frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 08 April 2024
DOI 10.3389/fenrg.2024.1382887

OPEN ACCESS

EDITED BY
Ki Il Kim,
Chungnam National University, Republic of Korea

REVIEWED BY
Nishant Kumar,
Indian Institute of Technology Jodhpur, India
Neeraj Kumar Singh,
HCL Technologies, India

*CORRESPONDENCE
Hong Fan,
✉ fanhong@shiep.edu.cn

RECEIVED 06 February 2024
ACCEPTED 07 March 2024
PUBLISHED 08 April 2024

CITATION
Fan H, Huang X, Wang D and Zhou B (2024), Communication network robust routing optimization in an integrated energy cyber–physical system based on a random denial-of-service attack.
Front. Energy Res. 12:1382887.
doi: 10.3389/fenrg.2024.1382887

Communication network robust routing optimization in an integrated energy cyber–physical system based on a random denial-of-service attack

Hong Fan[1]*, Xu Huang[1], Diwei Wang[1] and Boyang Zhou[2]

[1]Electric Power Engineering, Shanghai University of Electric Power, Shanghai, China, [2]Research Center on High-Productivity Computing Systems, Zhejiang Lab, Hangzhou, China

The integration of power grids and communication networks in smart grids enhances system safety and reliability but also exposes vulnerabilities to network attacks, such as Denial-of-Service (DoS) attacks targeting communication networks. A multi-index evaluation approach is proposed to optimize routing modes in integrated energy cyber-physical systems (IECPS) considering potential failures from attacks. Security and economic service evaluation indexes are incorporated to quantify the significance of information flow routing. An optimization model for electric, heat, and gas routing in worst-case scenarios is formulated and solved using a column and constraint generation algorithm. The optimized routing method effectively circumvents specified attack areas, reducing the correlation degree of communication links within the attack area. Comparison with single-service optimization methods demonstrates the superiority of the proposed approach in mitigating the impact of network attacks on IECPS. The study highlights the importance of considering security and economic factors in optimizing routing modes to enhance the resilience of integrated energy cyber-physical systems against network attacks, particularly DoS attacks on communication networks. The evaluation index approach presented in this study provides a comprehensive method for assessing the importance of communication links in IECPS and optimizing routing modes to improve system robustness and reliability in the face of network attacks.

KEYWORDS

smart grid, integrated energy cyber–physical system, communication network optimization, denial-of-service attack, routing optimization

1 Introduction

In the process of smart grid development, the communication network plays an increasingly important role. The evolution of cyber–physical power systems (CPPSs) is also moving toward a more integrated direction, enhancing the security and reliability of the overall system (Popat et al., 2021). However, the coupling of communication networks with the grid can introduce additional risks, potentially resulting in serious consequences (Siu et al., 2022; Solanki et al., 2022). One such risk is the superposition of risks caused by the interference of a communication network with the transmission of information. This interference can lead to the occupation of routing bandwidth, ultimately affecting the generation of control commands and subsequently impacting the system frequency. This interference, known as a denial-of-service (DoS) attack, poses a significant threat to the stability and functionality of the system (Hu et al., 2020). To mitigate the harm caused by DoS attacks and improve the overall stability of the system, extensive research has been conducted in various countries (Hu et al., 2020; Gupta et al., 2021; Kakadiya et al., 2022). This research focuses on enhancing the security control of communication systems, implementing routing load-balancing strategies for communication networks, and improving communication performance.

Numerous studies have been conducted on communication network security and network attacks, particularly in the context of CPPSs. Security control is a widely adopted strategy to counter network attacks in CPPSs (Dai et al., 2023; Wang et al., 2023). This strategy can be implemented through three main approaches: stochastic system approach, game theory approach (Li et al., 2017), and resilient control approach (Franze et al., 2020). Security control methods are effective in safeguarding system stability. However, designing control systems that can effectively handle DoS attacks in different scenarios can be challenging as these attacks often require specific corrections. For instance, in the case of an asynchronous DoS attack affecting two channels, even a lower attack frequency than that in a synchronous DoS attack can result in a prolonged failure of control signal updates (Li et al., 2023). For the integrated energy cyber–physical system (IECPS), the state under the DoS attack is estimated to be difficult to carry out as well. In such scenarios, the commonly used brake strategy in control system designs may not be sufficient to ensure timely updates of control signals (Lv et al., 2023). In addition, the impact on routers in a DoS attack is actually more non-negligible. Communication delays and data loss can affect the robustness of security controls (Wang et al., 2023). Consequently, the performance of the system may be compromised. This calls for a redesign of the active security control approach to address specific challenges (Li et al., 2021). Kumar et al. (2020) provided an optimal control technique that mitigates oscillations under steady-state conditions and slow response under dynamically changing conditions. Kumari et al. (2023), Saxena et al. (2021), and Kumar et al. (2019) took into account the impact of the dynamic environment on its basis. Kumar et al. (2023), on the other hand, employed a model control scheme without voltage sensors to predict the operating state of the system afterward and improve the response speed in the face of attacks.

Compared to designing security control methods, information flow scheduling from the perspective of communication networks is a more efficient and economical approach. Given the interdependence between the communication network and the power grid, it is crucial to improve the performance of the CPPS when facing chain-coupled failures caused by network attacks. This requires the establishment of a reliable and optimal information delivery path, which can be achieved through an effective routing method that minimizes risk.

In a communication network, each communication path typically exhibits varying communication performance and reliability. The task of selecting the optimal communication path for service information flow, based on specific objectives, is known as a routing optimization problem (Karamdel et al., 2022; Kong and Jiang, 2022; Li et al., 2022). This problem can be further divided into routing balance optimization (Hammoudeh and Newman, 2015; Cai et al., 2022) and communication performance optimization (Du et al., 2022), depending on the optimization goals. To address the issue of load imbalance on certain communication links and nodes resulting from the shortest routing, Zhang et al. (2019) proposed a load-balancing optimization method for power communication networks. This method optimizes the routing approach to reduce the load imbalance on communication links, thus achieving a more reasonable distribution of service information flow and alleviating the communication burden on highly loaded links. Zhao et al. (2021) proposed a decentralized load frequency control method for dealing with the impact of cyberattacks on networked power systems. The method combines game theory and optimization algorithms with an optimization analysis of a high percentage of renewable power systems. Considering the shared risk inherent in the laying of fiber optic links in communication networks, Li et al. (2014) developed a routing optimization model for power communication networks that incorporates risk balance. By integrating the importance of different services, the routing method can be optimized to reduce the average risk associated with each communication service. For enhancing the communication performance of the network, Ti et al. (2022) developed a reliable routing optimization model for power communication networks that takes into account communication delay constraints, routing hop count constraints, and reliability constraints. This model aims to reduce the congestion of communication nodes by optimizing routing, thereby achieving a more efficient allocation of node communication resources.

Indeed, the existing approaches mentioned above do not fully consider the interdependence between energy and communication networks, even though initial faults in the communication network can aggravate grid-side faults. To address this issue, a solution was proposed by Kong (2019) that focuses on optimizing power-disjoint communication routes between power nodes and control centers. This approach aims to prevent the propagation of initial faults and mitigate inter-network cascading failures. Based on this work, Kong (2020) further investigated the power supply dependency of routers in the routing optimization process. They developed a communication routing failure probability model and quantified the impact of routing failures in terms of load loss. Zhang et al. (2022) modeled the dependence of communication and physical networks and further analyzed the effect of coupling relationships on chain failures. By optimizing the routing approach, they aimed to minimize the amount of load loss triggered by initial routing failures. However, it is important to note that these methods have only been verified in single-energy power grids. In the context of current multi-energy systems, which exhibit direct interdependence between energy and communication networks, the challenges posed by network risks are even more complex. Multi-energy systems, such as the IECPS, introduce additional complexity due to the presence of multiple energy flow nodes (Pazouki et al., 2021; Ding et al., 2022). Using a single control service to accurately capture the importance of such systems becomes challenging (Soltan et al., 2019). Recent security incidents in the IECPS, such as the cyberattack on the Ukrainian power grid in 2015, highlight the potential for substantial losses when control servers of underlying generators and substations are compromised. This emphasizes the need for research on cyber security in integrated energy systems, expanding the scope of the CPPS to include the IECPS, and developing modeling and optimization methods specific to the IECPS. With the increasing integration of electric, heat, and gas networks, responsible for the conversion, transmission, and data communication of heterogeneous energy flow across different regions, cyberattacks on the IECPS can have wide-ranging and profound impacts. Therefore, it is crucial to focus on the cyber security of integrated energy systems, conduct research on IECPS modeling and optimization, and prioritize these areas in national energy security strategies.

Currently, there is limited literature available on the study of the IECPS under the context of cyberattacks. Furthermore, there is no research on optimizing IECPS communication networks, specifically considering DoS attacks. Therefore, this paper aims to address the following challenges in establishing optimal routing for the IECPS: first, there is a need for a routing protocol that takes into account the interdependencies between different networks within the IECPS. It should minimize the negative impact that may arise when the optimal routing approach of the communication network does not align with the optimal routing approach of the power system. Second, there is a need for a multi-service importance evaluation method that considers the diverse energy networks present in the IECPS. This method should appropriately assess the importance of different energy networks within the system. Taking these challenges into account, based on previous research (Ti et al., 2022), this paper explores the robust optimization of routing under DoS attack scenarios in the communication network of an integrated energy system that consists of electric, heat, and gas energy. The key contributions of this paper are as follows:

1. Proposing an evaluation index for the importance of a dual-service routing method that takes into account the safety and economy of an integrated energy system that includes three forms of energy.
2. Establishing a robust optimization model for IECPS routing including electric, heat, and gas energy with the objective of minimizing the correlation degree of operations in the high-risk area of stochastic DoS attacks.
3. Utilizing the column and constraint generation algorithm to solve the optimization problem with the objective of minimizing service correlation in high-risk areas. Based on the degree of associated operations, it proves to be superior to traditional single-service optimization methods.

The remainder of this paper is organized as follows: Section 2 introduces the concept of the IECPS and its layers; Section 3 proposes an importance evaluation index of routing methods considering dual services; Section 4 presents an IECPS communication network routing robust optimization method; the simulation results are analyzed in Section 5; and finally, the conclusion of this work is summarized in Section 6.

2 IECPS communication network modeling

2.1 Basic concepts of the IECPS

The overall framework of the IECPS is shown in Figure 1, which is composed of electricity, heat, and gas energy. From the functional level, it can be divided into the energy layer, transmission layer, and information layer.

2.2 Communication network and routing modeling

The transmission layer in the IECPS is mainly composed of a communication network responsible for the production control and information management of electric, heat, and gas energy. The communication network includes communication substations and communication links. For power communication network modeling, Xin et al. (2015) and Li et al. (2020) abstracted the multi-dimensional and multi-level information network as a directed graph composed of data nodes and network branches. The data node represents the dataset of input and output information of various modules in the power system, while the directed branch represents the processing and transmission process of information. According to the theory, it abstracts the communication network in the IECPS into a directed graph G composed of nodes and branches: G = $\left(v_c \cup v_s \cup v_e \cup v_h \cup v_g, e_c \cup e_s \cup e_e \cup e_h \cup e_g\right)$.

In order to describe the topological relationship between communication substations and communication links in the IECPS communication network, the adjacency matrix of the communication network is defined as A_G. A_G is a $M_c + M_s + M_e + M_h + M_g$ order matrix. Its rows and columns are arranged in the order of *c*, *s*, *e*, *h*, and *g*. The corresponding element is represented as

$$A_{G,ij} = \begin{cases} 0 & (i,j) \notin e_k \\ 1 & (i,j) \in e_k \end{cases} \tag{1}$$

where the corresponding element is 1, which means that there is a communication link between the two substation nodes; otherwise, it means that there is no communication link between the two station nodes.

The adjacency matrix A_G reflects the topology of the communication link in the IECPS communication network. When the information layer processes a certain service, the information flow flows along a certain path in the communication link, which constitutes the routing method of the information flow. As shown in Figure 2, only the flow of information flow at the communication network level is considered, and the control center and router are mapped on the same plane for analysis. Since a certain service may have multiple information flows, such as the load control service that simultaneously reduces the load of multiple nodes, and the routing methods are diverse, in order to clearly represent the multiple routing methods of a certain service information flow and consider

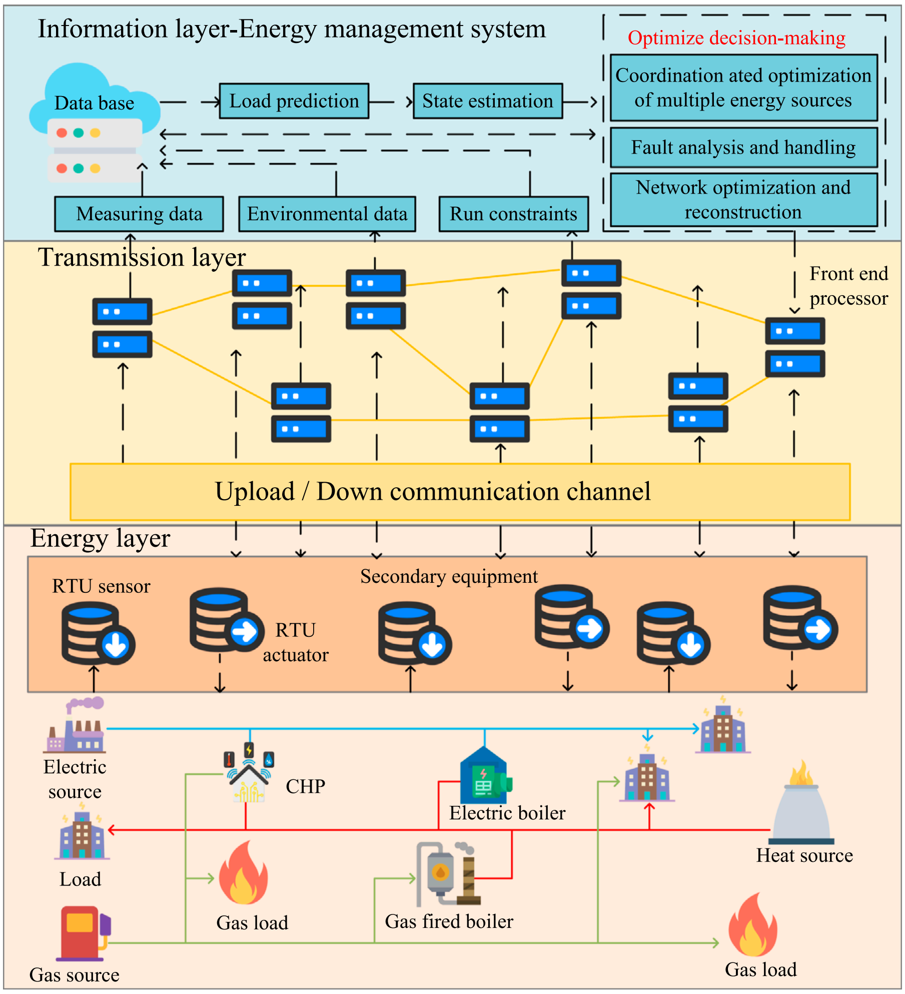


FIGURE 1
ntegrated energy cyber–physical system (IECPS) overall architecture.

the primary and backup routing methods of the information flow, the primary and backup routes of the service information flow are defined as matrices X_{kq} and Y_{kq}, whose structure is similar to the adjacency matrix A_G, and the corresponding elements are expressed as

$$X_{kq,ij} = \begin{cases} 0 & q \text{ } does \text{ } not \text{ } flow \text{ } through \text{ } i-j \\ 1 & q \text{ } flow \text{ } through \text{ } i-j \end{cases} \tag{2}$$

$$Y_{kq,ij} = \begin{cases} 0 & q \text{ } does \text{ } not \text{ } flow \text{ } through \text{ } i-j \\ 1 & q \text{ } flow \text{ } through \text{ } i-j \end{cases} \tag{3}$$

where $k(=1,2,3\cdots N)$ represents different information layer services and N is the total number of services. $q(=1,2,3\cdots D)$ indicates the different information flows of service k. D is the total number of information flows of service k. $X_{kq,ij}$ is an element of the main routing matrix. If the information flow q of service k does not pass through links i–j, then the corresponding element of this matrix is 0; conversely, the element is 1.

3 The importance evaluation index of the routing mode considering dual services

3.1 Importance index of information flow

The state of information flow is closely related to the safety and economy of IECPS operation. However, different information flows have different influences on the safety and economy of IECPS operation, which involves three different importance factors: 1) the importance of different business information flows; 2) the importance of different information flows in the same business; and 3) the importance of different routing methods. There is a one-to-many relationship between the information flow and routing mode. When the information layer optimization decision function is fixed and the communication link is normal and free from damage and interference, the importance of certain information flow is also fixed. However, the same information flow corresponds to many different

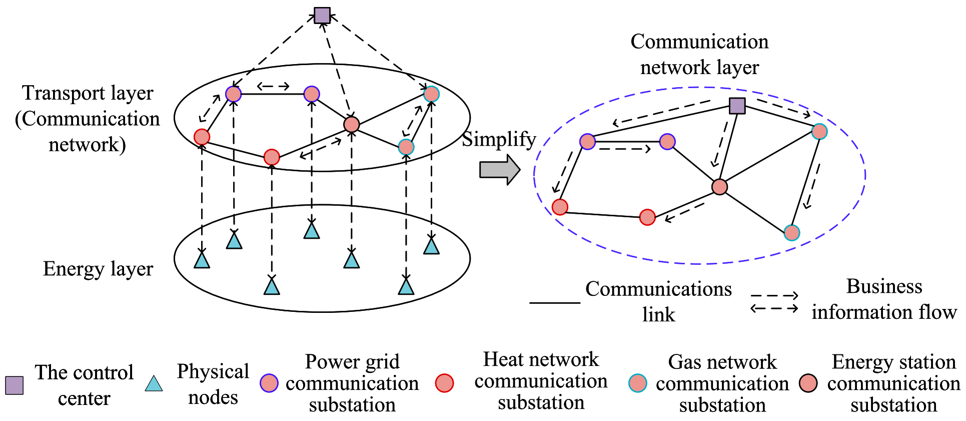


FIGURE 2
Simple IECPS communication network routing.

routing modes, and the way to assign information flows to more important and reliable links or choose a reliable routing method for information flows is the key issue of IECPS routing optimization, while determining the importance of information flows and routing methods is the pre-requisite for routing optimization. In order to evaluate the importance of information flow, the importance index of substation information flow q of service k is defined as

$$I_{kq} = \begin{cases} \sum_{s\in S}\delta_s\left(\omega_e L_e^{sq} + \omega_h L_h^{sq} + \omega_g L_g^{sq}\right) & k = l \\ \sum_{s\in S}\delta_s\left(\left|C_e^{sq} - C_e^{sq'}\right| + \left|C_h^{sq} - C_h^{sq'}\right|\right. & \\ \qquad\left. + \left|C_g^{sq} - C_g^{sq'}\right| + \left|C_s^{sq} - C_s^{sq'}\right|\right) & k = d. \end{cases} \tag{4}$$

It should be noted that since the substations, except the substations of the energy station, correspond to only one form of energy, the load reduction and nodal operating cost of the other energy forms involved in the calculation of I_{kq} in this case should be 0.

The importance index of information flow I_{kq} quantitatively indicates the importance of information flow q of service k in terms of the loss of IECPS operational safety and economy caused by physical side failures. For the load control service, the load reduction of energy network nodes corresponding to different substation information flows under different failure scenarios is different, and the sum of the load reduction penalty costs of energy network nodes corresponding to information flows q in each fault scenario is taken as the importance index of substation information flows q. For economic dispatch business, the operating cost of energy network nodes corresponding to different substation information flows in different fault scenarios is different from that of nodes under load control business. The sum of the absolute difference values of the operating costs of energy network nodes corresponding to information flow q in each fault scenario under two businesses is taken as the importance index of information flow q.

3.2 Importance index of communication links

The route of information flow is composed of communication links in the communication network, and different service information flows can flow through the same communication link. In Eq.5, on the basis of the evaluation index of the information flow importance defined above, considering the joint action of the load control business and economic dispatch business, the communication link correlation business degree matrix E is defined, and the mathematical expression is expressed as

$$E = \frac{\alpha}{\alpha+\beta}\sum_{s\in S}\delta_s\sum_{q=1}^{N_{lq}}\left[I_{lq}\left(X_{lq} + Y_{lq} + \left(X_{lq} + Y_{lq}\right)^T\right)\right] + \frac{\beta}{\alpha+\beta}\sum_{s\in S}\delta_s\sum_{q=1}^{N_{dq}}\left[I_{dq}\left(X_{dq} + Y_{dq} + \left(X_{dq} + Y_{dq}\right)^T\right)\right]. \tag{5}$$

In Eq. 5, α and β are the importance of load control service and economic dispatch service, respectively. Table 1 shows the "DDD" communication network planning report of the State Grid Corporation of China, which shows that α and β can be 0.94 and 0.62, respectively.

4 IECPS communication network routing robust optimization modeling

4.1 Worst-DoS attack scenario modeling

The following assumptions are made for the worst-case DoS attack scenario: the attacker will try to make the attack traffic exceed the total bandwidth, causing a service outage; the attack point location is the node with the most information flow through the shortest routing method; and the duration of the attack is limited by a linear function of time. For any $t \geq t_0 \geq 0$, there exist τ_0 and $1 > \zeta > 0$ satisfying

$$\Xi_{(t_0,t)} \leq \tau_0 + \zeta\left(t - t_0\right). \tag{6}$$

TABLE 1 Importance of different communication services.

Type	Business name	Basic bandwidth/(Mbit/s)	Importance degree
1	500-kV/220-kV relay protection service	8	0.99
2	Scheduling automation and wide-area phase measurement	16	0.62
3	Video monitoring, conferencing, and protection information management	100	0.29
4	Office automation, executive telephony, and cloud terminal application business	150	0.13

The substation will lose its communication ability, and the link directly connected to the substation will fail to complete the data transmission task after being attacked by DoS. The link fault matrix under the set of DoS attack fault Φ can be defined as $F_{Dos,k}$; when any substation k is attacked by DoS, $F_{Dos,k}$ can be expressed as

$$F_{Dos,k} = A_G \odot A_{k0}, k \in \Phi \in v_k. \tag{7}$$

The operation state of the communication link is reflected by the link fault matrix $F_{Dos,k}$; if substation k is attacked by DoS, the element of $F_{Dos,k}$ related to the link associated with substation k is 1, indicating that the link has lost its communication ability.

When the active and standby routes of the traffic information flow do not work due to the loss of the communication ability of the link caused by DoS attacks, the traffic flow is interrupted. In order to judge whether two types of service flows are interrupted, r_{lq} and r_{dq} are defined as the interruption discriminant variables of information flow q of load control service and economic dispatching service, respectively:

$$r_{lq} = \sum_{(i,j)\in e_k} \left(X_{lq} \odot F_{Dos,k}\right)_{(i,j)} \cdot \sum_{(i,j)\in e_k} \left(Y_{lq} \odot F_{Dos,k}\right)_{(i,j)}, \quad k \in \Phi \in v_k \tag{8}$$

$$r_{dq} = \sum_{(i,j)\in e_k} \left(X_{dq} \odot F_{Dos,k}\right)_{(i,j)} \cdot \sum_{(i,j)\in e_k} \left(Y_{dq} \odot F_{Dos,k}\right)_{(i,j)}. \quad k \in \Phi \in v_k \tag{9}$$

According to Eqs 8, 9, r_{lq} and r_{dq} are 0–1 discriminant variables. When the value of r_l or r_d is 0, it indicates that the service information flow is not interrupted. Otherwise, it indicates that the service information flow is interrupted. The impact of the DoS attack on communication substation k on the two types of service information flows may be different, and there are several possibilities, i.e.,

$$r_{lq} \cdot r_{dq} = \begin{cases} 0 \begin{cases} r_{lq} = 1 \& r_{dq} = 0, \text{Load control service} \\ \text{information flow is interrupted} \\ r_{lq} = 0 \& r_{dq} = 1, \text{Economic dispatching} \\ \text{service information flow is interrupted} \\ r_{lq} = 0 \& r_{dq} = 0, \text{Two service information} \\ \text{flows are not interrupted} \end{cases} \\ 1, \text{Two service information} \\ \quad \text{flows are interrupted.} \end{cases} \tag{10}$$

In addition, DoS attacks on communication substation k will cause a communication interruption of multiple links, which may cause the interruption of multiple service information flows. So, the worst DoS attack scenario will occur under the interruption of multiple information flows, and the worst scenario under the fault set Φ of DoS attacks on a certain area of the communication network is

$$\max_{\Phi} \left(\sum_{q=1}^{N_{lq}} r_{lq} I_{lq} + \sum_{q=1}^{N_{dq}} r_{dq} I_{dq} \right). \tag{11}$$

It is worth noting that the attack frequency and attack duration are major influencing factors that reflect the DoS attacks.

4.2 Routing optimization modeling

The routing robust optimization problem of the IECPS communication network in the worst scenario of DoS attacks to improve the resilience of the IECPS in extreme scenarios is considered in this paper. The routing robust optimization problem aims to optimize the information flow routing mode of load control services and economic dispatching services so as to minimize the degree of associated services in high-risk areas of DoS attacks. The objective function is shown as follows:

$$\min_{\substack{x_{lq,ij}, y_{lq,ij} \\ x_{dq,ij}, y_{dq,ij}}} \left[\delta \sum_{q=1}^{N_{lq}} I_{lq} \sum_{(i,j)\in e_k} \left(x_{lq,ij} + \chi y_{lq,ij}\right) + \delta \sum_{q=1}^{N_{dq}} I_{dq} \sum_{(i,j)\in e_k} \left(x_{dq,ij} + \chi y_{dq,ij}\right) + \max_{\Phi} \left(\sum_{q=1}^{N_{lq}} r_{lq} I_{lq} + \sum_{q=1}^{N_{dq}} r_{dq} I_{dq} \right) \right]. \tag{12}$$

The decision variables of the objective function are $x_{lq,ij}$, $y_{lq,ij}$, $x_{dq,ij}$, and $y_{dq,ij}$ that determine the information flow q of the load control service and economic dispatch service. In addition, the number of information flows of load control service is different from that of economic dispatch service. Economic dispatch service only dispatches electric, heat, and gas source nodes, while load control service controls not only each load node but also electric, heat, gas, and energy station nodes. Therefore, the number of information flows of load control service is greater than that of economic dispatch service, and its corresponding decision variables are more. In Eq. (12), δ and χ are both minuteness used to set the priority of the optimization objective. The smaller δ makes the optimized routingmethod first meet the communication network resilience under the worst attack scenario and then reduces the associated traffic degree of the routing method. The smaller χ makes the optimized primary route meet the above objectives more preferentially than the standby route.

In order to ensure the rationality and effectiveness of the optimized active and standby routing methods, the above robust routing optimization problem should meet the following constraints.

4.2.1 Communication network topology constraints

$$\begin{cases} \sum\limits_{j:(s^q,j)\in e_k} x_{lq,s^qj} - \sum\limits_{j:(j,s^q)\in e_k} x_{lq,js^q=1} \quad \forall q \\ \sum\limits_{j:(t^q,j)\in e_k} x_{lq,t^qj} - \sum\limits_{j:(j,t^q)\in e_k} x_{lq,jt^q=-1} \quad \forall q \\ \sum\limits_{\substack{j:(i,j)\in e_k \\ i\neq s^q,t^q}} x_{lq,ij} - \sum\limits_{\substack{j:(j,i)\in e_k \\ i\neq s^q,t^q}} x_{lq,ji=0} \quad \forall q \end{cases} \tag{13}$$

$$\begin{cases} \sum\limits_{j:(s^q,j)\in e_k} x_{dq,s^qj} - \sum\limits_{j:(j,s^q)\in e_k} x_{dq,js^q=1} \quad \forall q \\ \sum\limits_{j:(t^q,j)\in e_k} x_{dq,t^qj} - \sum\limits_{j:(j,t^q)\in e_k} x_{dq,jt^q=-1} \quad \forall q \\ \sum\limits_{\substack{j:(i,j)\in e_k \\ i\neq s^q,t^q}} x_{dq,ij} - \sum\limits_{\substack{j:(j,i)\in e_k \\ i\neq s^q,t^q}} x_{dq,ji=0} \quad \forall q \end{cases} \tag{14}$$

$$\begin{cases} \sum\limits_{j:(s^q,j)\in e_k} y_{lq,s^qj} - \sum\limits_{j:(j,s^q)\in e_k} y_{lq,js^q=1} \quad \forall q \\ \sum\limits_{j:(t^q,j)\in e_k} y_{lq,t^qj} - \sum\limits_{j:(j,t^q)\in e_k} y_{lq,jt^q=-1} \quad \forall q \\ \sum\limits_{\substack{j:(i,j)\in e_k \\ i\neq s^q,t^q}} y_{lq,ij} - \sum\limits_{\substack{j:(j,i)\in e_k \\ i\neq s^q,t^q}} y_{lq,ji=0} \quad \forall q \end{cases} \tag{15}$$

$$\begin{cases} \sum\limits_{j:(s^q,j)\in e_k} y_{dq,s^qj} - \sum\limits_{j:(j,s^q)\in e_k} y_{dq,js^q=1} \quad \forall q \\ \sum\limits_{j:(t^q,j)\in e_k} y_{dq,t^qj} - \sum\limits_{j:(j,t^q)\in e_k} y_{dq,jt^q=-1} \quad \forall q \\ \sum\limits_{\substack{j:(i,j)\in e_k \\ i\neq s^q,t^q}} y_{dq,ij} - \sum\limits_{\substack{j:(j,i)\in e_k \\ i\neq s^q,t^q}} y_{dq,ji=0} \quad \forall q \end{cases} \tag{16}$$

Eqs 13 and 14 refer to the topology constraints of the source node, end node, and intermediate node in the main routing method of the load control service and economic dispatching service information flow, respectively. The formulas in brackets represent the restrictions on the information flow in and out of the source node, end node, and intermediate node in the routing method, i.e., the source node can only outflow information, the end node can only receive information, and the intermediate node can both send and receive information. Eqs 15 and 16 are the topology constraints of the source node, terminal node, and intermediate node in the information flow backup routing mode of load control service and economic dispatching service, respectively.

4.2.2 Active and standby route non-coincidence constraints

In order to prevent the failure of all the active and standby routing methods due to the failure of a communication link, the active and standby routing methods of information flow q are required to have no overlapping links. The restrictions on the active and standby routing methods of two types of traffic flows are as follows:

$$\begin{cases} x_{lq,ij} + y_{lq,ij} \leq 1 \\ x_{dq,ij} + y_{dq,ij} \leq 1 \end{cases} \tag{17}$$

4.2.3 Attack result identification constraints

The discriminant equation for two types of service information flow interruption is shown in Eqs 8–10. However, the discriminant constraint is nonlinear, which is not convenient for solving the subsequent robust optimization problem, so it needs to be linearized into a linear constraint. Rewriting Eqs 8, 9 yields

$$r_{lq} = r_{lq,x} \cdot r_{lq,y}, \tag{18}$$

$$r_{dq} = r_{dq,x} \cdot r_{dq,y}. \tag{19}$$

The linearization results of Eqs 10 and Eq 18,19 can be obtained as

$$r_{lq,x} + r_{lq,y} - 1 \leq r_{lq} \leq \frac{r_{lq,x} + r_{lq,y}}{2}, \tag{20}$$

$$r_{dq,x} + r_{dq,y} - 1 \leq r_{dq} \leq \frac{r_{dq,x} + r_{dq,y}}{2}, \tag{21}$$

$$r_{lq} + r_{dq} - 1 \leq r_{ld} r_{dq} \leq \frac{r_{lq} + r_{dq}}{2}. \tag{22}$$

Eqs 20–22 correspond to the load control service information interruption constraint, economic dispatching service information flow interruption constraint, and both service information flow interruption constraints, respectively.

4.2.4 Communication link bandwidth constraints

The available communication optical path c_{ij} of the communication optical cable is limited, and the communication optical path occupied by the two kinds of service information flows when flowing through the same communication link should not be bigger than c_{ij}; it should meet the following requirements:

$$\sum_{q=1}^{N_{lq}} \left(x_{lq,ij} + y_{lq,ij} \right) + \sum_{q=1}^{N_{dq}} \left(x_{dq,ij} + y_{dq,ij} \right) \leq c_{ij}. \tag{23}$$

Thus, the communication network robust routing optimization (CNRRO) model can be expressed as

$$\begin{cases} \min\limits_{\substack{x_{lq,i,j}, y_{lq,jj} \\ x_{dq,ij}, y_{dq,j}}} \Bigg[\delta \sum\limits_{q=1}^{N_{lq}} I_{lq} \sum\limits_{(i,j)\in e_k} \left(x_{lq,ij} + \chi y_{lq,ij} \right) \\ \qquad + \delta \sum\limits_{q=1}^{N_{dq}} I_{dq} \sum\limits_{(i,j)\in e_k} \left(x_{dq,ij} + \chi y_{dq,ij} \right) \\ \qquad + \max_{\Phi} \left(\sum\limits_{q=1}^{N_{lq}} r_{lq} I_{lq} + \sum\limits_{q=1}^{N_{dq}} r_{dq} I_{dq} \right) \Bigg] \\ s.t\,(12)-(16),(19)-(22) \\ x_{lq,ij}, y_{lq,ij}, x_{dq,ij}, y_{dq,ij}, r_{dq,ij}, r_{lq,ij}, r_{dq,ij}, \\ r_{lq,ij} \in \{0,1\} \end{cases} \tag{24}$$

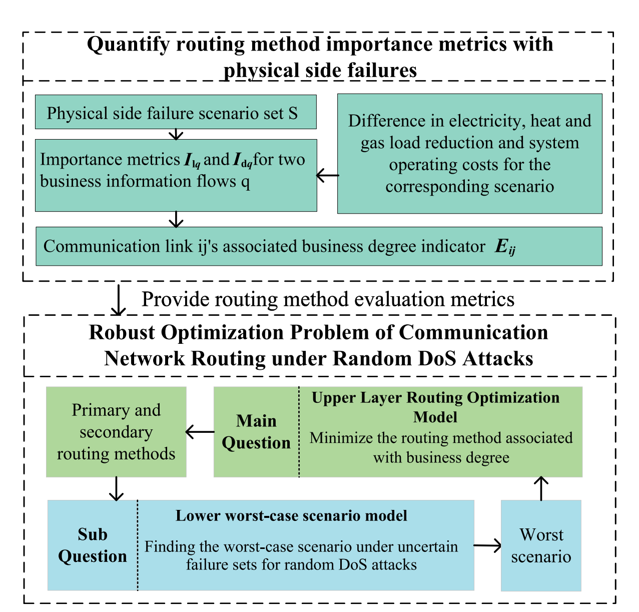

Quantify routing method importance metrics with physical side failures
Physical side failure scenario set S
Importance metrics I_{lq} and I_{dq} for two business information flows q
Difference in electricity, heat and gas load reduction and system operating costs for the corresponding scenario
Communication link ij's associated business degree indicator E_{ij}
Provide routing method evaluation metrics
Robust Optimization Problem of Communication Network Routing under Random DoS Attacks
Primary and secondary routing methods
Main Question
Upper Layer Routing Optimization Model
Minimize the routing method associated with business degree
Sub Question
Lower worst-case scenario model
Finding the worst-case scenario under uncertain failure sets for random DoS attacks
Worst scenario

FIGURE 3
ommunication network robust routing optimization (CNRRO) logical architecture.

CNRRO is a bi-level mixed-integer linear programming problem with an uncertainty set, which is a typical non-deterministic polynomial (NP)-hard problem, i.e., all uncertain polynomial problems can be reduced to polynomial time complexity. The logic architecture of the optimization problem is shown in Figure 3. The upper layer is the main problem of routing optimization for reducing the degree of traffic associated with communication links, and the lower layer is the optimization subproblem of the worst scenario for providing DoS attacks for the upper layer.

4.3 Solving method

As CNRRO is an NP-hard problem, the computational complexity increases with the increase in the number of communication network nodes. To reduce the computational complexity, the column and constraint generation (CCG) algorithm is used to solve the above model, and its principle is as follows: for convenience, the above model is expressed in standard form:

$$\min_{z\in\mathbb{C}} \boldsymbol{az} + \max_{u\in\Phi} \max_{g\in\mathbb{Q}(z,u)} \boldsymbol{bg}, \tag{25}$$

$$s.t\mathbb{C} = \{\boldsymbol{z} \in \mathbb{Z}^{m}:\ \ \boldsymbol{Gz} \geq c\}, \tag{26}$$

$$\Phi = \left\{\boldsymbol{u} \in \mathbb{R}^{n} \times \mathbb{Z}^{n'}:\ \ \boldsymbol{Hu} \leq \boldsymbol{d}\right\}, \tag{27}$$

$$\mathbb{Q}(\boldsymbol{z},\boldsymbol{u}) = \left\{g \in \mathbb{R}^{p}\text{:}\boldsymbol{Eg} \geq \boldsymbol{f} - \boldsymbol{Ru} - \boldsymbol{Dz}\right\}. \tag{28}$$

Eq. 26 corresponds to the communication network topology constraint (Eq. 13–14), Eq. 27 represents the uncertain fault set of the communication substation, and Eq. 28 represents the functional relationship among the internal decision variables and the external decision variables, as well as the uncertain variables, corresponding to the Eqs 20–22.

In order to solve the problem hierarchically and iteratively, the standard form of the routing robust optimization model is transformed into a main problem and a subproblem, as shown below.

Main problem:

$$\begin{cases} \min_{z,\rho} \boldsymbol{az} + \rho \\ s.t\boldsymbol{Gz} \geq \boldsymbol{c} \\ \rho \geq \boldsymbol{bg}^{l} \quad \forall 1 \leq l \leq k \\ \boldsymbol{Eg}^{l} \geq \boldsymbol{f} - \boldsymbol{Ru}_{l}^{*} - \boldsymbol{Dz} \quad \forall 1 \leq l \leq k \\ \boldsymbol{Hu}_{l}^{*} \leq \boldsymbol{d}\forall 1 \leq l \leq k \\ \boldsymbol{z} \in \mathbb{Z}, \rho \in \mathbb{R}, \boldsymbol{g}^{l} \in \mathbb{R} \quad \forall 1 \leq l \leq k \\ \boldsymbol{u}_{l}^{*} \in \mathbb{R} \times \mathbb{Z} \quad \forall 1 \leq l \leq k \end{cases} \tag{29}$$

Subproblem:

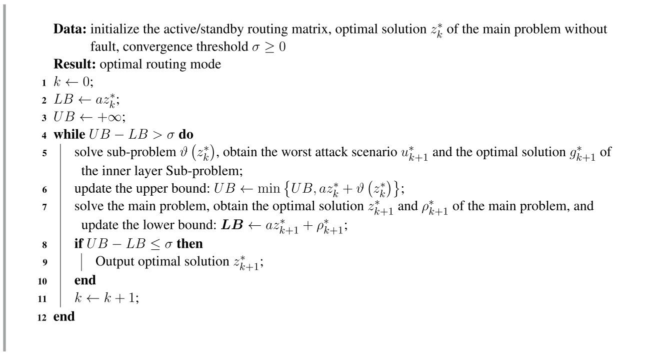
$$\begin{cases} \vartheta(z^{*}) = \max_{u\in\Phi} \max_{g} \boldsymbol{bg} \\ s.t\boldsymbol{Eg} \geq \boldsymbol{f} - \boldsymbol{Ru} - \boldsymbol{Dz}^{*} \\ \boldsymbol{Hu} \leq \boldsymbol{d} \\ \boldsymbol{g} \in \mathbb{R}, \boldsymbol{u} \in \mathbb{R} \times \mathbb{Z} \end{cases} \tag{30}$$

The decision variable $z*$ can minimize the degree of traffic associated with the communication link in the area subject to DoS attacks by solving the main problem and pass the optimal solution to the subproblem; then, the worst scenario u_{l}^{*} in the area subject to attacks can be obtained by solving the subproblem. The scenario is passed to the main problem and iterated repeatedly, so that the final obtained main and standby routing methods are robust, and the resilience to extreme scenarios is improved. The specific steps are as follows.

5 Case study

5.1 Original data

In this case, the IECPS consists of an energy network and communication network. The energy network is combined with an IEEE 30-bus power network, 14-bus heat network, and 20-bus gas network. The communication network contains 68 communication network nodes, i.e., 30 power grid communication substations,



```
Data: initialize the active/standby routing matrix, optimal solution $z_k^*$ of the main problem without
      fault, convergence threshold $\sigma \geq 0$
Result: optimal routing mode
$k \leftarrow 0$;
$LB \leftarrow az_k^*$;
$UB \leftarrow +\infty$;
while $UB - LB > \sigma$ do
    solve sub-problem $\vartheta\left(z_k^*\right)$, obtain the worst attack scenario $u_{k+1}^*$ and the optimal solution $g_{k+1}^*$ of
      the inner layer Sub-problem;
    update the upper bound: $UB \leftarrow \min\left\{UB, az_k^* + \vartheta\left(z_k^*\right)\right\}$;
    solve the main problem, obtain the optimal solution $z_{k+1}^*$ and $\rho_{k+1}^*$ of the main problem, and
      update the lower bound: $\boldsymbol{LB} \leftarrow az_{k+1}^* + \rho_{k+1}^*$;
    if $UB - LB \leq \sigma$ then
        Output optimal solution $z_{k+1}^*$;
    end
    $k \leftarrow k + 1$;
end
```

Algorithm 1. CCG algorithm flow.

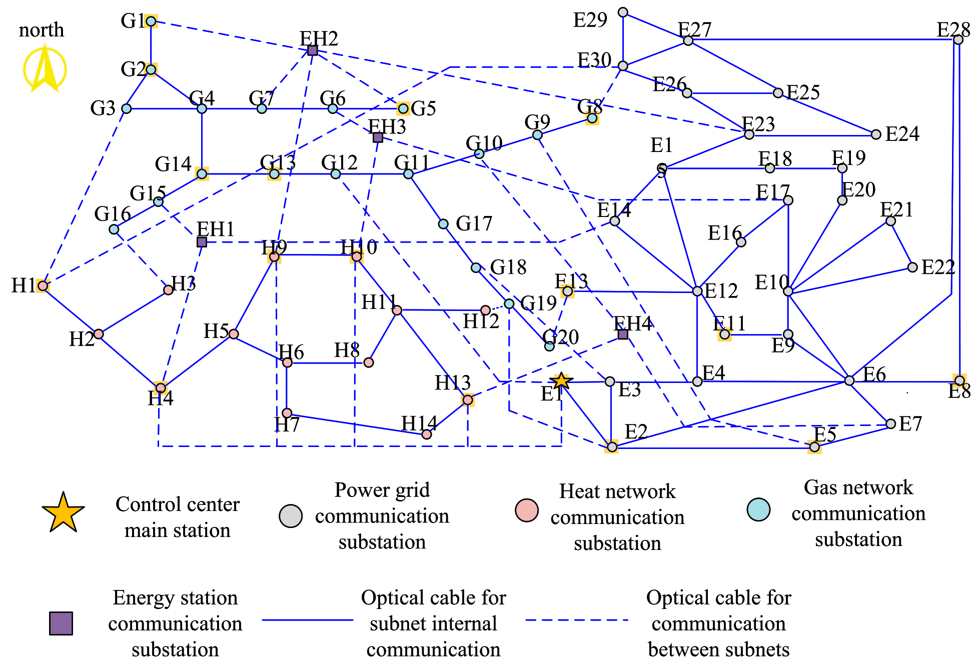

north
G1
G2
G3
G4
G7
G6
G5
EH2
EH3
G14
G13
G12
G11
G10
G9
G8
G15
G16
EH1
H9
H10
G17
G18
G19
G20
H1
H3
H2
H5
H6
H8
H11
H12
H13
H14
H7
H4
E29
E30
E27
E28
E26
E25
E24
E23
E1
E18
E19
E17
E20
E21
E14
E16
E22
E13
E12
E10
EH4
E11
E9
E4
E6
E8
E3
E7
E2
E5
Control center main station
Power grid communication substation
Heat network communication substation
Gas network communication substation
Energy station communication substation
Optical cable for subnet internal communication
Optical cable for communication between subnets

FIGURE 4
IECPS communication network topology.

20 gas network communication substations, 14 heat network communication substations, 4 energy station communication substations, and 1 control center main station. The specific parameters of the example system are detailed by Shabanpour-Haghighi and Seifi (2015), and its topological structure is shown in Figure 4. The parameters of the example are set as follows: the rated bandwidth of each fiber link is 200 Mbit/s, and the rated optical path is 20 m. The outage probability of the transmission line in the physical side fault concentration is 2%, and the outage probability of the heating pipeline and the gas supply pipeline is 1%. In CNRRO, the minuscule quantities δ and χ used to distinguish priorities are both 10^{-4}, and the convergence threshold σ of the CCG algorithm is also 10^{-4}.

5.2 Analysis of routing optimization results of the IECPS communication network

In order to verify the effectiveness of the IECPS routing robust optimization method proposed in this paper, the power grid part of the communication network, the heat network part of the communication network, and a certain area of the gas network part are taken as the target area of the DoS attack. All the communication substations in this area are exposed to the risk of the DoS attack. In this case, the communication link directly connected to the substation will temporarily lose its communication function. In addition, to reflect the optimization result more intuitively, assume that the link that is not directly connected to the substation in the attack area but passes through the attack area also exits the operation. In the scenario where the three areas are high-risk areas to be attacked, CNRRO is solved to optimize the routing mode of the IECPS economic dispatching service and load control service. For the convenience of comparison and optimization results, as shown in Figure 5, the former IECPS is optimized according to the shortest path to obtain the various substation economic dispatches of business information flow and information flow routing load control mode (due to the load control in the business and the corresponding electric source, heat source, and air source node flow routing with the economic operation business in the same way, it is no longer the picture). The attack areas listed in Table 2 are shown in the gray-shaded area in Figure 5. It can be seen that routing with the shortest path as the goal will cause a large number of service information flows to route through the high-risk areas and cannot avoid the risk of service interruption of the subsites and links caused by a random DoS attack.

1) Analysis of optimization results in scenario 1: The main route optimization results of the IECPS economic dispatching service and load control service under the DoS attack in the grid communication area are shown in Figure 5. According to the figure, the information flow of the two services of the optimized communication substation E8 reaches E8 through E2 and E6, thus bypassing high-risk area ϕ_e. The load control service information flow of substations E30, E29, E26, E24, E23, E20, E19, E18, E15, and E14 in the north of the communication network detours northward through the link on the east of the communication network (E8, E28) so as to avoid passing through the substations and links that may be attacked. It is worth noting that the load control service information of the two substations E17 and E16 after optimization is delivered by the link (EH3, E17) through the corresponding communication network of the heat network and gas network, because there is no safe path on the grid side to bypass to the target substation. Since area ϕ_e contains the communication substation node EH4 of the

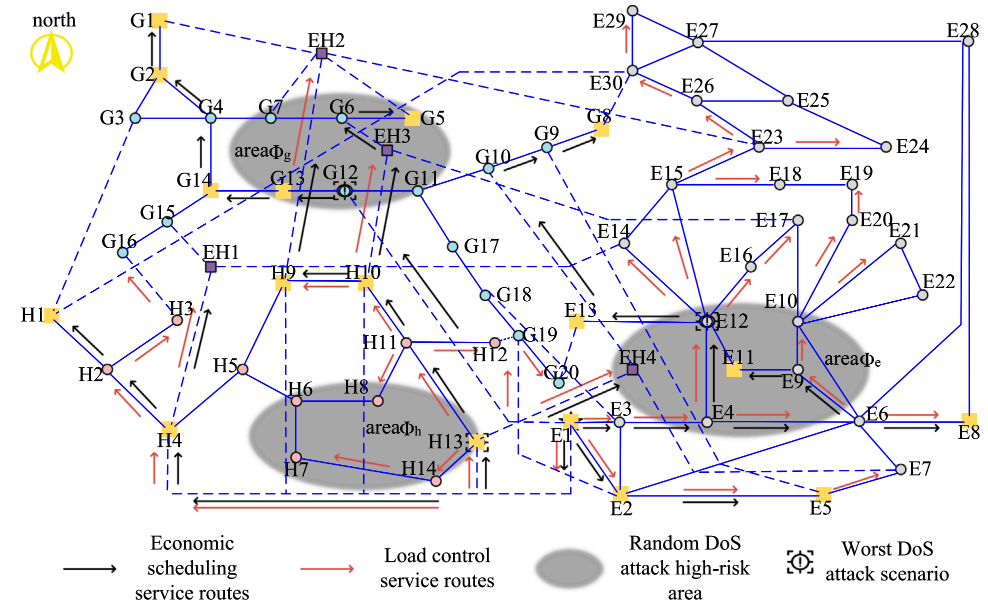


FIGURE 5
Routing method of IECPS service information flow based on the shortest path before optimization.

TABLE 2 DoS) attack area.

Target	Attack area		
	Section number	Affected substations	Affected link
Grid	ϕ_e	E4, E9, E10, E11, E12, and EH4	(E3, E4), (E4, E12), (H13, EH4), (EH4, E7), (G9, E5), (E13, E12), (E14, E12), (E15, E12), (E16, E12), (E11, E9), (E9, E10), (E17, E10), (E20, E10), (E21, E10), (E22, E10), (E9, E6), (E4, E6), (E10, E6), and (EH4, G10)
Heat supply network	ϕ_h	H6, H7, H8, H13, and H14	(H5, H6), (H6, H8), (H6, H7), (H13, H14), (H13, H11), (E1, H9), (E1, H10), and (H13, EH4)
Gas network	ϕ_g	G5, G6, G7, G11, G12, G13, and EH3	(G4, G7), (EH2, G7), (G7, G6), (G6, G5), (G11, G12), (G12, G13), (G13, G14), (EH3, G6), (H10, EH3), (EH3, E17), (H9, EH2), and (E1, G12)

energy station, the communication link (EH4, G10) is at high risk, which threatens the smooth instruction of the control center to the economic dispatching command of the gas network substation G8. However, the economic dispatching service information flow of the optimized gas network substation G8 departs to the west and transfers the information flow to the link (E1, G12). The link (EH4, G10) was successfully avoided. However, the figure shows that after optimization, the service information flow of the communication substations E12, E11, E10, and E21 still passes through the high-risk area, because all feasible paths pass through the high-risk area. What is different from the previous optimization is that the load control service flow of the optimized E12, E10, and E21 is delivered from the north of the high-risk area. Fewer high-risk links pass through. This is because fewer high-risk links are involved in a routing mode, and the associated services of high-risk areas are lower.

2) Optimization result analysis of scenario 2: The main route optimization results of the IECPS economic dispatching service and load control service under the DoS attack in the heat network communication area are shown in Figure 5. The figure shows that the information flow of load control service and economic dispatching service of EH2 and EH3 no longer passes through the link (H13, H11) after optimization. Instead, it is delivered by E3, G18, G19, H12, and H11, thus avoiding the possibility that the information flow is threatened by the DoS attack. The economic dispatching service information from the control center to G8 via

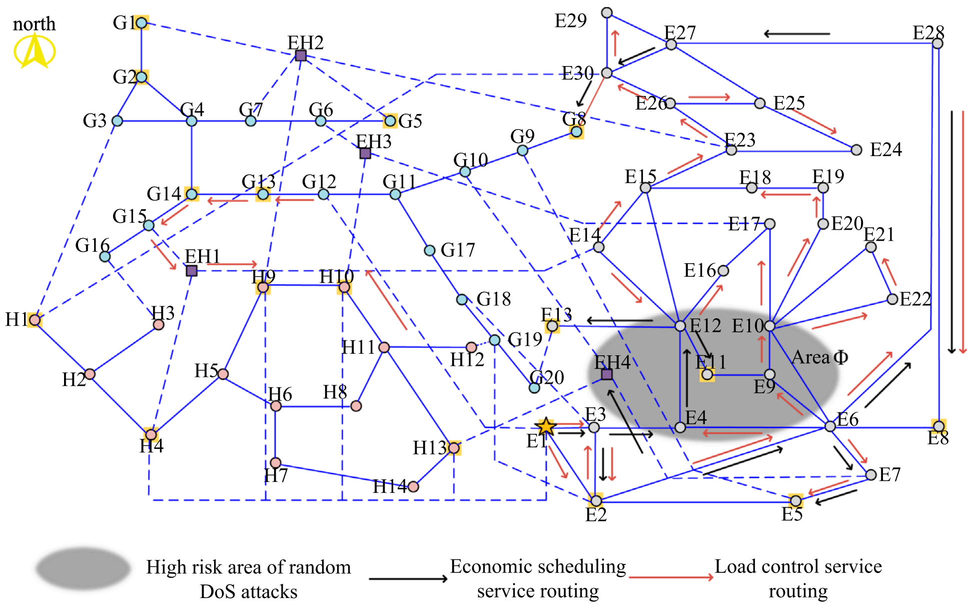


FIGURE 6
Optimization result of the IECPS backup routing mode under denial-of-service (DoS) attack on the power grid.

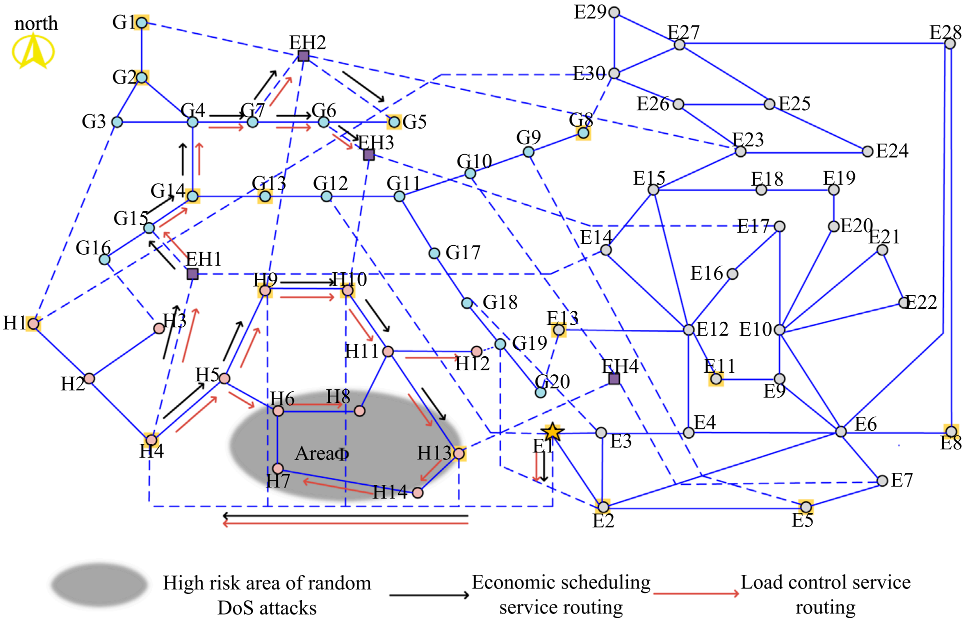


FIGURE 7
Optimization result of the IECPS backup routing mode under DoS attack on the hot network.

the communication substation EH4 of the energy station passes through E3, G18, G17, and G11 after optimization and is delivered after a detour, effectively avoiding the link (H13, EH4) in area ϕ_h. After optimization, the load control service flow of H7 is delivered from the northwest side, reducing the number of links flowing through high-risk areas. Compared with scenario 2, since grid area ϕ_e is no longer a high-risk area, the links in this area recover to assume service information flow after optimization. It can be seen that the optimization results of this routing robust optimization model can adaptively adjust the routing scheme according to the set high-risk area.

3) Analysis of optimization results of scenario 3: The main route optimization results of the IECPS economic dispatch service and load control service under the DoS attack in the air network communication area are shown in Figure 5. The figure shows that the information flow of economic dispatch service reaching G1,

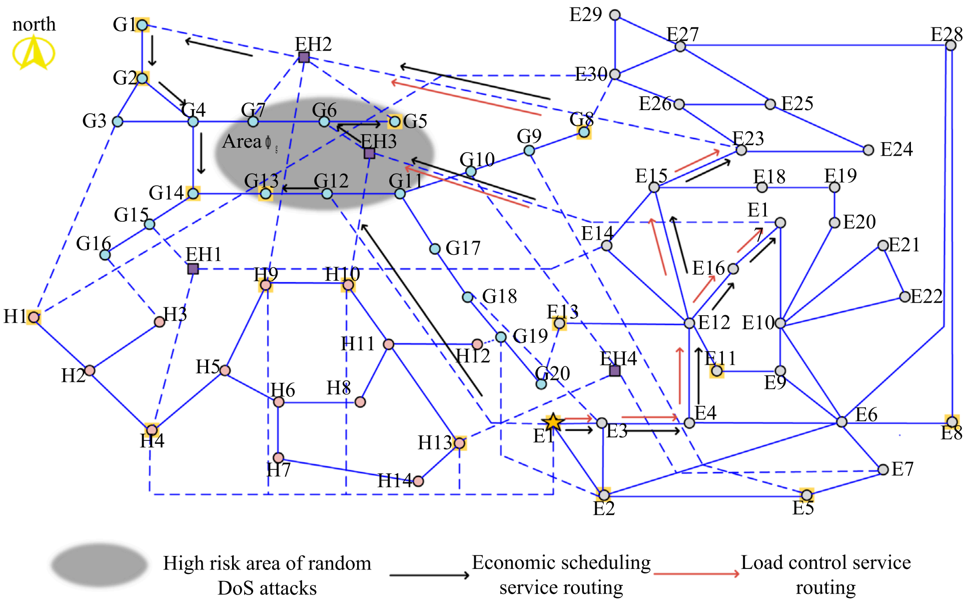


FIGURE 8
Optimization result of the IECPS backup routing mode under DoS attack on the gas network.

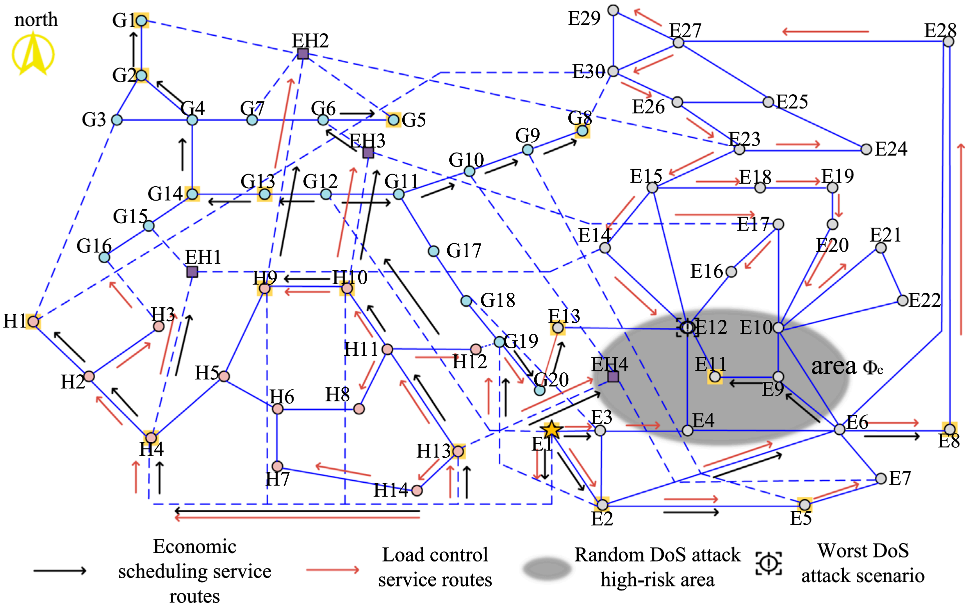


FIGURE 9
Optimization results of the main routing mode of IECPS services under the DoS attack on the power grid.

G2, and G14 after optimization no longer passes through high-risk links (G13, G14), (G12, G13), and (E1, G12). However, because G13 and G5 are located in high-risk areas, the optimized routing method of load control service information flow of their substations cannot avoid such high-risk areas and can only reduce the number of links passing through high-risk areas in the route. For energy station EH2, the information flow originally delivered by (H9, EH2) becomes roundabout and then delivered by (G1, EH2) after optimization, while the routing method of information flow of two services of energy station EH3 does not change before and after optimization. This is because EH3 is not only in a high-risk area but also the routing method before optimization has only one link path in the high-risk area, so there is no room for further optimization.

In addition, except by way of the main road, routing provides a robust optimization model to optimize the backup routing, as shown

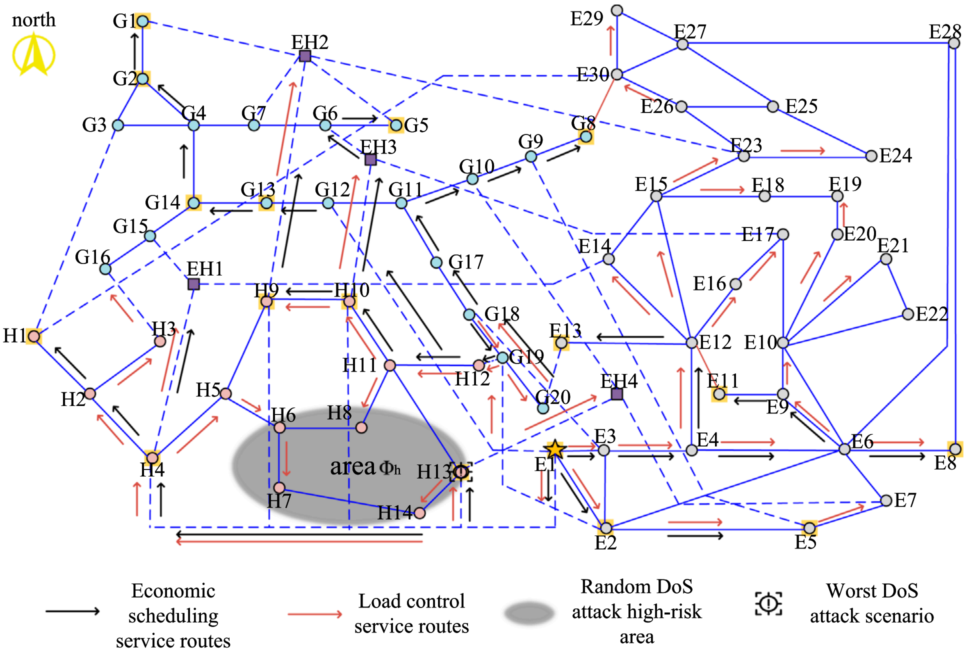


FIGURE 10
Optimization results of the IECPS service main routing mode under DoS attack on the hot network.

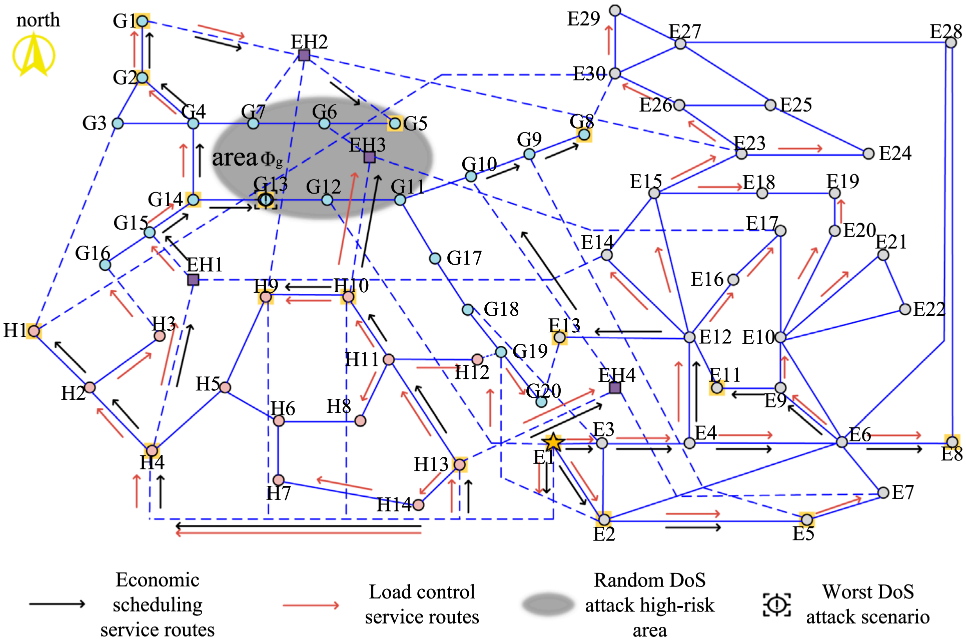


FIGURE 11
Optimization results of the IECPS service main routing mode under DoS attack on the gas network.

in Figures 6–8 (only substation alternate routes affected by high-risk areas are listed). It can be seen that due to the load for the routing optimization model of the effect that cannot overlap and communication network topology constraints, resulting in a large number of the routing information flow through more links and greater distances to reach the target substation or inevitably through the high-risk areas. Therefore, the optimization results are difficult to meet the requirements of reducing the degree of service association in high-risk areas and will not be described here.

In conclusion, after analyzing the optimization results of the above three scenarios, the CNRRO model established in this paper can effectively adaptively avoid high-risk areas according to

TABLE 3 Comparison of the worst scenarios before and after optimization.

Area of the worst scenario	Number of unreachable substations		Amount of load affected		Associated service degree	
	Before	After	Before	After	Before	After
Area ϕ_e	12	1	50.64	7.28	1,068.9	135.57
Area ϕ_h	9	3	95.20	44.81	166.61	19.13
Area ϕ_g	6	1	0	0	695.34	150.83

their locations and provide more secure routing modes for both service information flows, thereby avoiding or reducing the risk of DoS attacks.

5.3 Comparison of IECPS toughness before and after optimization

The routing optimization results mentioned in the above section should meet the toughness of the communication network in the worst scenario. The worst scenario before optimization determined according to Eq. 10 is shown in black in Figure 5, and the worst scenario after optimization is shown in black in Figures 9–11. The analysis of the worst scenario corresponding to the three high-risk areas is shown in Table 3.

The above table shows that, according to CNRRO, the number of unreachable service information flows, affected load, and associated service degree in the worst scenario of region ϕ_e and region ϕ_h after optimization are significantly reduced compared with those under the shortest path before optimization. However, the affected load in the worst scenario of region C before and after optimization is all 0. This is because the worst-case scenario does not affect the information flow of load control services but only that of economic scheduling services.

Specifically, according to the definition of association service degree in Eq. 5, the routing method optimized by CNRRO will change the association service degree of communication network links. According to the optimization objective, the associated service degree of the communication link in the high-risk area should be reduced after optimization compared with that before optimization so as to ensure that the service volume of the high-risk area is reduced. According to the route optimization results, the association service degree of the affected links in the above three high-risk areas of the IECPS communication network is calculated, and the comparison with the association service degree of the links in high-risk areas under the shortest path before optimization is shown in Figure 12. For the actual communication links corresponding to link numbers, see Table 4.

In Figure 12, by analysis, (a) shows that the correlation business degree of substations 1 and 2 is much higher than that of other substations in the region, which will lead to a large amount of load being affected if substation 1 is attacked. After the optimization, the correlation degree of substations 1 and 2 is significantly reduced. Substation 5 in (b) has a very high business correlation, indicating that the risk of the substation is very high. The optimization significantly reduces the risk of this substation being attacked. This is because according to CNRRO obtained by way of the main road to avoid the influence of DoS attack to bypass the high-risk areas, business information flow distribution occurs to the rest of the security link. The number of service information flows passing through high-risk areas is reduced, and the association degree of links in high-risk areas is reduced, which corresponds to the optimization goal of CNRRO. Alternate routing the suboptimal solution of the corresponding optimization, although the high-risk areas under alternate routing associated business degrees below before optimization-related business, but as a result of, the numerical example of communication network architecture itself leads to alternate routing cannot bypass the high-risk areas, lead to high-risk

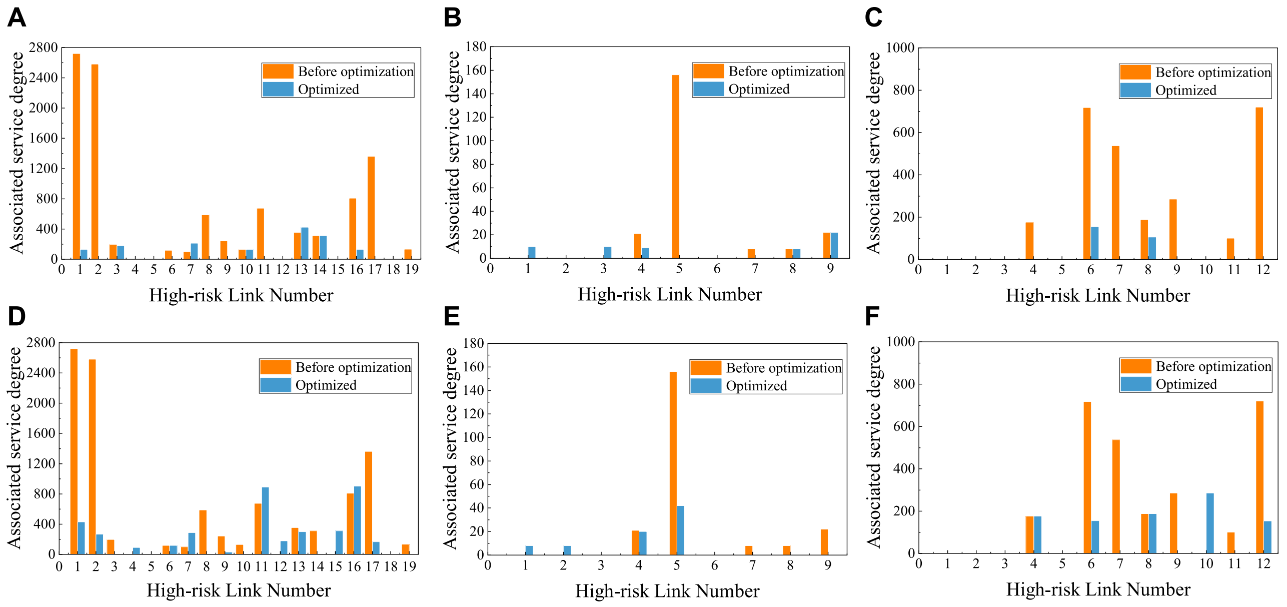


FIGURE 12
Comparison of link-related business degrees in high-risk areas before and after optimization: **(A–C)** link-associated service degrees of areas ϕ_e,ϕ_h, and ϕ_g in the main routing mode; **(D–F)** link-associated service degrees of areas ϕ_e,ϕ_h, and ϕ_g in the standby routing mode area. **(D)** in the standby routing mode; **(E, F)** link-associated service degree.

areas part link associated business degree is higher than the shortest path under the link associated business degrees. In summary, the route optimization method proposed in this paper can reduce the degree of service association in high-risk areas and improve the toughness of the IECPS communication network under the background of service information flow disturbance caused by DoS attacks.

5.4 Comparison of optimization results of the single-service index and double-service index

The simulation results compare the routing optimization results of only load control services, only economic dispatch services, and both services. The associated service degree of the high-risk area (the sum of the associated service degree of all links in the high-risk area) in the three cases is shown in Table 5.

Different importance indexes will directly affect the route optimization results, and the regional association service degree will be different under different optimization results. According to the analysis given in the above table, the associated business degree of high-risk area ϕ_e of the power grid and high-risk area ϕ_h of the heat network under the routing robust optimization based on the importance index of dual-service information flow is significantly lower than that of the high-risk area under the routing robust optimization based on the importance index of single-service information flow. Moreover, since the number of load control information flows undertaken by the two regions is more than the number of economic dispatch service information flows, the regional association service degree considering only load control service indicators is lower than that considering economic dispatch service indicators. However, for gas network high-risk area ϕ_g and areas under load control operations only, the associated business degree is significantly lower than that in the other two cases; this is because in the gas network information flow, only four-load control and load control-only businesses would lead to a large number of communication links, and the importance index is zero, which cannot effectively evaluate the importance of the communication links. In general, the routing robust optimization method considering both security and economy is better than the routing optimization method considering only the single-service index.

6 Conclusion

A routing optimization model with the dual objectives of security and economy is proposed for IECPS communication networks under DoS attacks. The optimization problem is solved using the CCG algorithm. Comparing with a single business optimization approach provides the following conclusions.

(1) A robust optimization model for routing in IECPS communication networks is developed, considering the worst scenario of a DoS attack. The results demonstrate that by minimizing the associated business degree in high-risk areas, the proposed optimization method effectively routes economic dispatch and load control information flows to bypass these areas. Furthermore, it adaptively optimizes each business information flow as the high-risk area changes, improving the resilience of the IECPS communication network.

TABLE 4 Shortest route for load control services.

High-risk area of the power grid		High-risk area of the heat network		High-risk area of the gas network	
Link number	Corresponding link	Link number	Corresponding link	Link number	Corresponding link
1	E3, E4	1	H5, H6	1	G4, G7
2	E4, E12			2	G7, EH2
3	H13, EH4	2	H6, H8	3	G7, G6
4	EH4, E7			4	G6, G5
5	E5, G9	3	H6, H7	5	G11, G12
6	E12, E13			6	G12, G13
7	E12, E14	4	H13, H14	7	G13, G14
8	E12, E15			8	EH3, G6
9	E12, E16	5	H13, H11	9	H10, G7
10	E9, E11			10	EH3, E17
11	E9, E10	6	E1, H9	11	H9, EH2
12	E10, E17			12	E1, G12
13	E10, E20	7	E1, H10		
14	E10, E21				
15	E10, E22	8	H8, H11		
16	E6, E9				
17	E4, E6	9	E1, H13		
18	E6, E10				
19	EH4, G10				

TABLE 5 Comparison of related business degrees in high-risk areas under different business indicators.

High-risk area	Degree of service association in high-risk areas			
	Before optimization	Load control services	Economic dispatch services	Both businesses are accounted
Area ϕ_e	10,342.53	2,683.34	3,854.39	1,563.67
Area ϕ_h	212.31	101.24	134.51	58.96
Area ϕ_g	2,636.23	103.46	825.61	253.15

(2) The integrated energy system fiber optic communication network consisting of an improved IEEE 30-node power grid, 14-node heat network, and 20-node gas network is used as an arithmetic example to analyze the change in the degree of business associated with the communication link in the attack area in conjunction with a DoS attack under the worst-case scenario. It significantly reduces the business relevance of high-risk substations. Thus, it helps minimize the loss when the system is attacked.

(3) This study uniquely combines the information flow importance index and communication link importance index to capture the dual objectives of security and economy. A comparison with a single-service optimization method confirms the superiority of the proposed approach.

It should be noted that this study considers only one control center in the information layer, while actual integrated energy systems may have multiple control centers. Future research should explore the IECPS routing optimization method for multiple control centers, which would involve more complex routing modes for each service information flow and closer coupling between information and physics.

Data availability statement

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

Author contributions

HF: writing–original draft and writing–review and editing. XH: writing–original draft and writing–review and editing. DW: writing–review and editing. BZ: writing–review and editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

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.

References

Cai, M., Zhang, E., Lin, J., Wang, K., Jiang, K., and Zhou, M. (2022). Route optimization equalization scheme based on graph theory for liquid metal battery strings. *IEEE Trans. Industry Appl.* 59, 2502–2508. doi:10.1109/TIA.2022.3221383

Dai, Y., Li, M., Zhang, K., and Shi, Y. (2023). Robust and resilient distributed mpc for cyber-physical systems against dos attacks. *IEEE Trans. Industrial Cyber-Physical Syst.* 1, 44–55. doi:10.1109/TICPS.2023.3283229

Ding, S., Gu, W., Lu, S., Yu, R., and Sheng, L. (2022). Cyber-attack against heating system in integrated energy systems: model and propagation mechanism. *Appl. Energy* 311, 118650. doi:10.1016/j.apenergy.2022.118650

Du, H., Zhang, J., Guan, K., Niyato, D., Jiao, H., Wang, Z., et al. (2022). Performance and optimization of reconfigurable intelligent surface aided thz communications. *IEEE Trans. Commun.* 70, 3575–3593. doi:10.1109/TCOMM.2022.3162645

Franze, G., Famularo, D., Lucia, W., and Tedesco, F. (2020). A resilient control strategy for cyber-physical systems subject to denial of service attacks: a leader-follower set-theoretic approach. *IEEE/CAA J. Automatica Sinica* 7, 1204–1214. doi:10.1109/JAS.2020.1003189

Gupta, P. K., Singh, N. K., and Mahajan, V. (2021). Intrusion detection in cyber-physical layer of smart grid using intelligent loop based artificial neural network technique. *Int. J. Eng.* doi:10.5829/IJE.2021.34.05B.18

Hammoudeh, M., and Newman, R. (2015). Adaptive routing in wireless sensor networks: qos optimisation for enhanced application performance. *Inf. Fusion* 22, 3–15. doi:10.1016/j.inffus.2013.02.005

Hu, S., Yue, D., Han, Q.-L., Xie, X., Chen, X., and Dou, C. (2020). Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks. *IEEE Trans. Cybern.* 50, 1952–1964. doi:10.1109/TCYB.2019.2903817

Kakadiya, H., Popat, J., Singh, N. K., Tak, L., Majeed, M. A., Mudgal, S., et al. (2022). "Analysis and prevention of denial of service attacks in smart grid using iot," in *Sustainable Technology and advanced computing in electrical engineering.* Editors V. Mahajan, A. Chowdhury, N. P. Padhy, and F. Lezama (Singapore: Springer Nature Singapore), 367–378.

Karamdel, S., Liang, X., Faried, S. O., and Mitolo, M. (2022). Optimization models in cyber-physical power systems: a review. *IEEE Access* 10, 130469–130486. doi:10.1109/ACCESS.2022.3229626

Kong, P.-Y. (2019). Optimal configuration of interdependence between communication network and power grid. *IEEE Trans. Industrial Inf.* 15, 4054–4065. doi:10.1109/TII.2019.2893132

Kong, P.-Y. (2020). Routing in communication networks with interdependent power grid. *IEEE/ACM Trans. Netw.* 28, 1899–1911. doi:10.1109/TNET.2020.3001759

Kong, P.-Y., and Jiang, Y. (2022). Vnf orchestration and power-disjoint traffic flow routing for optimal communication robustness in smart grid with cyber-physical interdependence. *IEEE Trans. Netw. Serv. Manag.* 19, 4479–4490. doi:10.1109/TNSM.2022.3165219

Kumar, N., Singh, B., and Panigrahi, B. K. (2019). Grid synchronisation framework for partially shaded solar pv-based microgrid using intelligent control strategy. *IET Generation, Transm. Distribution* 13, 829–837. doi:10.1049/iet-gtd.2018.6079

Kumar, N., Singh, B., and Panigrahi, B. K. (2023). Voltage sensorless based model predictive control with battery management system: for solar pv powered on-board ev charging. *IEEE Trans. Transp. Electrification* 9, 2583–2592. doi:10.1109/TTE.2022.3213253

Kumar, N., Singh, B., Wang, J., and Panigrahi, B. K. (2020). A framework of l-hc and am-mkf for accurate harmonic supportive control schemes. *IEEE Trans. Circuits Syst. I Regul. Pap.* 67, 5246–5256. doi:10.1109/TCSI.2020.2996775

Kumari, P., Kumar, N., and Panigrahi, B. K. (2023). A framework of reduced sensor rooftop spv system using parabolic curve fitting mppt technology for household consumers. *IEEE Trans. Consumer Electron.* 69, 29–37. doi:10.1109/TCE.2022.3209974

Li, B., Lu, C., Qi, B., Sun, Y., and Han, J. (2022). Risk and traffic based service routing optimization for electric power communication network. *Int. J. Electr. Power Energy Syst.* 137, 107782. doi:10.1016/j.ijepes.2021.107782

Li, B., Yang, J., Qi, B., Sun, Y., Yan, H., and Chen, S. (2014). Application of *p*-cycle protection for the substation communication network under srlg constraints. *IEEE Trans. Power Deliv.* 29, 2510–2518. doi:10.1109/TPWRD.2014.2358571

Li, M., Xue, Y., Ni, M., and Li, X. (2020). Modeling and hybrid calculation architecture for cyber physical power systems. *IEEE Access* 8, 138251–138263. doi:10.1109/ACCESS.2020.3011213

Li, T., Chen, B., Yu, L., and Zhang, W.-A. (2021). Active security control approach against dos attacks in cyber-physical systems. *IEEE Trans. Automatic Control* 66, 4303–4310. doi:10.1109/TAC.2020.3032598

Li, Y., Quevedo, D. E., Dey, S., and Shi, L. (2017). Sinr-based dos attack on remote state estimation: a game-theoretic approach. *IEEE Trans. Control Netw. Syst.* 4, 632–642. doi:10.1109/TCNS.2016.2549640

Li, Y., Ren, R., Huang, B., Wang, R., Sun, Q., Gao, D. W., et al. (2023). Distributed hybrid-triggering-based secure dispatch approach for smart grid against dos attacks. *IEEE Trans. Syst. Man, Cybern. Syst.* 53, 3574–3587. doi:10.1109/TSMC.2022.3228780

Lv, M., Lv, Y., Yu, W., and Meng, H. (2023). Finite-time attack detection and secure state estimation for cyber-physical systems. *IEEE/CAA J. Automatica Sinica* 10, 2032–2034. doi:10.1109/JAS.2023.123351

Pazouki, S., Naderi, E., and Asrari, A. (2021). A remedial action framework against cyberattacks targeting energy hubs integrated with distributed energy resources. *Appl. Energy* 304, 117895. doi:10.1016/j.apenergy.2021.117895

Popat, J., Kakadiya, H., Tak, L., Singh, N. K., Majeed, M. A., and Mahajan, V. (2021). "Reliability of smart grid including cyber impact: a case study," in *Computational methodologies for electrical and electronics engineers* (IGI Global), 163–174. Available at: https://api.semanticscholar.org/CorpusID:234186951

Saxena, V., Kumar, N., Singh, B., and Panigrahi, B. K. (2021). An mpc based algorithm for a multipurpose grid integrated solar pv system with enhanced power quality and pcc voltage assist. *IEEE Trans. Energy Convers.* 36, 1469–1478. doi:10.1109/TEC.2021.3059754

Shabanpour-Haghighi, A., and Seifi, A. R. (2015). Simultaneous integrated optimal energy flow of electricity, gas, and heat. *Energy Convers. Manag.* 101, 579–591. doi:10.1016/j.enconman.2015.06.002

Siu, J. Y., Kumar, N., and Panda, S. K. (2022). Command authentication using multiagent system for attacks on the economic dispatch problem. *IEEE Trans. Industry Appl.* 58, 4381–4393. doi:10.1109/TIA.2022.3172240

Solanki, M. G., Patel, K. S., Kanzariya, B. R., Parekh, T. H., Singh, N. K., Yadav, A. K., et al. (2022). "Review on cybersecurity and major cyberthreats of smart meters," in *Sustainable Technology and advanced computing in electrical engineering*. Editors V. Mahajan, A. Chowdhury, N. P. Padhy, and F. Lezama (Singapore: Springer Nature Singapore), 527–541.

Soltan, S., Yannakakis, M., and Zussman, G. (2019). React to cyber attacks on power grids. *IEEE Trans. Netw. Sci. Eng.* 6, 459–473. doi:10.1109/TNSE.2018.2837894

Ti, B., Wang, J., Li, G., and Zhou, M. (2022). Operational risk-averse routing optimization for cyber-physical power systems. *CSEE J. Power Energy Syst.* 8, 801–811. doi:10.17775/CSEEJPES.2021.00370

Wang, A., Fei, M., Song, Y., Peng, C., Du, D., and Sun, Q. (2023). Secure adaptive event-triggered control for cyber–physical power systems under denial-of-service attacks. *IEEE Trans. Cybern.* 54, 1722–1733. doi:10.1109/TCYB.2023.3241179

Xin, S., Guo, Q., Sun, H., Zhang, B., Wang, J., and Chen, C. (2015). Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems. *IEEE Trans. Smart Grid* 6, 2375–2385. doi:10.1109/TSG.2014.2387381

Zhang, Q., Lin, M., Yang, L. T., Chen, Z., and Li, P. (2019). Energy-efficient scheduling for real-time systems based on deep q-learning model. *IEEE Trans. Sustain. Comput.* 4, 132–141. doi:10.1109/TSUSC.2017.2743704

Zhang, Y., Jiang, T., Shi, Q., Liu, W., and Huang, S. (2022). Modeling and vulnerability assessment of cyber physical system considering coupling characteristics. *Int. J. Electr. Power Energy Syst.* 142, 108321. doi:10.1016/j.ijepes.2022.108321

Zhao, X., Zou, S., and Ma, Z. (2021). Decentralized resilient h_{∞} load frequency control for cyber-physical power systems under dos attacks. *IEEE/CAA J. Automatica Sinica* 8, 1737–1751. doi:10.1109/JAS.2021.1004162

Nomenclature

Parameters	Definition
α, β	Importance of load control service/ economic dispatch service
G	Directional graph consisting of nodes and branches
v	Collection of nodes
M	Number of child station nodes
e	Set of communication links to substations
B	Number of communication links
A_G	Adjacent matrix of the communication network
X_{kq}, Y_{kq}	Primary routing matrix/backup routing matrix of the service information flow
S	Set of fault scenarios on the physical side
δ_s	Probability of failure in scenario s
L^{sq}	Load reduction corresponding to the information flow q of the substation in fault scenario s
ω	Load reduction penalty cost coefficient
I_{kq}	Information flow importance index
E	Communication link association service degree matrix
Φ	Denial-of-service (DoS) attack fault set
$F_{Dos,k}$	Link failure matrix in the fault set Φ
A_{k0}	Communication substation fault matrix under DoS attack
$\odot$	Hadamard product
δ, χ	Micro-quantity used to set the priority of the optimization target
s^q, t^q	Number of source nodes/end nodes of information flow q route
c_{ij}	Available path of the communication optical cable
az, z	Upper objective function/decision variable vector
bg, g	Lower objective function/decision variable vector
u	Vector of variables in an uncertain fault set
k	Number of subproblems
ρ	Maximum objective function value of all subproblems
u_l^*	Optimal fault scenario of subproblem l
$z*$	Decision variables for the solved upper-level master problem
$C^{sq}, C^{sq\prime}$	Operating cost of the information flow q corresponding to the substation in the fault scenario s determined by the economic dispatch/load control task
N	Set of service information flows
X, Y	Primary/backup routing matrices of information flow q
$x_{,ij}, y_{,ij}$	0–1 variables for communication links
r	Interrupt discriminant variable for information flow q
$X_{kq,ij}$	Primary routing matrix of the service information flow
$Y_{kq,ij}$	Backup routing matrix of the service information flow

Subscripts	Definition
c, s, e, h, g	Master station/energy station/electric/heat/gas
l, d	Load control/economic dispatch operations
x, y	Primary/backup routing