frontiers | Frontiers in Energy Research

ORIGINAL RESEARCH
published: 12 May 2022
doi: 10.3389/fenrg.2022.887870

Cooperative Resilience of Cyber–Physical Power Systems Under Hybrid Attacks *via* Dynamic Topology

Jiahui Jin, Yonghui Liu*, Peiyue Li and Mengyan Chang

School of Electrical Engineering, Shanghai DianJi University, Shanghai, China

In this study, the cooperative resilience of cyber–physical power systems under hybrid attacks is investigated. First, a detection model of physical attacks depending on the residual of the output impedance angle is established. Second, by analyzing the encrypted communication between physical and cyber systems, a detection algorithm for cyberattacks is proposed. Then, by using an enumeration method, islanded cyber–physical power systems are built with non-attacked and repaired parts. Moreover, to save resilient resources, cooperative optimization is established after the individual optimization of islanded cyber and physical systems. Since the building and optimization are executed alternately, the topology of the systems is dynamic. Finally, simulation results demonstrate the effectiveness of the proposed method.

Keywords: cooperative resilience, dynamic topology, islanded cyber–physical power systems, enumeration method, hybrid attacks

OPEN ACCESS

Edited by:
Enhua Wang,
Beijing Institute of Technology, China

Reviewed by:
Zhijian Hu,
Nanyang Technological University,
Singapore
Xiaozheng Jin,
Qilu University of Technology, China

****Correspondence:***
Yonghui Liu
liuyh@sdju.edu.cn

Specialty section:
This article was submitted to Process and Energy Systems Engineering, a section of the journal Frontiers in Energy Research

Received: *02 March 2022*
Accepted: *07 April 2022*
Published: *12 May 2022*

Citation:
Jin J, Liu Y, Li P and Chang M (2022) Cooperative Resilience of Cyber–Physical Power Systems Under Hybrid Attacks via Dynamic Topology.
Front. Energy Res. 10:887870.
doi: 10.3389/fenrg.2022.887870

1 INTRODUCTION

Cyber–physical power systems (CPPSs) have received more and more attention in the past few decades because of their widespread applications, such as automatic control of power systems, intelligent systems, and smart grids. CPPSs are composed of physical systems and cyber systems. Traditionally, physical systems are composed of power generation equipment, transmission lines, transformation equipment, and electric equipment. Since the network among communication hardware, communication software, and systems is open, the communication over an open network may be subjected to malicious cyberattacks. Hybrid attacks are composed of physical attacks (Dong and Xu, 2020) and cyberattacks (Huang et al., 2022). When hybrid attacks occur, CPPSs suffer more damage. Resilience is composed of detecting attacks when they occur and implementing resilient strategies under attack. The resilience of systems is one that is better able to sustain and recover from adverse events. A more resilient grid is one with fewer and shorter power interruptions (Amoretti and Ferrari, 2013). According to the U.K. Cabinet Office, resilience encompasses reliability, and it further includes resistance, redundancy, response, and recovery as key features (Huang et al., 2017). Therefore, it is essential to design a resilient strategy to ensure the security of CPPSs. The resilience of CPPSs is the recovery of attacked CPPSs with a quick response (Kshetri and Voas, 2017).

In recent years, many types of research are focused on the resilience of physical attacks. In Sahoo et al. (2020), an event-driven attack resilient strategy is introduced for DC microgrids, which replaces the attacked signal with an event-driven signal. By analyzing the impacts of attacks on communication links, local controllers, and master controller, distributed resilient control is proposed in Zhou Q. et al. (2020). To solve the secondary control of islanded microgrids under false data injection attacks, a hidden layer-based attack resilient distributed cooperative control algorithm is introduced (Chen et al., 2021). To deal with physical attacks, a distributed resilient control strategy for multiple energy storage systems of islanded microgrids is proposed in Deng et al. (2021). To increase the resilience of the shipboard power systems, an optimal defense strategy is proposed to protect critical lines against attacks (Ding et al., 2020). With the development of multiarea-synchronous CPPSs, more and more cyber equipment is installed in the feedback loop of power grids (Zhou Q. et al., 2020). Hence, with the increase in cyber equipment, the risks of cyberattacks have also increased.

Recently, to deal with cyberattacks, including denial-of-service attacks and deception attacks, many results on resilient strategy have been obtained (Franzè et al., 2019; Li et al., 2020; Wu et al., 2020; Yuan et al., 2020; Mousavinejad et al., 2021). Among them, resilient control of the wireless networked systems under denial-of-service attacks is designed (Yuan et al., 2020). A resilient distributed strategy of multi-task systems is designed (Li et al., 2020). Based on the event-triggered strategy, a distributed algorithm for resilient control of multi-agent networks under deception attacks is proposed (Wu et al., 2020). Resilient control of discrete-time linear systems subjected to state and input constraints, bounded disturbances, and measurement noises under replay attacks is designed (Franzè et al., 2019). To ensure stability of the systems under deception attacks, a resilient set-membership estimation strategy is designed (Mousavinejad et al., 2021). For multi-area power systems, a novel distributed fuzzy load frequency control approach is proposed under cross-layer attacks (Hu et al., 2020). Under cyberattacks, a new distributed economic model predictive control strategy is proposed for the load frequency control with the participation of plug-in electric vehicles (Hu et al., 2021).

From the aforementioned research, it is seen that a physical resilient strategy is designed only to solve physical attacks and a cyber-resilient strategy is designed only to solve cyberattacks. However, hybrid attacks composed of physical and cyberattacks are not considered.

More recently, to deal with hybrid attacks, many resilient strategies have been proposed. A reconfigurable system is designed with embedded intelligence and cooperative resilient schemes (Qi et al., 2011). A fuzzy system-based reinforcement learning approach is proposed for the resilient optimal of interconnected microgrids (Zhang et al., 2021). The problem of event-based security control is investigated for state-dependent uncertain systems under hybrid attacks (Liu et al., 2019). It is known that black start is used to repair CPPSs. Since the resilient time of black start depends on the longest repaired time, in black start, some equipment does not work even though it is repaired, and some non-attacked equipment stops working until the connected equipment is repaired. Obviously, some non-attacked equipment is idle, which leads to wastage of resources. To improve the utilization efficiency of the resources, some repaired equipment and non-attacked

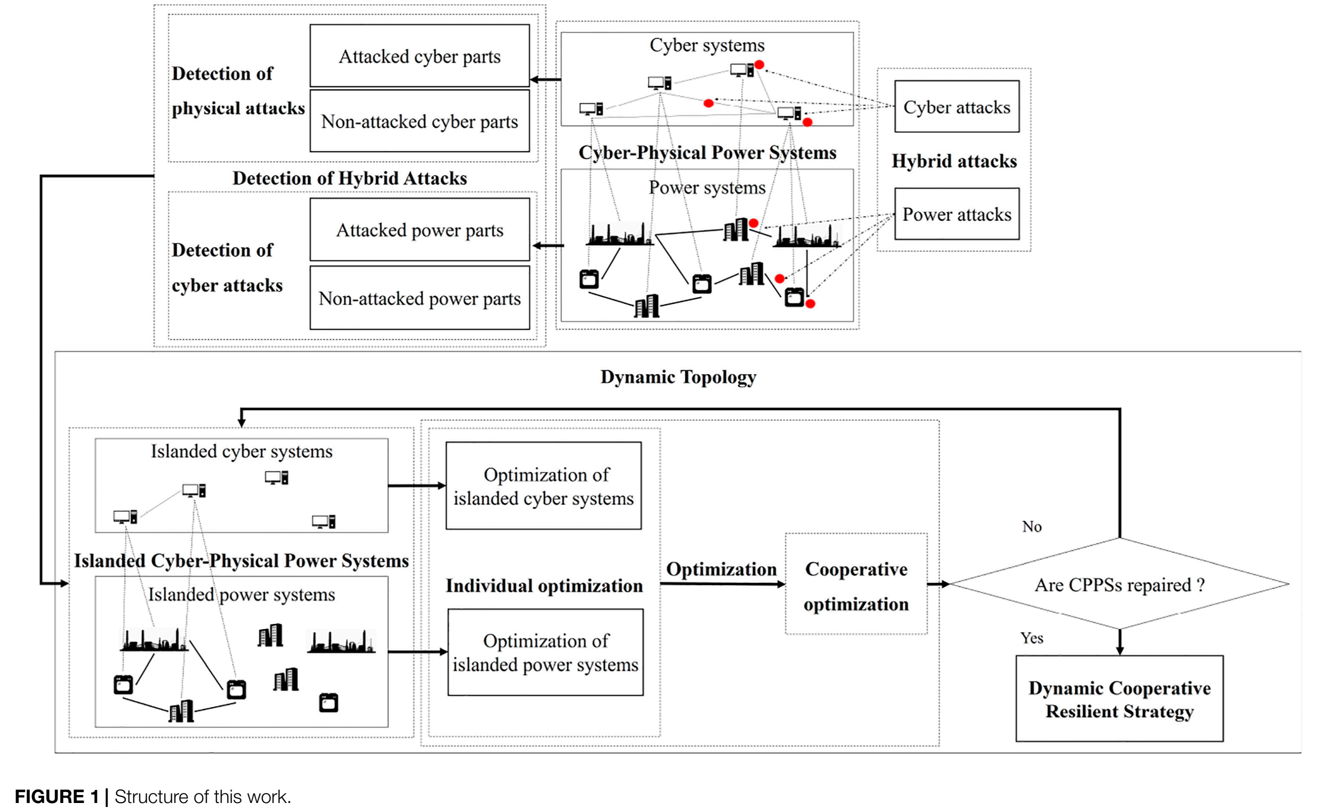

FIGURE 1 | Structure of this work.

equipment are designed to build islanded cyber–physical power systems (ICPPSs), which motivates this work.

Based on the aforementioned discussion, cooperative resilience of CPPSs under hybrid attacks via dynamic topology is considered. Cooperative resilience of cyber–physical power systems is composed of the detection of hybrid attacks and dynamic topology. Compared with the resilient strategies of CPPSs under hybrid attacks, the main contributions are as follows:

1) To detect the attacks in power systems, the detection model is constructed. Differing from the previous works (Franzè et al., 2019; Li et al., 2020; Wu et al., 2020; Yuan et al., 2020; Mousavinejad et al., 2021) where the detection model or algorithm was constructed based on mathematical characteristics of communication data, the detection algorithm of cyberattacks is proposed by the detection results of physical attacks.
2) To analyze the dynamic topology of ICPPSs, the constraints of ICPPSs under non-attacked parts are considered. Differing from the previous works (Rachmawati et al., 2020; Sanaullah et al., 2020) where the minimum spanning tree algorithm was selected to solve the topology, the solution algorithm of ICPPSs is proposed to obtain the topology.
3) By optimizing islanded power systems and islanded cyber systems individually, cooperative optimization is constructed such that the resources of the dynamic resilience are reduced, which has not been well studied in the existing literature.

The structure of this work is shown in **Figure 1**. The remainder of this article is organized as follows. CPPSs are described in **Section 2**. In **Section 3**, the detection model is obtained, and an outlier detection algorithm is established. Based on the constraints of CPPSs, the solution algorithm of ICPPSs is built in **Section 4**. In **Section 5**, the resilient strategies of ICPPSs are optimized. In **Section 6**, an illustrative example is given to show the effectiveness of the cooperative resilient strategy. The conclusion is presented in **Section 7**.

Remark 1: In **Figure 1**, dynamic topologies are composed of modeling and optimization. Based on the old ICPPSs, the aggregation of ICPPSs is constructed and optimized. With the update of the modeling and optimization of ICPPSs, the topologies are updated dynamically.

2 SYSTEM DESCRIPTION

2.1 Power Systems

Consider the power flow calculation described by an equation of the following form:

$$h(P, Q, \theta) = 0, \tag{1}$$

where P is the active power, Q is the reactive power, and θ is the error of phase.

The input power of the nodes is the sum of the input of the power source and the load power. The load power is dependent on the user. It is an uncontrollable parameter (Guo et al., 2021). The active and reactive power, which are controlled by the operator, are supplied by the power source. It is a controllable parameter (Fan et al., 2021). The error of phase, which is changed by uncontrollable and controllable parameters, is the state parameter (Zhou S. et al., 2020). Based on the three parameters, **Eq. 1** is rewritten as follows:

$$P_i = U_i \sum_{j \in i} U_j \left(G_{ij} \cos\theta_{ij} + B_{ij} \sin\theta_{ij} \right), \tag{2}$$

$$Q_i = U_i \sum_{j \in i} U_j \left(G_{ij} \sin\theta_{ij} - B_{ij} \cos\theta_{ij} \right), \tag{3}$$

where P_i is the active power of the node i, Q_i is the reactive power of the node i, U_i is the voltage of the node i, G_i is the conductance of the node i, B_i is the susceptance of the node i, θ_{ij} is the error of phase between the node i and node j, and $j \in i$ is that the node j is linked with the node i.

2.2 Cyber Systems

For the proposed detection algorithm of cyberattacks, the somewhat homomorphic encryption (SWHE) scheme (Dyer et al., 2019) is applied since it is designed as an improved encryption scheme to apply CPPSs. The SWHE scheme allows only positive integer values. However, some of the parameters are complex and have negative values in the CPPSs. Therefore, it is often necessary to transform the parameters into positive integer values. The complex and negative values are transformed into positive integer values (Quirce et al., 2020). During production and tests, the utilization of the central processing unit (CPU) is important. In this study, the application of virtual CPU (VP) is considered. In the virtual environment, the utilization of the CPU is better than the entitled capacity (EC) (Viveros and Lopez-Pires, 2021). The utilization of the CPU is as follows:

$$D = \begin{cases} D_{EC}, \text{Non} - \text{virtual environment} \\ D_{EC} + D_{VP}, \text{Virtual environment} \end{cases}, \tag{4}$$

where D is the utilization of the CPU, D_{EC} is the utilization of EC, and D_{VP} is the utilization of VP. Then, the utilizations of EC and VP are described as follows:

$$D_{EC} = \frac{EC\_U_{ser}\% + ECC\_Sys\%}{EC}, \tag{5}$$

$$EC\_User\% = \frac{O\left(C\_U_{Ser}\right)}{EC}, \tag{6}$$

$$EC\_Sys\% = \frac{O(C\_Sys)}{EC}, \tag{7}$$

$$D_{VP} = VP - User\% + VP - Sys\%, \tag{8}$$

$$VP\_U_{ser}\% = \frac{O(C\_User)}{VP}, \tag{9}$$

$$VP\_Sys\% = \frac{O(C\_Sys)}{VP}, \tag{10}$$

where *EC_User%* is the utilization of the calculation in EC, *EC_Sys%* is the utilization of the calculating data in EC, *O*() is the time complexity of the calculation, *EC* is the number of EC, *VP_User%* is the utilization of the calculation in VP, *VP_Sys%* is the utilization of the calculating data in VP, and *VP* is the number of VP.

3 DETECTION OF HYBRID ATTACKS

Under physical attacks, power equipment is damaged. Thus, the balance between power supply and demand is broken. Under cyberattacks, the cyber nodes and lines are attacked by false data or blocked communication lines. When CPPSs are attacked by hybrid attacks, the unbalance of power is not repaired by communication. The frequency is sensitive to the unbalance. Therefore, the error of the frequency is used to detect the attacks. To detect the hybrid attacks, the frequency satisfies the following expression:

$$|f - f_e| > \varepsilon, \tag{11}$$

where f is the actual frequency, f_e is the theoretical frequency, and ε is the error of the frequency.

When CPPSs are attacked by hybrid attacks, the unbalance of power is not repaired by communication. With the communication and cascading faults, the unbalance of hybrid attacks is bigger than one of disturbances or error measurement. The frequency is sensitively influenced by the unbalance. In this study, the error of the attacks is set larger than one of disturbances or error measurement.

3.1 Detection of Physical Attacks

The output impedance angle is used to detect the physical attacks. Suppose nodes i and j are connected. The maximum voltage and phase angle of the voltage of node i are U_i and θ_i. The maximum current and phase angle of the current from node i to node j are I_{ij} and δ_{ij}. The equivalent impedance of the connected line from node i to node j is as follows:

$$\dot{I}_{ij} = I_{ij}\left(\cos\delta_{ij} + j\sin\delta_{ij}\right) = I_{ij}\mathrm{e}^{\mathrm{j}\delta_{ij}}, \tag{12}$$

$$Z_{ij} = \left(\dot{U}_i - \dot{U}_j\right)/\dot{I}_{ij}. \tag{13}$$

Then, the phase angle of the equivalent impedance is described as follows:

$$d_{ij} = \arg\left(Z_{ij} - Z_{ji}\right). \tag{14}$$

The error of phase angle with the equivalent impedance is as follows:

$$\Delta d_{ij} = d'_{ij} - d_{ij} = \arg\left(\frac{Z'_{ij} - Z'_{ji}}{Z_{ij} - Z_{ji}}\right). \tag{15}$$

Considering **Eq. 15**, one has

$$Z'_{ij} - Z'_{ji} = \frac{\left(I_{ij}\mathrm{e}^{\mathrm{j}\delta_i} + I_{ji}\mathrm{j}^{\mathrm{j}\delta_j}\right)\left(U_i\mathrm{e}^{\mathrm{j}\theta_i} - U_j\mathrm{e}^{\mathrm{j}\theta_j}\right)}{I_{ij}I_{ji}\mathrm{e}^{\mathrm{j}\left(\delta_i+\delta_j\right)}}. \tag{16}$$

Combining $I_{ij} \approx I_{ji}$, $U_i \approx U_j$, and **Eq. 14–16**, it is obtained that

$$\Delta d_{ij} = \arg\left(\frac{\mathrm{e}^{\mathrm{j}a_i} - \mathrm{e}^{\mathrm{j}\left(\theta_j-\theta_i\right)}}{1 - \mathrm{e}^{\mathrm{j}\left(\theta_j-\theta_i\right)}}\right). \tag{17}$$

It is shown from **Eq. 17** that the error of phase angle is relative to the degree of the attacks in power systems. Considering **Eq. 17**, the recognition criteria of the nodes is written as follows:

$$\frac{\left|d_{ij}^t - d_{ij}^{t-1}\right| - \mu_{\mathrm{his}}}{\sigma_{\mathrm{his}}^2} \geq \tau_2, \tag{18}$$

where $d_{ij}^t - d_{ij}^{t-1}$ is the error between the adjacent d_{ij} in the sampling; μ_{his} and σ_{his} are the mathematical expectation and standard deviation of the historical data, respectively; and τ_2 is the detection threshold of attacks.

By detecting the nodes in power systems, the vector of nodes $M = [m_i]_{1\times n}$ is obtained, where m_i is the per unit of the power in node i.

Remark 2: $A = \left[a_{ij}\right]_{n\times n}$ is the matrix of lines in power systems. a_{ij} is the per unit of the line from node i to node j. When power systems are attacked, detection of the lines is as follows:

1) If $\dot{U}_i = \dot{U}_j$ and $a_{ij}(t) \neq a_{ij}(t-1)$, short circuit occurs in the line between node i and node j.
2) If $\dot{I}_{ij} = \dot{I}_{ji} = 0$ and $a_{ij}(t) \neq a_{ij}(t-1)$, open circuit occurs in the line between node i and node j.

3.2 Detection of Cyberattacks

In this part, the algorithm is established to detect the cyberattacks. When the communication lines that are connected to cyber and power systems are not attacked, the communication vector of the nodes $M^x = [m_i^x]_{1\times n}$ and the communication matrix of the lines $A^x = \left[a_{ij}^x\right]_{n\times n}$ are detected. In the case of attacked cyber nodes, the detection algorithm of cyber attacks is shown as Algorithm 1.

Remark 3:

1) Based on the concept of residual, a detection model is proposed in power systems. Therefore, the detected physical attacks are the attacks that damage the power equipment of the nodes and lines.
2) In cyber systems, based on the mechanism for transmitting sensitive encrypted data, a detection algorithm is established. Therefore, the detected cyberattacks are denial-of-service (DoS) attacks (Li et al., 2018), including synchronizing attacks and teardrop attacks.

Algorithm 1: Detection algorithm of attacked cyber nodes.

```
Input: Vector of power nodes: $M = [m_i]_{1\times n}$;
Cyber-physical cryptographic function: $f(m_i)$.
Output: Vector of cyber nodes: $N = [n_i]_{1\times k}$.
Initialize $i = 1$ and $j = 1$;
$m_i$ is sent from the power nodes to the cyber nodes only once.
if Communication line returns 0 then
    Communication line is attacked communication lines.
else
    if Communication line returns $f(m_i)$ then
        Cyber nodes are non-attacked cyber nodes.
        Communication line is non-attacked communication lines.
    else
        Cyber nodes are attacked cyber nodes.
        Communication line is non-attacked communication lines.
    Update $i$ and $j$ by;
```

4 ISLANDED CYBER–PHYSICAL POWER SYSTEMS

ICPPSs are divided into the non-attacked and the repaired parts. In **Section 3**, the non-attacked parts are marked. Since some attacked parts are repaired faster than others, ICPPSs consist of the non-attacked and the faster repaired parts. The updated ICPPSs consist of the old ICPPSs and the repaired parts.

Remark 4: The model of ICPPSs is obtained under the following assumptions (Zeng and Hui, 2015; Wu et al., 2018):

1) Repair important loads. The important power generation nodes are repaired to support the power consumption.
2) Establish the balance between supply and consumption. The nodes and lines of ICPPSs work steadily.

4.1 Constraints of Power Systems

The power nodes are selected as the power of supply and consumption. The power lines are selected as the power of transmission. As in remark 4, the group is limited by the power production of nodes or the power transmission of lines. Hence, the constraints of the islanded power systems are established.

4.1.1 Constraint of Power

When power reductions occur, the supplied power is reduced by switching off the supplied power. But the consumptive power is not reduced when the supplied power is reduced. Thus, the power constraint satisfies

$$\sum_{i=1}^{N} P_{i,con} \le \sum_{i=1}^{M} P_{i,sup}, \tag{19}$$

$$\sum_{i=1}^{N} Q_{i,con} \le \sum_{i=1}^{M} Q_{i,sup}, \tag{20}$$

where $P_{i,con}$ is the consumptive active power in node i, $P_{i,\,\mathrm{sup}}$ is the supplied active power in node i, N is the number of the consumptive power nodes, $Q_{i,con}$ is the consumptive reactive power in node i, $Q_{i,\,\mathrm{sup}}$ is the supplied reactive power in node i, N is the number of the consumptive power nodes, and M is the number of the supplied power nodes.

4.1.2 Constraint of Voltage

Quality of power is denoted by voltage of the nodes. Thus, the voltage satisfies

$$U_{b\min} \le U_b \le U_{b\max}, \tag{21}$$

where U_b, $U_{b\min}$, and $U_{b\max}$ are the voltage, the lowest voltage, and the highest voltage of node b, respectively.

4.2 Constraints of Cyber Systems

The islanded cyber systems are composed of cyber nodes and lines that are selected. The group is limited by the utilization of the CPU of the nodes or the bandwidth of the lines. Hence, the constraints of the islanded cyber systems are obtained.

4.2.1 Constraint of the Utilization About the CPU

Communication data are calculated simultaneously by the CPU. When the utilization of the CPU becomes maximum, with the addition of communication data, the data get stuck. The capacity of the nodes, which is the utilization of the CPU, satisfies

$$D_i \le \sum_{l=1}^{C} D_{i,l}, \tag{22}$$

where D_i is the size of running memory in node i, $D_{i,l}$ is the size of the communication signal from line l in node i, and C is the number of the lines connected to node i.

4.2.2 Constraint of Band Width

The communication signal of the lines is limited by bandwidth Friedberg et al. (2017). Thus, the constraint of bandwidth is

$$C_l \le C_{l,\max}, \tag{23}$$

where C_l and $I_{l,\,\max}$ are the size of communication data and the bandwidth of line l, respectively.

4.3 Solution Algorithm

If ICPPSs work normally, the lines satisfy the definition of trees in a circuit. Since islanded power systems and islanded cyber systems influence each other, it is difficult to define the weight of nodes and lines. Therefore, the Kruskal algorithm (Rachmawati et al., 2020) and the Prim algorithm (Sanaullah et al., 2020) cannot be used. Based on constraints, the enumeration algorithm of ICPPSs is established as Algorithm 2.

In this work, $F = (N, L)$ is the aggregate with the nodes and lines, N is the aggregate with the non-attacked nodes and the resilient nodes, and L is the aggregate with the non-attacked lines and the resilient lines. **Equations 19–23** are the constraints of the algorithm in ICPPSs. First, the topology of ICPPSs is constructed by using the enumeration method. Then, the parameters of ICPPSs are calculated by **Eqs 1–10**. If the calculated parameters satisfy **Eqs 19–23**, the topology is added into the aggregation of ICPPSs. If not, the topology is updated.

Algorithm 2: Solution algorithm of ICPPSs.

```
Input: Aggregate with the nodes : $F = (N,\Phi)$;
Number of the nodes : n.
Output: Aggregate with the nodes and lines : $F = (N,L)$.
Initialize : $x = 1$ & $y = 1$ & $i = x$ & $j = y$ ;$i \neq j$;
The line $l_{ij}$ is selected.
if $i$ and $j$ belong to $N$ & $L < n-1$ then
    $l_{ij}$ is added to $L$.
else
    if $i$ and $j$ do not belong to $N$ & $L < n-1$ then
        Update $i$ and $j$ by;
    else
        The parameters of $F = (N,L)$ are calculated by Eq. 1-10 in Section II.
        if $F = (N,L)$ satisfies the constraints of Eq. 19-23 then
            Output $F = (N,L)$
        else
            Update $F = (N,\Phi)$
        Update $i$ and $j$ by;
    Update $x$ and $y$ by;
```

5 OPTIMIZATION

Since the solution of ICPPSs is an aggregation, **Section 4** satisfies the constraints of **Eqs 19–23**. In **Section 5**, the power systems and cyber systems of ICPPSs are optimized individually. With the state coefficient and **Eqs 32–34**, cooperative optimization of physical and cyber systems is one where the power systems and cyber systems of ICPPSs are optimized cooperatively after individual optimization.

For the same attacks, the repair time is not reduced by extra human and material resources. Therefore, to save resilient resources, the resilient resources are optimized individually in islanded power and cyber systems by **Eqs 24**, **28**. In this study, ICPPSs are built for retaining the functions of CPPSs in a resilient process. The functions are reflected by the power of CPPSs. Therefore, considering the interplay between islanded power and cyber systems, they are optimized cooperatively for the power by **Eq. 31**.

5.1 Individual Optimization

In ICPPSs, the local optimum is composed of the optimization of the islanded power systems and the cyber systems.

5.1.1 Optimization of Islanded Power Systems

When CPPSs are attacked, islanded power systems are repaired by the power-resilient resources. Hence, in islanded power systems, the resilient resources are optimized by calculating the resilient nodes' power and the resilient lines' length.

In islanded power systems, the resilient resources are optimized. Thus, the objective function is described as follows:

$$\min Z_1 = \min \sum_{i\in N} c_i P_i t_i + \sum_{j\in L} c_j l_j t_j, \tag{24}$$

where c_i is the resilient resources in per unit power, P_i is the active power of the resilient nodes, t_i and t_j are the resilient time, c_j is the resilient resources in per unit length, and l_j is the length of the resilient lines.

When nodes of power generation are attacked, output power of the node satisfies

$$P_{i,r} \geq \max\left\{S_i \Delta T_i, P_{i,\min}\right\}, \tag{25}$$

$$P_{i,r} \leq \min\left\{S_i \Delta T_i, P_{i,\max}\right\}, \tag{26}$$

where $P_{i,r}$ is the resilient output power of node i, R_g is the resilient speed of active power, ΔT_i is the resilient duration, $P_{g,\min}^{G}$ is the lowest active output power, and $P_{g,\max}^{G}$ is the highest active output power.

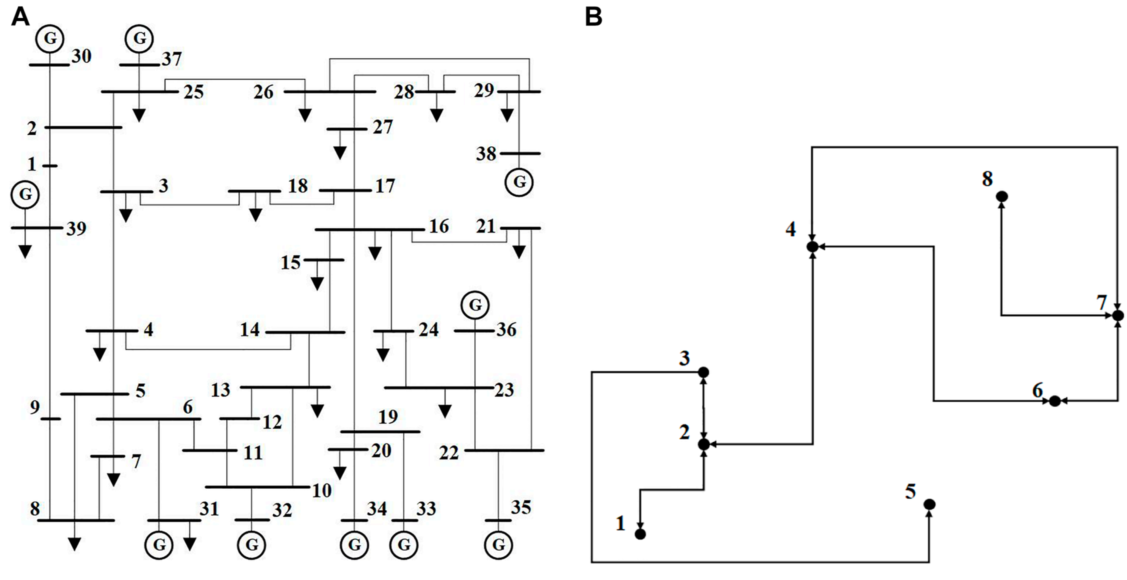

FIGURE 2 | Test cyber–physical power systems. **(A)** Power grid. **(B)** Cyber systems.

TABLE 1 | Cyber nodes connected to the power nodes.

Cyber node	Power node	Cyber node	Power node
1	1, 2, 3, 30, 37, 39	5	4, 5, 6, 7, 8, 9
2	15, 18, 25, 26	6	11, 12, 13, 14, 31
3	17, 27,28	7	10, 20, 32, 33, 34
4	16, 21, 29, 38	8	19, 22, 23, 24, 35, 36

The resilient time of lines is affected by the nodes. If the nodes connected to the lines are attacked, the resilience of the power lines will wait until the power nodes connected to the power lines are repaired. Thus, the resilient time of the lines satisfies

$$t_j \geq \sum_{i \in N_j} \Delta T_i, \tag{27}$$

where t_j is the resilient time of the power lines, ΔT_i is the resilient duration of the power nodes, and N_i is the set of the power nodes connected to the resilient line.

5.1.2 Optimization of Islanded Cyber Systems

In islanded cyber systems, the running memory of nodes and the bandwidth of lines are important. Thus, the resilient resources are optimized by calculating the resilient nodes' running memory and the resilient lines' bandwidth.

In islanded cyber systems, the resilient resources are optimized. Thus, the objective function is

$$\min Z_2 = \min \sum_{i \in N'} c_i' C_i' t_i' + \sum_{j \in L'} c_j' B_j' t_j', \tag{28}$$

where c_i' is the resilient resource in per unit capacity, C_i' is the capacity of running memory in the resilient nodes, t_i' and t_j' are the resilient time, c_j' is the resilient resources in per unit bandwidth, B_j' is the bandwidth of the resilient lines, and N' is the set of the resilient cyber nodes.

To avoid islanded power systems being influenced by cyberattacks, the power nodes connected to the cyber nodes are repaired after repairing the cyber nodes. Thus, the constraint of resilient time of cyber nodes is given as follows:

$$t_{i,r} \leq \min \sum_{j \in N_i'} \{t_j\}, \qquad \forall i \in N', \tag{29}$$

where $t_{i,r}$ is the resilient time of the power nodes and N_i' is the set of the cyber nodes connected to the power nodes.

Since the lines do not work before the nodes are repaired. To improve the utilization of the resilient resources, the resilience of the cyber lines will wait until the cyber nodes are repaired. Thus, the constraint of resilient time of cyber lines is

$$t_j' \geq \sum_{i \in N'} \Delta T_i', \tag{30}$$

where t_j' is the resilient time of the cyber lines and $\Delta T_i'$ is the resilient duration of the cyber nodes.

5.2 Cooperative Optimization

In this part, based on the local optimum of the islanded power systems and the cyber systems, ICPPSs are optimized cooperatively.

To balance the resilient resources of islanded power and cyber systems, the objective function of cooperative optimization is selected as follows:

$$\max P = \max \sum_{i \in M, j \in M'} x_i y_j P_i, \tag{31}$$

where P is all active power of ICPPSs, M is the set of the power nodes in ICPPSs, and M is the set of the cyber nodes in ICPPSs. The state coefficient of the power nodes x_i and the state coefficient of the cyber nodes y_j in **Eq. 21** are set to the following form:

$$x_i = \begin{cases} 1, \text{non} - \text{attacked or repaired} \\ 0, \text{attacked} \end{cases}$$
$$y_i = \begin{cases} 1, \text{non} - \text{attacked or repaired} \\ 0, \text{attacked} \end{cases}$$

The resilient resources are limited. Thus, constraints of the cooperative resilience is

$$W = Z_1 + Z_2 \leq W_{\max}, \tag{32}$$

$$Z_1 \geq Z_{1,\min}, \tag{33}$$

$$Z_2 \geq Z_{2,\min}, \tag{34}$$

where W is the cooperative resilient resources, $W_{\max}$ is the highest resources, $Z_{1,\min}$ is the lowest resources in islanded power systems, and $Z_{2,\min}$ is the lowest resources in islanded cyber systems.

6 SIMULATIONS

In this part, cooperative resilience is demonstrated with hybrid attacks. The simulation test platform is built in the MATLAB environment. All results are implemented on a computer with Intel(R) Core(TM) i5-10210U and @1.60 GHz with 16.0 GB of RAM. This test system consists of a 39-bus power system and an 8-node cyber system, and its topology and communication are shown in **Figure 2** and **Table 1**. The communication mode adopted in this study is the point-to-point mode. In this study, the attacked nodes and lines are repaired. The repair sequence is determined by optimal dynamic topology.

In this section, hybrid attacks are shown in **Table 2**. The cooperative dynamic resilient strategy is shown in **Table 3**. The cooperative dynamic resilient topology is shown in **Figure 3**.In **Figure 3**, communication distance is the distance between repeaters and data centers. Considering **Eqs 25–27** and **Eqs 29, 30**, at first, attacked cyber nodes are repaired in attacked parts. Since more power is supplied by the power nodes, they are linked with cyber node 5. To satisfy **Eq. 31**, in **Figure 3A**, the first step is performed. Then, in **Figure 3B**, the second step is performed. With the repair of the cyber nodes 5 and 8, **Eqs 25–27** and **Eq. 30** are considered in the next step. To satisfy **Eq. 31**,

TABLE 2 | Attacked parts of hybrid attacks.

Attacked power node	Attacked power line	Attacked cyber node	Attacked cyber line
2, 3, 6, 10, 14, 17, 19, 25,28, 36	4, 17, 28, 36	5, 8	5, 8

TABLE 3 | Dynamic resilience under hybrid attacks.

Dynamic topology	Repaired power node	Repaired power line	Repaired cyber node	Repaired cyber line
First step	6	–	5	–
Second step	19, 36	–	8	–
Third step	14, 17, 28, 25	36	–	3
Last step	2, 3, 10	4, 17, 28	–	6

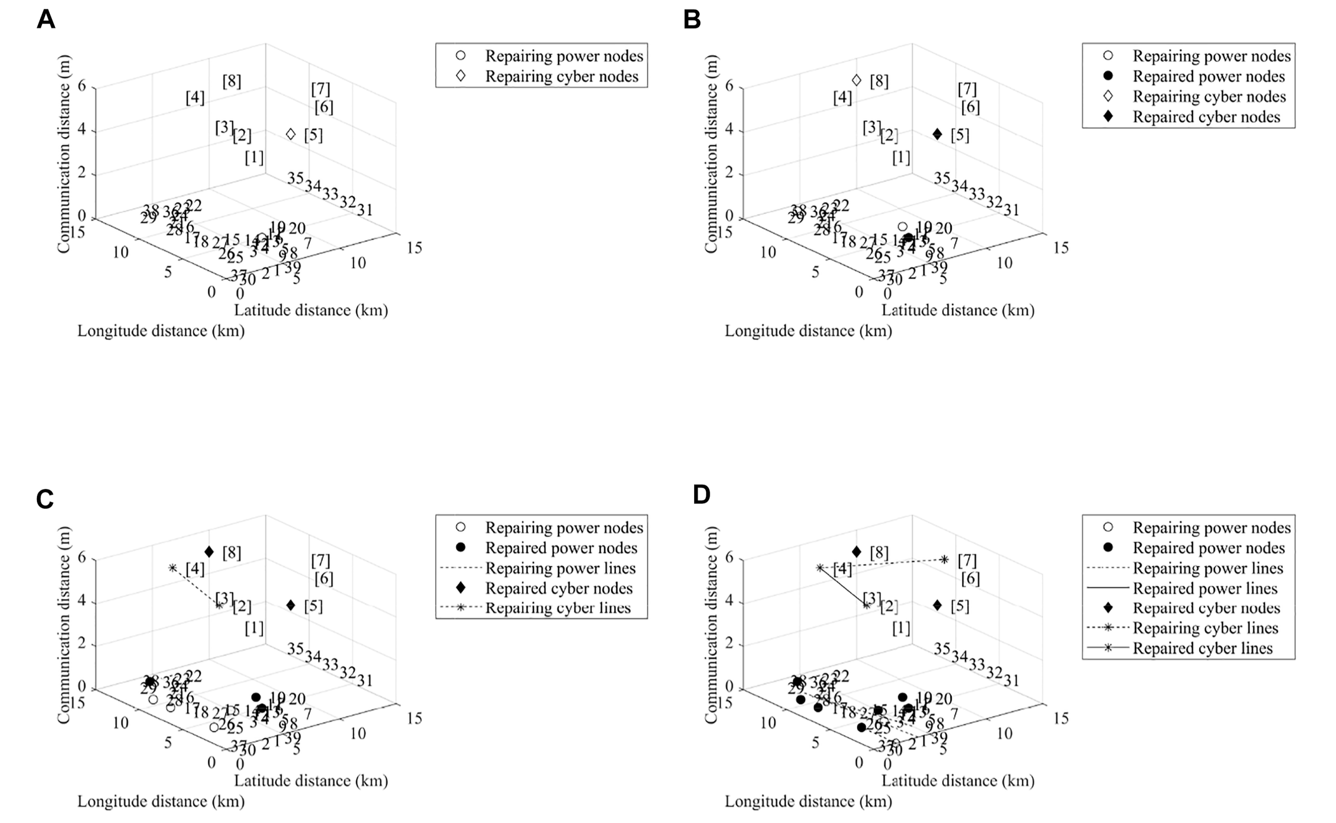

FIGURE 3 | Dynamic topology of ICPPSs under hybrid attacks. **(A)** First resilient step. **(B)** Second resilient step. **(C)** Third resilient step. **(D)** Last resilient step.

TABLE 4 | Resilient resources of dynamic resilient strategy and (Li et al., 2019) under hybrid attacks.

Dynamic topology	Human resource	Material resource	Total resource
First step	1941.57	1948.28	3889.85
Second step	1965.89	1922.52	3888.41
Third step	1862.52	1812.43	3674.95
Last step	1756.80	1341.65	3098.45
Sum	7526.77	7024.87	14551.65
Li et al. (2019)	12048.53	10884.22	22932.75
Error	60.08%	54.94%	57.60%

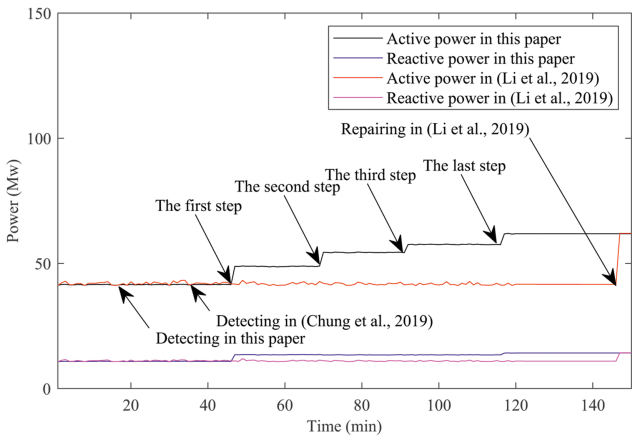

FIGURE 4 | Repaired active power and reactive power of ICPPSs under hybrid attacks.

in **Figure 3C**, the third step is performed. Then, in **Figure 3D**, the last step is performed. To verify the effectiveness of the detecting speed, the cooperative dynamic resilient strategy is compared with Chung et al. (2019) in detecting time. To verify the effectiveness of the resilient speed, the cooperative dynamic resilient strategy is compared with Li et al. (2019) in resilient time. The repaired active power and reactive power are shown in **Figure 4**.

Compared with Chung et al. (2019), where the attacks were detected many times, physical attacks and cyberattacks are detected once by using **Eqs 12–18** and Algorithm 1 in this study. Therefore, in **Figure 4**, hybrid attacks are detected faster with the proposed method, and the distribution of resilient resources is optimized by **Eq. 24**, **Eq. 28**, and **Eqs 32–34**. With the optimized distribution, the repair time is reduced. Thus, it is seen from **Figure 4** that CPPSs are repaired faster with the proposed method.

To verify the effectiveness of cooperative resilience, the resilient resources are compared with those of the dynamic resilient strategy and those used in Li et al. (2019). Based on the optimization model in **Section 5**, the resilient resources are shown in **Table 4**.

It is shown from **Table 4** that the resilient resources of the proposed method are lower than (Li et al., 2019) those in human, material, and total resources. Therefore, under hybrid attacks, the effectiveness of the dynamic resilient resources is verified.

7 CONCLUSION

This study has proposed a dynamic strategy for cooperative resilience in CPPSs, which reduces the power shortage and saves resilient resources. It is noted that only one kind of hybrid attack is considered in this work. In power systems, particularly critical infrastructure grids, cascading faults are a common phenomenon after the attacks (Wang et al., 2017). The secure control of the networked complex system is actuated after the occurrence of faults (Jin et al., 2021). In the future, these will be further considered.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

JJ and YL participated in the conception and design of the study. JJ organized the database. PL performed the simulation analysis. JJ wrote the first draft of the manuscript. JJ, YL, and MC revised sections of the manuscript. All authors contributed to manuscript revision, read, and approved the submitted version.

FUNDING

This research is supported by the National Natural Science Foundation of China (NFSC, Grant Nos. 61803253 and 61973209).

ACKNOWLEDGMENTS

The authors gratefully acknowledge the support from the National Natural Science Foundation of China (NFSC, Grant Nos. 61803253 and 61973209).

REFERENCES

Amoretti, M., and Ferrari, G. (2013). Investigating the Resilience of Unstructured Supernode Networks. *IEEE Commun. Lett.* 17, 1272–1275. doi:10.1109/LCOMM.2013.043013.130305

Chen, Y., Qi, D., Dong, H., Li, C., Li, Z., and Zhang, J. (2021). A Fdi Attack-Resilient Distributed Secondary Control Strategy for Islanded Microgrids. *IEEE Trans. Smart Grid.* 12, 1929–1938. doi:10.1109/TSG.2020.3047949

Chung, H.-M., Li, W.-T., Yuen, C., Chung, W.-H., Zhang, Y., and Wen, C.-K. (2019). Local Cyber-Physical Attack for Masking Line Outage and Topology Attack in Smart Grid. *IEEE Trans. Smart Grid.* 10, 4577–4588. doi:10.1109/tsg.2018.2865316

Deng, C., Wang, Y., Wen, C., Xu, Y., and Lin, P. (2021). Distributed Resilient Control for Energy Storage Systems in Cyber-Physical Microgrids. *IEEE Trans. Ind. Inf.* 17, 1331–1341. doi:10.1109/TII.2020.2981549

Ding, T., Qu, M., Wu, X., Qin, B., Yang, Y., and Blaabjerg, F. (2020). Defense Strategy for Resilient Shipboard Power Systems Considering Sequential Attacks. *IEEE Trans.Inform.Forensic Secur.* 15, 3443–3453. doi:10.1109/TIFS.2019.2960657

Dong, L., and Xu, H. (2020). "Adaptive Fuzzy Detector-Based Secure Correct Control for Cyber-Physical Systems Subject to Heterogeneous Physical Attacks," in 2020 39th Chinese Control Conference (CCC), 7632–7636. doi:10.23919/CCC50068.2020.9188577

Dyer J. Dyer M. Xu J. (2019). Practical Homomorphic Encryption Over the Integers for Secure Computation in the Cloud. *Int. J. Inf. Security* 18, 549–579. doi:10.1007/s10207-019-00427-0

Fan Z. Yang Z. Yu J. Xie K. Yang G. (2021). Minimize Linearization Error of Power Flow Model Based on Optimal Selection of Variable Space. *IEEE Trans. Power Syst.* 36, 1130–1140. doi:10.1109/TPWRS.2020.3012894

Franzè, G., Tedesco, F., and Lucia, W. (2019). Resilient Control for Cyber-Physical Systems Subject to Replay Attacks. *IEEE Control. Syst. Lett.* 3, 984–989. doi:10.1109/LCSYS.2019.2920507

Friedberg, I., Hong, X., Mclaughlin, K., Smith, P., and Miller, P. C. (2017). Evidential Network Modeling for Cyber-Physical System State Inference. *IEEE Access.* 5, 17149–17164. doi:10.1109/ACCESS.2017.2718498

Guo, X., Bao, H., Xiao, J., and Chen, S. (2021). A Solution of Interval Power Flow Considering Correlation of Wind Power. *IEEE Access.* 9, 78915–78924. doi:10.1109/ACCESS.2021.3051745

Hu, Z., Liu, S., Luo, W., and Wu, L. (2021). Intrusion-detector-dependent Distributed Economic Model Predictive Control for Load Frequency Regulation with Pevs under Cyber Attacks. *IEEE Trans. Circuits Syst.* 68, 3857–3868. doi:10.1109/TCSI.2021.3089770

Hu, Z., Liu, S., Luo, W., and Wu, L. (2022). Resilient Distributed Fuzzy Load Frequency Regulation for Power Systems under Cross-Layer Random Denial-Of-Service Attacks. *IEEE Trans. Cybern.* 52, 2396–2406. doi:10.1109/TCYB.2020.3005283

Huang, B., Li, Y., Zhan, F., Sun, Q., and Zhang, H. (2022). A Distributed Robust Economic Dispatch Strategy for Integrated Energy System Considering Cyber-Attacks. *IEEE Trans. Ind. Inf.* 18, 880–890. doi:10.1109/TII.2021.3077509

Huang, G., Wang, J., Chen, C., Qi, J., and Guo, C. (2017). Integration of Preventive and Emergency Responses for Power Grid Resilience Enhancement. *IEEE Trans. Power Syst.* 32, 4451–4463. doi:10.1109/TPWRS.2017.2685640

Jin, X., Lu, S., and Yu, J. (2021). Adaptive Nn-Based Consensus for a Class of Nonlinear Multiagent Systems with Actuator Faults and Faulty Networks. *IEEE Trans. Neural Netw. Learn. Syst.*, 1–13. doi:10.1109/tnnls.2021.3053112

Kshetri, N., and Voas, J. (2017). Hacking Power Grids: A Current Problem. *Computer.* 50, 91–95. doi:10.1109/MC.2017.4451203

Li, J., Abbas, W., and Koutsoukos, X. (2020). Resilient Distributed Diffusion in Networks with Adversaries. *IEEE Trans. Signal. Inf. Process. Over Networks.* 6, 1–17. doi:10.1109/TSIPN.2019.2957731

Li, J., You, H., Qi, J., Kong, M., Zhang, S., and Zhang, H. (2019). Stratified Optimization Strategy Used for Restoration with Photovoltaic-Battery Energy Storage Systems as Black-Start Resources. *IEEE Access.* 7, 127339–127352. doi:10.1109/ACCESS.2019.2937833

Li, P., Liu, Y., Xin, H., and Jiang, X. (2018). A Robust Distributed Economic Dispatch Strategy of Virtual Power Plant under Cyber-Attacks. *IEEE Trans. Ind. Inf.* 14, 4343–4352. doi:10.1109/TII.2017.2788868

Liu, J., Yang, M., Tian, E., Cao, J., and Fei, S. (2019). Event-based Security Control for State-dependent Uncertain Systems under Hybrid-Attacks and its Application to Electronic Circuits. *IEEE Trans. Circuits Syst.* 66, 4817–4828. doi:10.1109/TCSI.2019.2930572

Mousavinejad, E., Ge, X., Han, Q.-L., Yang, F., and Vlacic, L. (2021). Resilient Tracking Control of Networked Control Systems under Cyber Attacks. *IEEE Trans. Cybern.* 51, 2107–2119. doi:10.1109/TCYB.2019.2948427

Qi, H., Wang, X., Tolbert, L. M., Li, F., Peng, F. Z., Ning, P., et al. (2011). A Resilient Real-Time System Design for a Secure and Reconfigurable Power Grid. *IEEE Trans. Smart Grid.* 2, 770–781. doi:10.1109/TSG.2011.2159819

Quirce, A., Rosado, A., Díez, J., Pérez-Serrano, A., Tijero, J. M. G., Valle, A., et al. (2020). "Nonlinear Dynamics of Optical Frequency combs Generated by Gain-Switched Semiconductor Lasers Subject to Optical Injection," in 2020 22nd International Conference on Transparent Optical Networks (ICTON), 1–4. doi:10.1109/ICTON51198.2020.9203266

Rachmawati, D., Herriyance, , and Putra Pakpahan, F. Y. (2020). "Comparative Analysis of the Kruskal and Boruvka Algorithms in Solving Minimum Spanning Tree on Complete Graph," in 2020 International Conference on Data Science, Artificial Intelligence, and Business Analytics (DATABIA), 55–62. doi:10.1109/DATABIA50434.2020.9190504

Sahoo, S., Dragicevic, T., and Blaabjerg, F. (2020). An Event-Driven Resilient Control Strategy for Dc Microgrids. *IEEE Trans. Power Electron.* 35, 13714–13724. doi:10.1109/TPEL.2020.2995584

Sanaullah, K., Xia, M., Hussain, M., Hussain, S., and Tahir, A. (2020). Optimal Islanding for Restoration of Power Distribution System Using Prim's MST Algorithm. *Csee Jpes.* 8, 599–608. doi:10.17775/CSEEJPES.2020.01580

Viveros, A., and Lopez-Pires, F. (2021). "Placement of Cpu-Intensive Virtual Machines in High Resource Utilization Cloud Datacenters. An Economical Revenue Maximization Analysis," in 2021 IEEE URUCON, 325–328. doi:10.1109/URUCON53396.2021.9647221

Wang, M., Lu, W., Wu, S., Zhao, C., Feng, Y., Luo, C., et al. (2017). "Vulnerability Assessment Model of Power Grid Cascading Failures Based on Fault Chain and Dynamic Fault Tree," in 2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), 1279–1284. doi:10.1109/CYBER.2017.8446361

Wu, G., Sun, J., and Chen, J. (2018). Optimal Data Injection Attacks in Cyber-Physical Systems. *IEEE Trans. Cybern.* 48, 3302–3312. doi:10.1109/TCYB.2018.2846365

Wu, Y., Xu, M., Zheng, N., and He, X. (2020). Event-triggered Resilient Consensus for Multi-Agent Networks under Deception Attacks. *IEEE Access.* 8, 78121–78129. doi:10.1109/ACCESS.2020.2989743

Yuan, Y., Yuan, H., Ho, D. W. C., and Guo, L. (2020). Resilient Control of Wireless Networked Control System under Denial-Of-Service Attacks: A Cross-Layer Design Approach. *IEEE Trans. Cybern.* 50, 48–60. doi:10.1109/TCYB.2018.2863689

Zeng, X., and Hui, Q. (2015). Energy-event-triggered Hybrid Supervisory Control for Cyber-Physical Network Systems. *IEEE Trans. Automat. Contr.* 60, 3083–3088. doi:10.1109/TAC.2015.2409900

Zhang, H., Yue, D., Dou, C., Xie, X., Li, K., and Hancke, G. P. (2021). Resilient Optimal Defensive Strategy of TSK Fuzzy-Model-Based Microgrids' System via a Novel Reinforcement Learning Approach. *IEEE Trans. Neural Netw. Learn. Syst.* 1, 1. doi:10.1109/TNNLS.2021.3105668

Zhou, Q., Shahidehpour, M., Alabdulwahab, A., and Abusorrah, A. (2020). A Cyber-Attack Resilient Distributed Control Strategy in Islanded Microgrids. *IEEE Trans. Smart Grid.* 11, 3690–3701. doi:10.1109/TSG.2020.2979160

Zhou, S., Wang, M., Wang, J., Yang, M., and Dong, X. (2020). Time-process Power Flow Calculation Considering thermal Behavior of Transmission Components. *IEEE Trans. Power Syst.* 35, 4232–4250. doi:10.1109/TPWRS.2020.2987945

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.