network in the ECPS relies on the IEEE 118-node system and its topological structure (as shown in Figures 4 and 5), and the cyber network is the 118-node BA scale-free network generated by Matlab 2016 (as shown in Figure 6). The weighted correlation matrices E_c, E_p, E_{cp} are generated in conformity with the preamble-mediated coupling method, and the ECPS network G=(G_c, G_p, E_{cp}) is characterized by G_c=(V_c, E_c, μ), G_p=(V_p, E_p, u), and E_{cp}.

The weighted correlation matrix is input to Python 3.5, and the model parameters are set as follows: cyber network weight coefficient σ=0.1; load-adjustable parameter ε=0.5, τ=1; double-network margin coefficient ρ_c=ρ_p=0.5; the load allocation strategy coefficient θ=ξ=1; the internetwork failure probability ω=0.5. Four model solving algorithms are selected [39–41]: classic firefly algorithm (FA), chaos firefly algorithm (CFA), improved chaos firefly algorithm (ICFA), and chaotic Lévy flight firefly algorithm (CLFFA). Algorithm parameter settings are shown in Table 1.

3.2. Evaluation Method Analysis. In order to verify the effectiveness and efficiency of the evaluation method, the following three aspects are analyzed: (1) comparison and

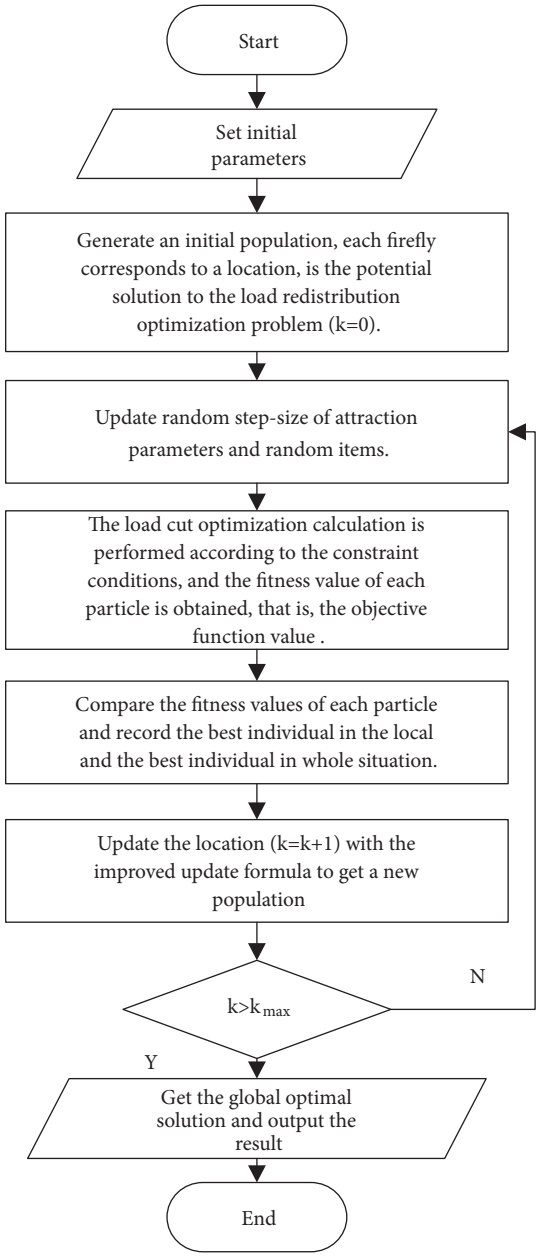


Figure 3: Algorithm flowchart of model solving.

analysis of ECPS survivability evaluation methods; (2) comparison and analysis of ECPS survivability under different attack modes; and (3) comparison and analysis of results and efficiency with different algorithms.

(1) Comparison and Analysis of ECPS Survivability Evaluation Methods. In the existing researches, the node cut rate and the power load cut rate are used as evaluation indicators to study the vulnerability of ECPS. When the vulnerability evaluation value is high, the survivability of ECPS is low. Using the A_{sdr} deliberate attack mode, the node cut rate and the power load cut rate are used as the survivability evaluation indicators. The ECPS of the typical IEEE118-BA118 was selected as the research subject, and the evaluation results of the following three evaluation methods are compared: (a) uncorrelated network seepage model (Method 1); (b) cascade failure model based on power flow optimization (Method 2); (c) the evaluation method in this paper, as shown in Figures 7(a) and 7(b).

From Figures 7(a) and 7(b), when the proportion of initial attack cyber nodes is low, the evaluation results of the three methods are similar. This is because the number of cyber node failures is small, the number of normal working nodes is large, the structural connectivity is good, the risk propagation range is small, and the information flow and power flow optimization are not obvious. When

Table 1: Algorithm parameter settings.

Solution algorithm	N	k_{max}	α	β	λ	γ	χ
FA	200	1000	0.5	1	-	1	-
CFA	200	1000	0.5	1	-	1	4
ICFA	200	1000	0.5	1	-	1	4
CLSFA	200	1000	0.5	1	1.5	-	4

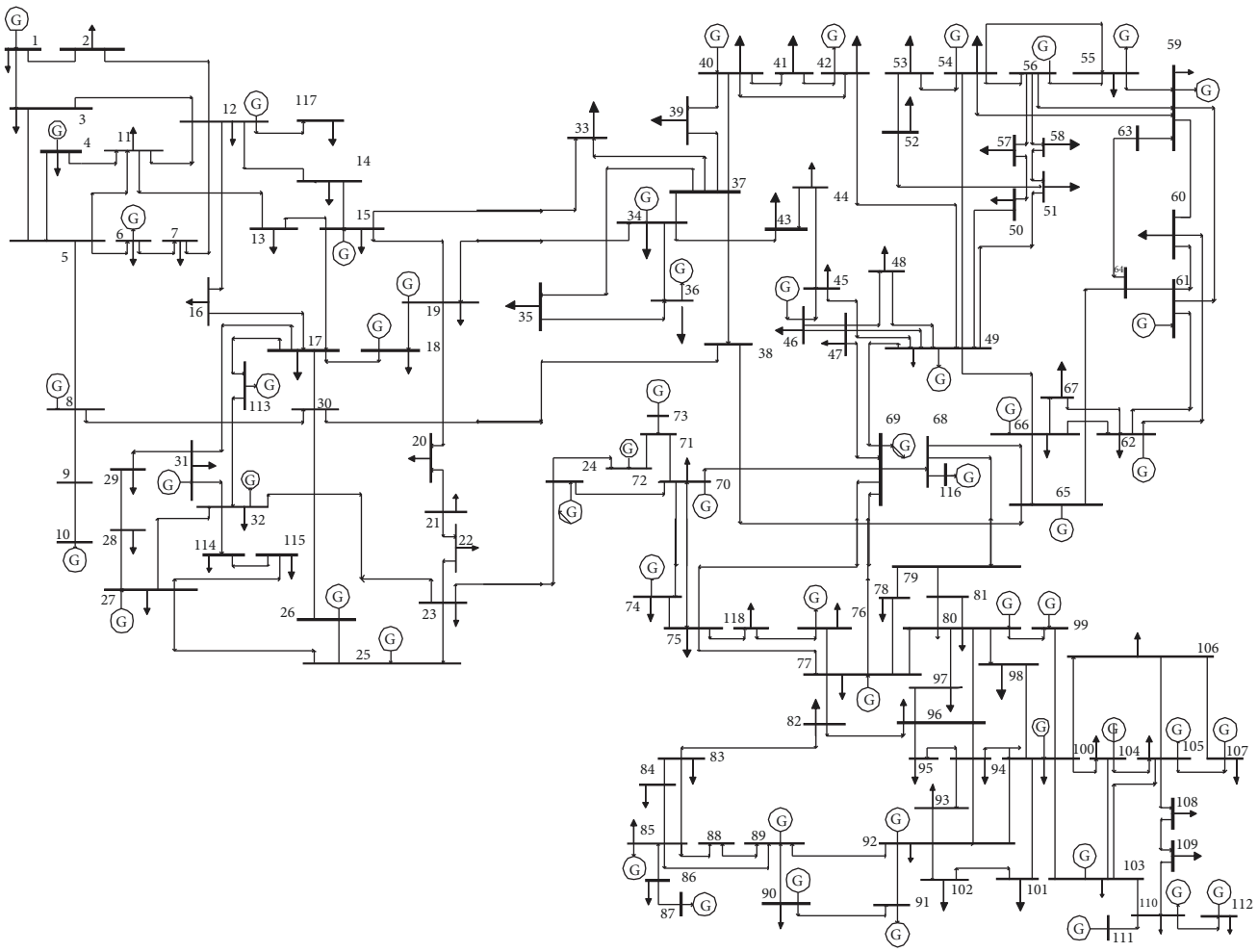


Figure 4: IEEE118-node system.

the ECPS structure is dissociated and the risk spread range is expanded, the evaluation results of the three methods are different. The method has the highest survivability. This is due to the structural characteristics analysis of the uncorrelated network seepage model. The node failure will cause the dependent nodes to directly depend on the failure, and the self-regulating ability of the coupled system is not considered. In fact, the cascading failure model based on the power flow optimization can consider certain power flow optimization. However, the actual information flow is not involved in the load optimization allocation feature; that is, there is no load optimization process on the cyber network side; this method introduces the load capacity factor of the dual-network node, considering the scheduling center to monitor the system topology and state changes in real time, and participating in the load allocation process of controlling traffic flow and power flow optimization enhances the ECPS ability to resist network attacks. In the actual operation process of ECPS, the system itself has the ability of sensing and regulation. There is the monitoring function of the dispatching center and the switching operation of the relay protection device. The evaluation method of this paper is closer to the actual operation. Therefore, considering the load optimization allocation can enhance reliability of the ECPS survivability evaluation results.

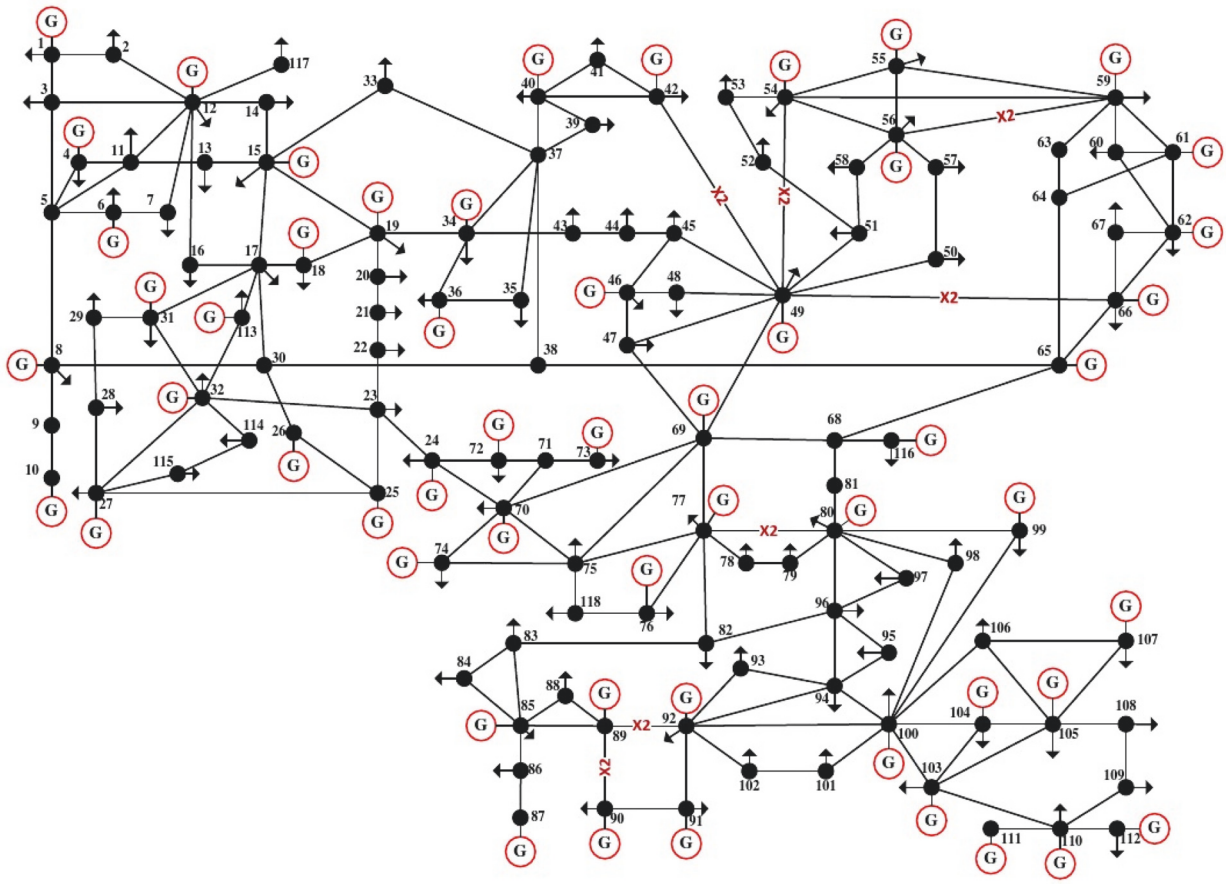


Figure 5: IEEE118-node network topology.

(2) Comparison and Analysis of ECPS Survivability under Different Attack Modes. The random attack and three deliberate attack modes were used to evaluate the ECPS structural connectivity and risk propagation range of the four different attack modes, as shown in Figures 8(a) and 8(b). The evaluation values of the comprehensive survivability V_{cs} obtained by the fusion index are shown in Table 2.

It can be seen from Figures 8(a) and 8(b) that, as the proportion of attack nodes in the cyber network increases, the connectivity of the ECPS and the survivability of the power load decrease, which indicated that the cyber node failure causes the cross-domain cascade failure of the coupled ECPS, so that the system topological structure is unpacked and hence the scope of risk spread is expanded. The overall trend of the two indicators is similar, but the slopes of the decline are not the same, which indicates that the survivability of coupled ECPS from a structural connectivity or operational state indicator is not comprehensive enough. For random attacks, the threshold ratio of attack nodes whose survival rate decreases to 0 is 23.7%, and the threshold ratio of attack nodes whose power load survival rate decreases to 0 is 22.8%, which indicates that the topological structure has lower vulnerability than the running status indicator. The defender needs to improve the robustness of the coupled system structure and also optimize the load allocation strategy of both information flow and power flow to improve the power load survival rate.

It can be seen from Table 2 that the evaluation results of the table combine the structural and state indicators to dynamically quantify the comprehensive survivability values of the ECPS under the four types of network attacks. The attack thresholds that caused the system to be completely paralyzed are 26%, 23%, 19%, and 13%. It is shown that the damage degree of the four attacks on ECPS survivability is ranked as: $A_{dlr} > A_{slr} > A_{sdr} > A_{random}$. Compared with random attacks, deliberate attacks are more harmful. Because of the actual grid operation, random attacks can be regarded as random disturbances caused by human errors and natural factors. The purpose of the attacks is not clear and the degree of damage is small. The deliberate attack means that the attacker has mastered the topological structure and operating parameters of the network in advance and designed the attack strategy more specifically. The load ranking attack is more harmful than the degree attack as far as the comparison is concerned, which indicates that the high-load node is more important. Because the method distinguishes the difference

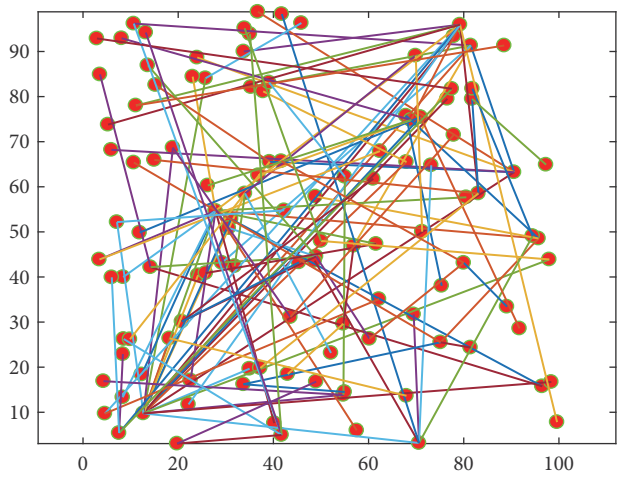
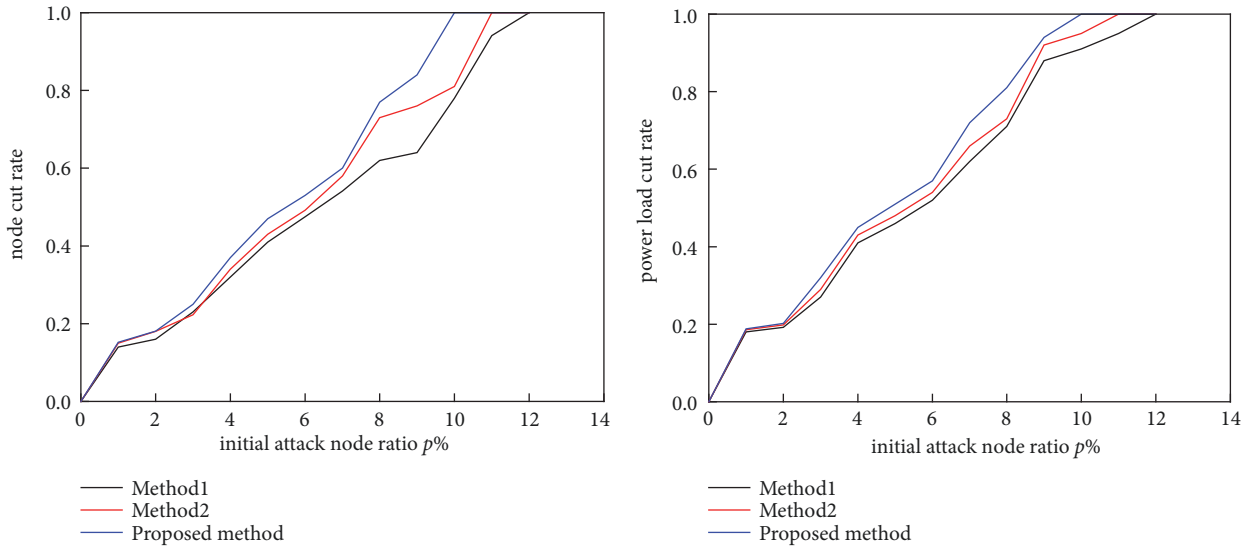


Figure 6: 118-node BA network topology.



(a) Chart of node cut rate comparison

(b) Chart of power load cut rate comparison

Figure 7: Comparison of ECPS survivability evaluation results with different methods.

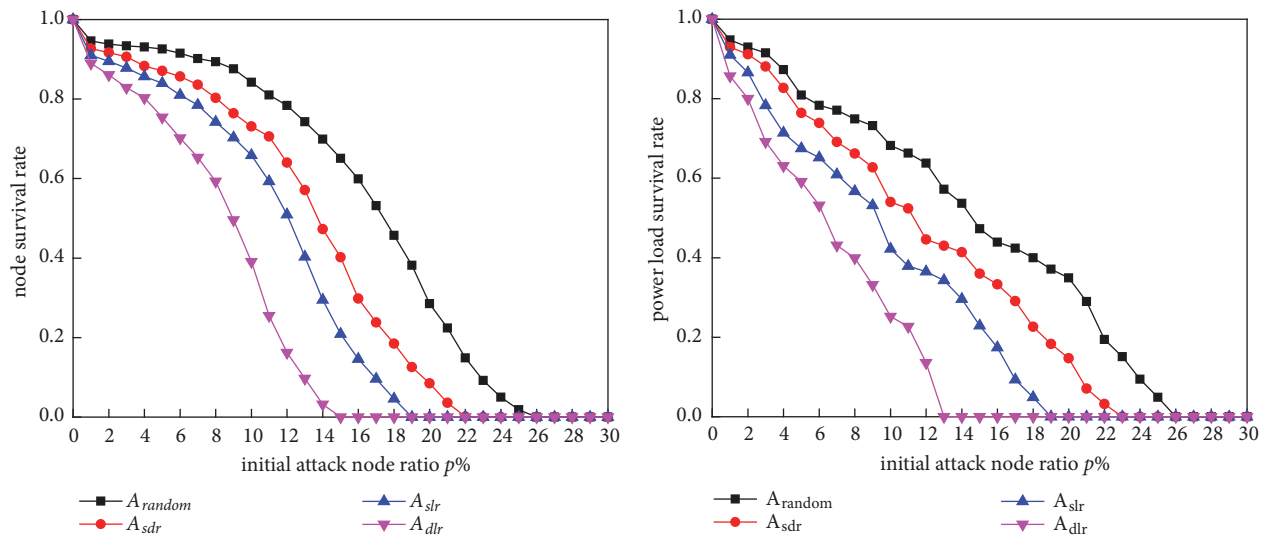
in node properties, the high-load node combined with the structure and state is the key node; it is not an important node of high-degree for single structure, so it requires a strong protection of these high-load nodes that improve the survivability of ECPS. In comparison with static attacks, dynamic attacks are more harmful. Improving survivability requires defenders to avoid ECPS network structure and state information leakage, monitor network status in real time, and develop dynamic defense strategies. Thus far, according to the evaluation method of this paper, the dynamic value of survivability of the ECPS cascade failure process can be effectively quantified.

(3) Comparison and Analysis of Results and Efficiency with Different Algorithms. Using A_{random} mode to attack 10% of the cyber nodes, the evaluation results of the four algorithms are compared, as shown in Table 3, and the solving efficiency of the four algorithms of different ECPS scales is compared, as shown in Figure 8.

From Table 3, we can see that the four algorithms can make the objective function value converge after several iterations and can obtain the optimal solution after load allocation. The survivability evaluation result of ECPS of CFA is better than that of FA, because CFA initializes the population with chaotic map sequence. Variables can traverse all nonrepetitive states in a certain range according to the sequence law to optimize the search. The range of chaotic optimization is extended to the optimal variable interval, and the initial solution with stronger search ability and uniform distribution can be obtained, which can avoid falling into premature convergence partial optimal solution. Moreover, the number of iterations of CFA is 23 times less than that

Table 2: ECPS comprehensive survivability evaluation values under different attack modes.

Initial attack node ratio p%	Comprehensive survivability value (V_{cs})			
	A_{random}	A_{sdr}	A_{slr}	A_{dlr}
0	1	1	1	1
1	0.9470	0.9285	0.9100	0.8733
2	0.9340	0.9145	0.8804	0.8299
3	0.9245	0.8934	0.8291	0.7574
4	0.9015	0.8545	0.7822	0.7118
5	0.8655	0.8157	0.7530	0.6675
6	0.8464	0.7958	0.7267	0.6111
7	0.8339	0.7600	0.6914	0.5305
8	0.8183	0.7291	0.6486	0.4864
9	0.8008	0.6921	0.6116	0.4058
10	0.7578	0.6283	0.5273	0.3139
11	0.7328	0.6082	0.4741	0.2406
12	0.7072	0.5343	0.4310	0.1484
13	0.6519	0.4955	0.3718	0
14	0.6127	0.4425	0.2955	0
15	0.5549	0.3804	0.2188	0
16	0.5128	0.3150	0.1594	0
17	0.4749	0.2632	0.0945	0
18	0.4276	0.2045	0.0474	0
19	0.3765	0.1518	0	0
20	0.3154	0.1118	0	0
21	0.2549	0.0506	0	0
22	0.1700	0.0057	0	0
23	0.1179	0	0	0
24	0.0687	0	0	0
25	0.0299	0	0	0
26	0	0	0	0



(a) ECPS structural connectivity

(b) ECPS risk spread range

Figure 8: Comparison of ECPS survivability under different attack modes.

Table 3: ECPS comprehensive survivability evaluation value with different algorithms.

Different algorithm	V_{cs}	Number of convergent iterations
FA	0.6641	144
CFA	0.6987	121
ICFA	0.7103	117
CLFFA	0.7578	102

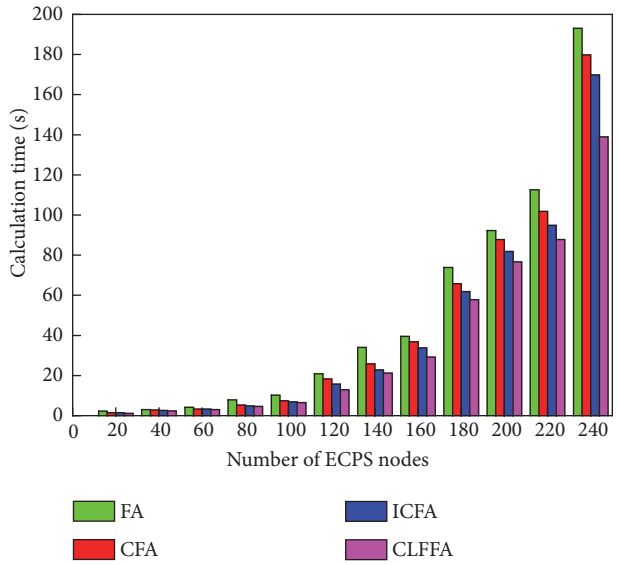


Figure 9: Comparison of efficiency of model solving algorithms with different ECPS scales.

of FA, which shows that the chaotic dynamic search area significantly improves the search speed of the algorithm. ICFA adds chaotic local search operator on the basis of CFA to search the current optimal solution by random substitution of individual population and using Gauss mutation. ICFA is superior to CFA in terms of the accuracy of local search space, but has no significant improvement in the speed of optimization. The survivability evaluation results of CLFFA algorithm presented in this paper are better than those of the other three algorithms. This is mainly due to the fact that the ICFA algorithm introduces the random step size of Lévy distribution in an effort to dynamically adjust the local and global search behavior, which can balance the proportion of local and global search, and take into consideration the local and global optimal characteristics. Therefore, it obtains the optimal solution with higher global accuracy and the number of iterations. Less than the other three algorithms, the results converge quickly.

Figure 9 shows that when the size of ECPS is small and the number of nodes is less than 60, the computing time of the four algorithms is almost the same, which shows that the optimization effect of small-scale coupled system is not obvious. This is owing to the small number of small-scale ECPS, the small search area, and the relatively high attraction of fireflies to each other, which cannot consider both local and global optimization characteristics. With the enlargement of ECPS scale and the number of nodes, CLFFA enhances the attraction between fireflies by chaotic optimization dynamics, dynamically adjusts the proportion of local and global searches by the random step size of Lévy distribution, changes the local premature convergence characteristics, makes the optimization results jump out of the local optimal solution quickly, improves the speed of solution, and shows great advantages in time consumption. This means that when the proposed algorithm is applied to large-scale ECPS, the evaluation model can be solved more efficiently.

4. Conclusions and Future Research

Based on the simulation results on the test cases, the conclusions can be drawn as follows.

(1) The weighted correlation matrix of ECPS is established to realize the formal representation of ECPS, which distinguishes the node properties and functional differences and overcomes the shortage of the unweighted model representation method.

(2) Considering the load optimal allocation, the ECPS survivability is designed. The evaluation model compensates for the limitations of the existing model ignoring the node load capacity as well as the information-energy flow optimization. The survivability of the ECPS is analyzed from the structural connectivity and the risk propagation range points of

view. Survivability provides a theoretical reference for guiding ECPS against network attacks.

(3) The model solving algorithm of chaotic Lévy flight firefly is proposed to make the calculation results converge quickly, and the evaluation efficiency is significantly improved when applied to large-scale systems.

This paper focuses on the impact of load optimal allocation on the survivability of the ECPS, and the differences in cyber network topological structure as well as transmission service types will also affect the evaluation results. Therefore, the follow-up research works will consider the above factors to further improve the survivability evaluation method, so that the evaluation results will be more realistic.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The research was funded by the following projects: National Natural Science Foundation Key Project: Extraction and Characterization of Power System Operation Behavior Recognition Based on Large Data (51437003); Jilin Province Science and Technology Development Plan Project: Research on Key Technologies of Network Information Attack Identification and Defense Considering Information Physical Fusion (20180201092GX); and Jilin Province Science and Technology Development Plan Project: Jilin Electric Power Big Data Intelligent Processing Engineering Research Center (20160623004TC). Thanks are due to Pro. Yang Li from the Argonne National Laboratory in the United States for providing the algorithm improvement guide.

References

[1] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in *Proceedings of the Design Automation Conference, IEEE*, vol. 14, pp. 731–736, 2010.

[2] K. D. Kim and P. R. Kumar, "Cyber–physical systems: a perspective at the centennial," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 1287–1308, 2012.

[3] Y. S. Xue, M. L. Li, J. B. Luo et al., "Modeling method for coupling relations in cyber physical power systems based on correlation characteristic matrix," *Automation of Electric Power Systems*, vol. 42, no. 2, pp. 11–19, 2018.

[4] Y. Li, Z. Yang, G. Li et al., "Optimal scheduling of isolated microgrid with an electric vehicle battery swapping station in multi-stakeholder scenarios: a bi-level programming approach via real-time pricing," *Applied Energy*, vol. 232, pp. 54–68, 2018.

[5] Y. Li, Y. Li, G. Li, D. Zhao, and C. Chen, "Two-stage multi-objective OPF for AC/DC grids with VSC-HVDC: incorporating decisions analysis into optimization process," *Energy*, vol. 147, pp. 286–296, 2018.

[6] S. Karnouskos, "Cyber-physical systems in the Smart Grid," in *Proceedings of the IEEE International Conference on Industrial Informatics*, pp. 20–23, July 2013.

[7] K. R. Davis, C. M. Davis, S. A. Zonouz et al., "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2464–2475, 2015.

[8] S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[9] Y. Song, X. Liu, Z. Li, M. Shahidehpour, and Z. Li, "Intelligent data attacks against power systems using incomplete network information: a review," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 4, pp. 630–641, 2018.

[10] L. Lyu, C. Chen, J. Yan, F. Lin, C. Hua, and X. Guan, "State estimation oriented wireless transmission for ubiquitous monitoring in industrial cyber-physical systems," *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 1, pp. 187–201, 2019.

[11] J. B. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and counter measures," *IEEE Transactions on Power Systems*, p. 1, 2018.

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

[13] A. Avritzer, S. Suresh, E. D. S. E. Silva et al., "Survivability models for the assessment of smart grid distribution automation network designs," in *Proceedings of the Joint Wosp/sipew International Conference on PERFORMANCE Engineering*, pp. 241–252, 2013.

[14] X. Ji, B. Wang, D. Liu, and T. Zhao, "Review on interdependent networks theory and its applications in the structural vulnerability analysis of electrical cyber-physical system," *Proceedings of the CSEE*, vol. 36, no. 17, pp. 4521–4533, 2016.

[15] C. Lo and N. Ansari, "Decentralized controls and communications for autonomous distribution networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 66–77, 2013.

[16] D. Zhou, H. E. Stanley, G. D'Agostino, and A. Scala, "Assortativity decreases the robustness of interdependent networks," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 86, no. 2, p. 066103, 2012.

[17] Z. Huang, C. Wang, M. Stojmenovic, and A. Nayak, "Characterization of cascading failures in interdependent cyber-physical systems," *IEEE Transactions on Computers*, vol. 64, no. 8, pp. 2158–2168, 2015.

[18] Z. Kong and E. M. Yeh, "Correlated and cascading node failures in random geometric networks: A percolation view," in *Proceedings of the 4th International Conference on Ubiquitous and Future Networks, ICUFN 2012*, pp. 520–525, July 2012.

[19] J. Guo, Y. Han, C. Guo, F. Lou, and Y. Wang, "Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties," *Energies*, vol. 10, no. 1, 2017.

[20] M. Parandehgheibi and E. Modiano, "Robustness of interdependent networks: The case of communication networks and the power grid," in *Proceedings of the 2013 IEEE Global Communications Conference, GLOBECOM 2013*, pp. 2164–2169, December 2013.

[21] S. Chattopadhyay and H. Dai, "Estimation of robustness of interdependent networks against failure of nodes," in *Proceedings of the GLOBECOM 2016 - 2016 IEEE Global Communications Conference*, pp. 1–6, Washington, DC, USA, December 2016.

[22] L. Tang, K. Jing, J. He, and H. E. Stanley, "Complex interdependent supply chain networks: cascading failure and robustness," *Physica A: Statistical Mechanics and its Applications*, vol. 443, pp. 58–69, 2016.

[23] G. B. Giannakis, V. Kekatos, N. Gatsis, S. Kim, H. Zhu, and B. F. Wollenberg, "Monitoring and optimization for power grids: a signal processing perspective," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 107–128, 2013.

[24] M. Beccuti, S. Chiaradonna, F. Di Giandomenico, S. Donatelli, G. Dondossola, and G. Franceschinis, "Quantification of dependencies between electrical and information infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 1, pp. 14–27, 2012.

[25] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 530–538, 2016.

[26] L. Wei, A. H. Moghadasi, A. Sundararajan, and A. I. Sarwat, "Defending mechanisms for protecting power systems against intelligent attacks," in *Proceedings of the 2015 10th System of Systems Engineering Conference, SoSE 2015*, pp. 12–17, May 2015.

[27] G. Chen, Z. Y. Dong, D. J. Hill, and Y. S. Xue, "Exploring reliable strategies for defending power systems against targeted attacks," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1000–1009, 2011.

[28] T. Ding, Y. Lin, G. Li et al., "A new model for resilient distribution systems by microgrids formation," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 4145–4147, 2017.

[29] T. Ding, Y. Lin, Z. Bie et al., "A resilient microgrid formation strategy for load restoration considering master-slave distributed generators and topology reconfiguration," *Applied Energy*, vol. 199, pp. 205–216, 2017.

[30] T. Ding, C. Li, C. Yan et al., "A bilevel optimization model for risk assessment and contingency ranking in transmission system reliability evaluation," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3803–3813, 2017.

[31] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2260–2272, 2016.

[32] Y. Sun and X. Tang, "Cascading failure analysis of power flow on wind power based on complex network theory," *Journal of Modern Power Systems and Clean Energy*, vol. 2, no. 4, pp. 411–421, 2014.

[33] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "SOCCA: a security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 3–13, 2014.

[34] J. S. Wang, X. P. Wu, and Y. Q. Cheng, "Invulnerability of weighted scale-free network against cascading failure," *Complex Systems and Complexity Science*, vol. 10, no. 2, pp. 13–19, 2013.

[35] H. Eman, E. Mellitus, and F. Abdallah, "Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification," *International Journal of Electrical Power & Energy Systems*, vol. 104, pp. 817–826, 2019.

[36] C. Ding, H. Yao, J. Du et al., "Load-induced cascading failures in interconnected network systems," *International Journal of Modern Physics C*, vol. 29, no. 8, 2018.

[37] Z. Zhao, P. Zhang, and H. Yang, "Cascading failures in interconnected networks with dynamical redistribution of loads," *Physica A: Statistical Mechanics and its Applications*, vol. 433, pp. 204–210, 2015.

[38] Z. Dong, Y. Fang, and M. Tian, "Influences of various coupled patterns and coupling strength on power-communication coupled networks," *High Voltage Engineering*, 2015.

[39] Z. Qu, Y. Zhang, P. Xin, J. Li, and K. Hu, "An energy internet routing algorithm on hypergraph based minimum-energy loss," *Journal of Northeast Electric Power University*, vol. 37, no. 6, pp. 93–99, 2017.

[40] O. Yagan, D. Qian, J. Zhang, and D. Cochran, "Optimal allocation of interconnecting links in cyber-physical systems: interdependence, cascading failures, and robustness," *IEEE Transactions on Parallel & Distributed Systems*, vol. 23, no. 9, pp. 1708–1720, 2012.

[41] T. Hassanzadeh, H. Vojodi, and A. M. Moghadam, "A multilevel thresholding approach based on levy-flight firefly algorithm," in *Proceedings of the 2011 7th Iranian Conference on Machine Vision and Image Processing (MVIP)*, pp. 1–5, Tehran, Iran, November 2011.