EAI Endorsed Transactions
on Scalable Information Systems

Research Article EAI.EU

Risk-Aware Secure Routing Mechanism for Power Communication Networks Based on GNNs

Yanjun Zhao*, Yue Zhang, Xiaowei Zhao, Liyu Liu, Xiang Wang and Kaiyue An

Inner Mongolia Power Communication Company, Hohhot 010020, China

Abstract

INTRODUCTION: As digital transformation progresses, power communication networks become exposed to increasingly complex security threats. Moreover, traditional routing algorithms cannot perceive or respond to dynamic security threats, making reliable data transmission difficult to achieve under network attack conditions. OBJECTIVES: Therefore, this study proposes a risk-aware secure routing (RASR) mechanism for power communication networks based on graph neural networks (GNNs). METHODS: The mechanism first introduces an autoencoder-graph neural network (AGNN) architecture for determining critical nodes, thus establishing a scoring prediction model customized to the structure of power communication backbone networks. It then integrates the essential scores of the nodes, historical failure rates, and traffic load factors to devise a path node risk quantification model. Finally, it incorporates risk quantification results into routing policies to enable proactive routing avoidance and thus bypass high-risk nodes. RESULTS: Experimental results show that the RASR algorithm effectively meets the differentiated service requirements of heterogeneous traffic—including delay-sensitive, bandwidth-sensitive, and reliability-sensitive traffic. Compared with traditional routing algorithms, it demonstrates greater stability and fault tolerance under high-risk attack scenarios while eliminating the need for redundant backup strategies, thereby markedly reducing resource overhead. CONCLUSION: Therefore, the proposed mechanism offers important theoretical support and a novel technical approach for establishing secure, reliable power communication networks.

Keywords: Cyberattack, Power Communication Network, Key Node Identification, Risk-Aware, Secure Routing

Received on 15 September 2025, accepted on 18 October 2025, published on 16 March 2026

doi: 10.4108/eetsis.12042

1. Introduction

As digital transformation advances, powerful communication networks increasingly support critical finance, industry, health care, and related sector operations. However, frequent cyberattacks driven by increasingly sophisticated methods have exposed these networks to unprecedented security threats [1,2]. Exacerbating this situation, traditional network routing mechanisms mainly rely on static topology information and performance metrics for path selection [3], thus lacking the ability to perceive and respond to dynamic security threats. When facing network infrastructure attacks such as DDoS attacks or node hijacking, such mechanisms have difficulty adjusting routing policies rapidly. As such, attacked nodes or links may experience performance degradation, data loss, or complete failure [4,5]. As networks continue to scale and attack methods evolve, this problem intensifies. Thus, an urgent need exists to develop new, risk-aware secure routing mechanisms to address complex cybersecurity challenges. Existing routing algorithms are primarily categorized into traditional routing, heuristic routing, and deep reinforcement learning-based routing algorithms [6]. Traditional routing algorithms compute paths based on predefined metrics such as the hop count, bandwidth, and latency. Furthermore, heuristic routing algorithms [7,8] incorporate bio-inspired and swarm intelligence concepts, enabling some adaptation to network changes. Moreover, deep reinforcement learning-based routing algorithms [9,10] represent the current technological frontier, possessing robust learning and

[*] Corresponding author. Email:zhaoyanjun198111@yeah.cn

adaptive capabilities. Nonetheless, they perform sub-optimally in risk identification and security awareness. Existing algorithms share a common limitation in that most focus on performance metrics [11,12], while neglecting adjustments to routing strategies during network attacks. Specifically, these algorithms often fail to promptly identify risky nodes and adjust routes when faced with security threats such as malicious attacks, node failures, or link disruptions. Recently, research has started to address the security aspects of routing algorithms. For instance, to meet the anti-sabotage requirements of power communication backbone networks, researchers [13] proposed a link-risk-balanced anti-sabotage routing optimization method, which optimizes for link risk equilibrium and service transmission delay. Moreover, researchers [14] designed a network routing optimization strategy based on an improved genetic algorithm [15], thereby enhancing the network's resilience against typical attacks. Addressing the issue of uneven service distribution across channel segments caused by a single-dimensional routing optimization metric system, researchers [16] established a risk assessment model for power communication networks.

Although these studies have made some advances in secure routing, two major issues persist in their practical applications. First, effective integration mechanisms between risk identification and routing decisions are lacking. That is, cybersecurity research focuses on intrusion detection and risk assessment, while routing protocol research mainly addresses performance optimization [17,18]. Second, traditional fault-tolerance mechanisms produce resource wastage. In resource-constrained environments, this requirement not only increases system costs [19] but may also introduce new points of failure owing to greater management complexity.

Against the aforementioned backdrop, this study proposes a communication network risk-aware secure routing (RASR) mechanism based on graph neural networks (GNNs). The main study contributions are summarized as follows.

(1) Given the unique characteristics of power communication backbone networks, the study proposes a key node identification method that combines autoencoders with GNN architecture, thus enabling effective identification of critical nodes within these networks.

(2) By integrating key node scoring, historical failure rates, and traffic load factors, the study constructs a risk quantification model for path nodes in power communication backbone networks, which effectively evaluates the potential risk values of nodes.

(3) Integrating the path node risk quantification model into the backbone network routing strategy, the study proposes an RASR mechanism. The strategy employs intelligent and secure routing avoidance to proactively bypass high-risk nodes and reduces resource overhead while maintaining network reliability.

(4) Experimental results show that the proposed algorithm effectively meets the differentiated service requirements of heterogeneous traffic types, including delay-sensitive, bandwidth-sensitive, and reliability-sensitive traffic.

2. Risk-Aware Secure Routing Mechanism Based on GNNs

2.1. Problem Description

This study models the power communication backbone network as a graph $G = (V, E)$, where $V = \{v_1, v_2, \dots, v_n\}$ signifies the node set, and $E = \{e_{12}, e_{23}, \dots, e_{ij}\}$ is the set of all communication links[20]. Here, $|V| = n$ and $|E| = m$ are the number of nodes and links, respectively. Furthermore, the path from the source node v_s to the destination node v_d in the network is represented by p_{sd}, where $p_{sd} = \{e_{sa}, e_{ab}, \dots, e_{cd}\}$. Further, $|s|$ and $|d|$ represent the number of source nodes and destination nodes, respectively. In graph theory, each node within the node set V is denoted as v_i, and a directed edge connecting the node v_i to node v_j in the edge set E is denoted by e_{ij}. For a graph containing n nodes, its topological structure can be characterized using an $n \times n$ adjacency matrix A. The matrix element A_{ij} is defined as follows: If the edge e_{ij} exists in the edge set E, then $A_{ij} = 1$; when no such edge is present, $A_{ij} = 0$.

Identifying influential nodes remains a key challenge in network analysis. For a given graph $G = (V, E)$, the aim is to compute importance values for each node $v \in V$, forming a score vector $S = (s_1, s_2, \dots, s_{n-1}, s_n)$, where s_i is the importance value of the node v_i . These computed scores enable the creation of a node importance hierarchy, expressed as $RK = (rk_1, rk_2, \dots, rk_{n-1}, rk_n)$, with rk_i indicating the hierarchical position of the node v_i. The ranking adopts the following principles: Equal scores yield identical rankings ($s_i = s_j \Rightarrow rk_i = rk_j$), higher scores correspond to superior rankings ($s_i > s_j \Rightarrow rk_i < rk_j$), and lower scores result in inferior rankings ($s_i < s_j \Rightarrow rk_i > rk_j$). Through this importance hierarchy RK, we can pinpoint the most influential vertices within graph G. As such, the essence of influential node detection lies in accurately ascertaining the node importance values S.

The proposed RASR mechanism is an intelligent routing algorithm that integrates fault prediction mechanisms with dynamic risk assessment to improve fault tolerance. This mechanism combines criticality scores derived from a GNN-based method for identifying key nodes in power communication networks to establish a path node risk quantification model. Based on this, a node fault prediction model is created. Incorporating real-time network status information enables proactive identification and avoidance of potential fault risks. This approach markedly enhances network communication reliability and fault tolerance while ensuring transmission efficiency.

2.2. GNNs-Based Method for Identifying Critical Nodes in Power Communication Networks

In this research, we present the autoencoder-graph neural network (AGNN), an innovative approach that combines autoencoding techniques with graph neural network (GNN) architectures to identify critical nodes in power communication backbone infrastructures. The AGNN architecture consists of two main parts, as shown in Figure 1: an autoencoder for extracting features and a predictor for ranking importance. The autoencoder part makes embedded node representations of the network's structure. There are both encoding and decoding mechanisms in this module. The input data is transformed into one-hot vectors. The encoding phase uses a dual-layer graph convolutional network (GCN) structure, and the decoding phase uses a multi-layered perceptron (MLP) structure with two fully connected (FC) layers. The comprehensive importance ranking predictor module then gets the embedded representations that were taken out during the encoding process.

The comprehensive importance ranking predictor looks at each node in the network topology and gives it a significance value. Higher numbers mean that the node is more important. There are two GNN layers and one FC layer in the model. We use batch normalization after each graph convolutional layer to make training more stable and speed up convergence. This helps the model generalize better and avoid overfitting. Before the FC layer, dropout regularization is also used. The ReLU activation function is used after every layer to add the ability to change things in a nonlinear way.

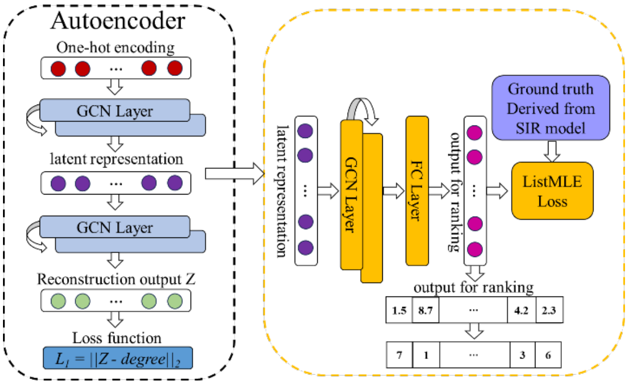

Figure 1. AGNN Framework Diagram

2.2.1 Autoencoder

We use an autoencoder with a GCN as its encoder in order to generate node feature vectors by utilizing network information to the fullest extent possible. This method guarantees that the node latent representations produced fully incorporate the topological structure of the network. We achieve semantically enriched node representation vectors by effectively integrating the network topology's diverse structural features and connectivity patterns through the deployment of the GCN. When compared to conventional methods, this architectural choice achieves better critical node detection accuracy and computing efficiency.

A matrix created by one-hot vectorizing every vertex in network topology G is sent to the first layer of the autoencoding module. The dual-layer GCN design of the encoding component can be described mathematically as follows:

$$H^{i+1} = \sigma\left(\widetilde{D}^{-\frac{1}{2}}\tilde{A}\widetilde{D}^{-\frac{1}{2}}H^{i}W_{GCN}^{i}\right) \tag{1}$$

where $\tilde{A} = A + I$ stands for the modified adjacency representation, A signifies the connectivity matrix of network G, and I denotes the identity matrix. Furthermore, $\widetilde{D}$ represents the degree matrix derived from $\tilde{A}$, H^i indicates node embeddings at the i-th GCN layer, W_{GCN}^{i} represents the learnable parameter matrix for layer i, and σ denotes the nonlinear activation function.

The comprehensive importance ranking predictor uses the embedded feature vectors produced by the encoding procedure as input data. The mathematical expression for the decoding component, which consists of an MLP architecture with two FC layers, is as follows:

$$Y^{i+1} = Y^{i}W_{MLP}^{i} + b^{i} \tag{2}$$

where Y^i stands for the node embeddings in the i-th FC layer. W_{MLP}^{i} represents the learnable parameter matrix, while b^i is the learnable bias vector. The autoencoding module's reconstructed output from the autoencoding module is expressed as $Z = Y^2$. We adopt the node connectivity degree as the module's reconstruction target, with the loss function formulated as follows:

$$L_1 = \left|\left|Z - degree\right|\right|_2 \tag{3}$$

where Z denotes the model's reconstructed prediction, and *degree* corresponds to the degree vector associated with network topology G.

2.2.2 Overall Ranking Prediction Model

We developed a thorough importance evaluation framework that assigns significance scores to each vertex in the network structure in order to take advantage of node properties generated by the autoencoding architecture. The comprehensive importance assessment framework receives embedded representations generated through the encoding process as input data. The concealed layers of this assessment framework incorporate dual GNN components alongside a single FC layer. The GNN formulation is expressed as follows:

$$E^{i+1} = (A{+}I)E^{i}W_{GNN}^{i} + b_{GNN}^{i} \tag{4}$$

where E^i is the node embeddings in the i-th layer; A stands for the adjacency matrix of the network; I is the unit matrix; and W_{GNN}^{i} and b_{GNN}^{i} are the learnable parameter matrix and bias vector, respectively.

We adopt the SIR epidemic framework to build real datasets. Here, S characterizes the vulnerable condition, I

signifies the contagious condition, and R is the recovered state. During each temporal iteration, a contagious node possesses the probability θ of spreading the infection to neighboring vulnerable vertices, while a vulnerable node maintains the probability β of achieving recovery. Recovered vertices become permanently resistant to infections in the future. The computational process continues until all contagious vertices are eliminated.

Initialize node v to the contagious condition while setting all remaining vertices to the vulnerable condition. Upon reaching the equilibrium state, we calculate the count of contagious and recovered vertices, denoted as F_v. Then, F_v serves as an indicator of node v's transmission capability. We adopt the mean value of F_v over 100 computational runs as the ground truth for node v, denoted as y_v. The transmission probability threshold θ_c is derived through mean-field theoretical analysis [21], formulated as follows:

$$\theta_c = \frac{<k>}{<k^2>-<k>} \tag{5}$$

where k signifies the node degree, and $<\cdot>$ represents averaging. In our study, we configure the β parameter of the SIR framework to unity and establish the θ parameter at 1.5 times the magnitude of θ_c.

We then employ listMLE [22] as the loss function for our comprehensive ranking prediction framework. Specifically, listMLE is a list-wise ranking loss function. Different from frequently used point-wise ranking loss functions (including mean squared error, MSE), list-wise approaches aim to enhance global ranking performance, rather than exclusively focusing on individual score values. Thus, these approaches typically deliver better outcomes in most scenarios. The mathematical expression for listMLE is as follows:

$$L_2 = -logP\left(\pi_y \middle| y'\right) \tag{6}$$

where y' denotes the ultimate prediction from the neural architecture, and π_y characterizes the ordering outcomes derived from the ground truth value y. P denotes the Plackett-Luce framework, whose mathematical formulation is as follows:

$$P(\pi|x) = \prod_{i=1}^{n} \frac{\exp\left(x_{\pi(i)}\right)}{\sum_{k=i}^{n} \exp\,(x_{\pi(k)}))} \tag{7}$$

2.3 Risk-Aware Routing Policy

2.3.1 Construction of Node Risk Quantification Models

The aim of constructing a node risk quantification model is to convert the node importance score $S(v)$ into a node risk value $R(e)$. $S(v)$ represents the criticality rating of a node, derived from a neural network–based method for determining key nodes in power communication networks. The calculation formula for $R(e)$ is as follows:

$$R(e) = I(v) \times \frac{\deg(v)}{\sum_{e' \in E_v} bw(e')} \times \left(1 + P_{fail}(v)\right) \tag{8}$$

where $\frac{\deg(v)}{\sum_{e' \in E_v} bw(e')}$ represents the traffic load factor, $\deg(v)$ denotes the degree of node v, $bw(e')$ signifies the bandwidth of the edge e', and $\sum_{e' \in E_v} bw(e')$ is the sum of the bandwidths of links directly connected to node v. Moreover, $P_{fail}(v)$ is the failure probability of node v based on historical data, and $I(v)$ is the failure impact radius of node v. The calculation formula for $I(v)$ is as follows:

$$I(v) = \sum_{u \in N(v,k)} w_{vu} \times S(v) \times e^{-\lambda d(u,v)} \tag{9}$$

where $N(v,k)$ denotes the set of all nodes within k hops of node v, and k represents the hop range. w_{vu} is the quality weight of the path from node u to node v, calculated using bandwidth, with $\lambda = 0.8$ as the attenuation factor. Last, $S(v)$ denotes the node importance score.

2.3.2 Construction of Node Failure Prediction Models

The core innovation of the RASR strategy lies in introducing a fault prediction model based on historical data and node characteristics. By analyzing the risk value features of nodes, this model establishes a simple yet effective linear prediction mechanism. Specifically, for each node v in the network, the system calculates the corresponding failure probability $\mathrm{P_{fail(v)}}$ based on its risk value R(v), as follows:

$$\mathrm{P_{fail(v)}} = \begin{cases} \min\left(0.8, \frac{\mathrm{R(v)}}{10.0}\right), & \mathrm{R(v)} \geq \sigma 1 \\ \min\left(0.3, \frac{\mathrm{R(v)}}{10.0}\right), & \sigma 1 \geq \mathrm{R(v)} \geq \sigma 2 \\ \min\left(0.1, \frac{\mathrm{R(v)}}{10.0}\right), & \mathrm{R(v)} \leq \sigma 2 \end{cases} \tag{10}$$

where $\sigma 1$ represents the high-risk threshold, and $\sigma 2$ denotes the medium-risk threshold. This hierarchical prediction mechanism effectively distinguishes nodes across different risk levels. It provides precise failure probability assessments for future path selection, thus equipping the system to accurately identify high-risk nodes with elevated failure tendencies and apply corresponding weight adjustments in routing decisions.

2.3.3 Path Cost Function and Predictive Edge Weight Calculation Mechanism

To fully exploit fault prediction information, the RASR strategy features a multidimensional path cost function that comprehensively considers traditional routing metrics and risk-aware factors. The path cost C is calculated as follows:

$$\begin{aligned} C = \alpha \times C_{original} + \beta \times R_{max} \\ + \gamma \times R_{total} + \delta \times P_{total} \end{aligned} \tag{11}$$

where $C_{original}$ denotes the original path cost based on delay and hop count; R_{max} and R_{total} represent the maximum risk and total risk on the path, respectively; and P_{total} indicates the sum of predicted failure probabilities across all nodes on the path. The weight parameters $\alpha = 0.3$, $\beta = 0.25$, $\gamma = 0.2$, and $\delta = 0.25$ reflect the strategy's emphasis on risk perception, thereby ensuring that transmission paths with lower risk are prioritized while maintaining fundamental transmission performance.

During the specific path search process, the RASR strategy utilizes a dynamic edge weight calculation method based on predictive modeling. Specifically, for each edge (u,v) in the network, the system not only considers its baseline transmission delay but also introduces a penalty mechanism based on the predicted failure probability of the destination node. The dynamic edge cost C_{edge} for edge (u,v) is calculated as follows:

$$C_{edge} = delay + P_{p(v)} \times delay \times 3.0 + R(v) \times 0.1 \qquad (12)$$

where $delay$ denotes the original transmission delay of edge (u, v), $P_{p(v)}$ is the failure prediction probability of target node v for edge (u, v), and $R(v)$ is the static risk assessment value of target node v for edge (u, v). This design enables the algorithm to automatically avoid nodes and links with high failure risks during the path search. The setting of the predictive probability penalty factor at 3.0 ensures that high-risk nodes are strongly penalized in path selection, thus allowing the algorithm to select more reliable transmission paths.

3. Simulation Scenario Setup and Results Analysis

3.1 Experimental Environment and Parameter Settings

To verify the effectiveness of the proposed risk-aware secure routing algorithm, this section provides a detailed explanation of the construction of a simulation environment. In the experiments, we employed Python 3.9 as the development language and implemented the algorithm model based on the NetworkX network analysis library and the PyTorch framework. Moreover, simulations were performed on a computer equipped with an AMD Ryzen 9 processor featuring Radeon Graphics (2.50 GHz) and 16GB of RAM.

In this experiment, we utilized a municipal-level power communication backbone network dataset comprising 300 nodes. The dataset underwent random degradation, and node failure rates were set at 3%, 6%, 9%, 12%, and 15% for each of the five testing scenarios. In order to assess algorithm performance comprehensively, we randomly sampled 5,000 distinct end-to-end paths as test cases. Each path included three candidate routing options to simulate real-world multipath selection scenarios.

3.2 Experimental Results and Analysis

3.2.1 Path Influence Rate Comparison

To assess the RASR strategy's fault tolerance performance under network failure scenarios, we present a test of the interference resistance of various routing strategies by simulating node failures at different levels of severity. In the experiment, we gradually increased the node failure rate from 3% to 15%. At each failure rate level, a corresponding proportion of network nodes was randomly selected for fault simulation. The path impact rate variation for each strategy was then statistically analyzed. Here, the path impact rate is the percentage of failed paths caused by node failures relative to all paths, and this metric intuitively reflects a routing strategy's robustness amid network failures.

In the experiment, we compared four routing strategies: shortest path first (SPF), minimum delay path (MDP), maximum bandwidth path (MBP), and the proposed RASR strategy. Figure 2 shows how the path impact rates of these four strategies vary under different node failure rates. The experimental results show that the RASR strategy and traditional routing strategies perform significantly differently in terms of fault-tolerance.

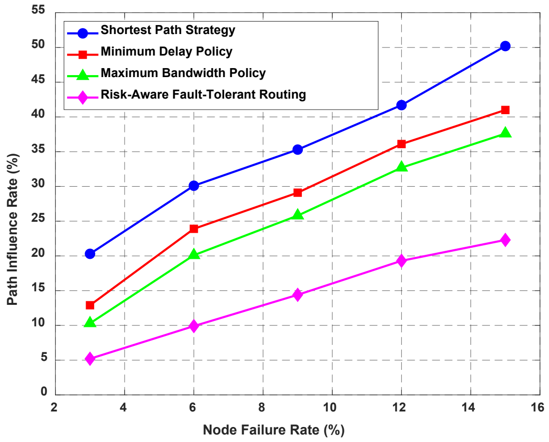

Figure 2. Comparison of Path Affected Rates Under Various Node Failure Rates for Different Algorithms

The experimental results show that the path impact rates of all three traditional strategies show a sharp upward trend as the node failure rate rises.

These traditional approaches often choose nodes that appear optimized but carry latent failure risks during initial path selection, since they don't have the ability to predict network risks. This leads to widespread failure of predefined paths when network conditions worsen, thereby severely compromising communication stability.

In contrast, the RASR strategy demonstrates exceptional resilience in controlling path impact rates. Throughout testing, RASR consistently maintains the lowest path impact rate. Under the stringent 15% disruption rate condition, the RASR strategy reduces the path impact rate by 15.3, 18.7, and 27.9 percentage points compared with the shortest path strategy, minimum delay path strategy, and maximum bandwidth path strategy, respectively, thereby showing significant advantages in performance. More importantly, the RASR strategy exhibits a relatively flat path impact rate growth curve, indicating robust resistance to interference.

3.2.2 Basic Performance Comparison

This section describes the construction of a multidimensional performance evaluation system for validating the effectiveness of the proposed RASR strategy. Three benchmark strategies were selected for comparison: shortest path first (SPF), minimum delay path (MDP), and mean maximum bandwidth path (MBP). The evaluation framework encompassed five core metrics: (1) average packet transmission delay, reflecting the timeliness of the routing strategy; (2) average throughput, measuring the network's data transmission capacity; (3) packet loss rate, assessing network service quality; (4) path risk assessment value, quantifying the security level of the path; and (5) path reliability, measuring the stability of the path. These metrics reflect the balance achieved by the RASR strategy between performance optimization and risk control from multiple perspectives.

Definition 1 (Average packet transmission delay) The average packet transmission delay is the ratio of the end-to-end delay to the path length, where the end-to-end delay is the sum of delays across all links in the path, acting as an additive parameter:

$$d(p_{sd}) = \sum\nolimits_{\forall e_{ij} \in p_{sd}} d\left(e_{ij}\right) \qquad (13)$$

where $d(p_{sd})$ represents the end-to-end delay of the path, and $d\left(e_{ij}\right)$ denotes the delay of the links on the path.

Definition 2 (Average Throughput) The end-to-end average throughput is the ratio of the total data transmitted along the path to the end-to-end delay:

$$T_{avg} = \frac{\sum_{e_{ij} \in p_{sd}} T(e_{ij})}{d(p_{sd})} \qquad (14)$$

where T_{avg} denotes the average throughput of the path, and $T\left(e_{ij}\right)$ represents the throughput of the link e_{ij} .

Definition 3 (Packet Loss Rate) The packet loss rate is defined as the ratio of the total number of (source, destination) node pairs experiencing packet loss during routing to the total number of (source, destination) node pairs in the routing process. For each (source, destination) node pair, three paths were identified for each routing strategy. If any of the three paths contained a damaged node, packet loss was deemed to have occurred when routing this node pair.

Definition 4 (Path Risk Assessment) The path risk assessment formula is as follows:

$$R_{sd} = rm_{sd} \times \alpha + \frac{\sum_{v_i \in p_{sd}, i \neq s, i \neq d} r_i}{l_{sd}} \times \beta \qquad (15)$$

where rm_{sd} denotes the risk value of the highest-risk node in the path p_{sd}, where $rm_{sd} = \max\{r_i | v_i \in p_{sd}\}$, with r_i representing the risk value of the node v_i in path p_{sd}, and l_{sd} being the number of nodes in the path p_{sd}, and $\alpha = \beta = 0.5$.

Definition 5 (Path Reliability) The formula for calculating the reliability $reliability_{sd}$ of path p_{sd} is as follows:

$$reliability_{sd} = \frac{1}{1+\frac{\sum_{v_i \in p_{sd}, i \neq s, i \neq d} r_i}{l_{sd}}} \qquad (16)$$

Figure 3 shows the packet loss rate performance comparison results of each algorithm under standard test conditions. As the experimental results in Figure 3 clearly illustrate, the RASR strategy consistently exhibits the lowest packet loss rate throughout the entire testing process. At a network failure rate of 3%, its packet loss rate is only 0.1%. At increased node failure rates of 6%, 9%, 12%, and 15%, the packet loss rates are only 0.2%, 1.0%, 2.2%, and 3.2%, respectively. Furthermore, compared with the other three benchmark routing strategies, it consistently exhibits a more gradual linear growth trend.

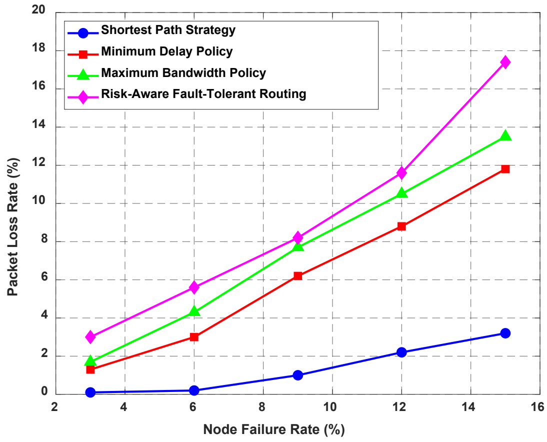

Figure 3. Comparison of packet loss performance across algorithms under varying node failure rates

Traditional strategies typically choose paths based on a single performance metric, while completely disregarding node reliability factors. When networks succumb to attacks that result in numerous failed nodes, these strategies fail to effectively avoid nodes vulnerable to destruction under attack conditions. In contrast, the RASR strategy employs a dynamic risk assessment mechanism to continuously monitor changes in node health status and dynamically adjust path selection accordingly. As such, it maintains stable transmission performance even in highly dynamic, high-intensity attack environments. Fig. 4 shows the packet transmission latency performance comparison results of different algorithms under standard test conditions.

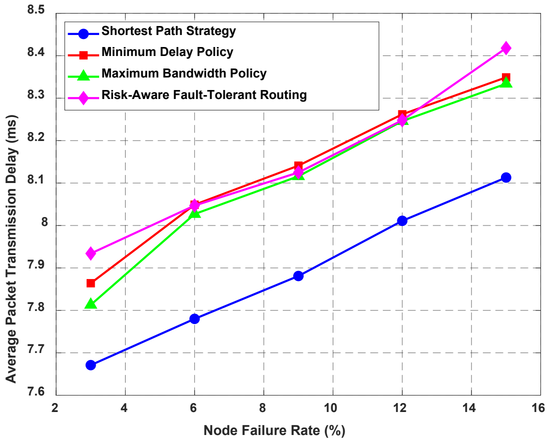

Figure 4. Comparison of packet transmission delay among algorithms under varying node failure rates

The RASR strategy also demonstrates outstanding performance in terms of latency. As observed in the experimental results of Figure 4, the RASR strategy consistently maintains the lowest transmission delay throughout the entire test. Under a 3% network failure rate, its average delay is only 7.671 ms. As the node failure rate rises to 6%, 9%, 12%, and 15%, the delays are 7.780 ms, 7.881 ms, 8.011 ms, and 8.113 ms, respectively. The RASR strategy reduces these delays by 2.8%, 2.7%, and 3.6%, compared with the three benchmark routing strategies. The RASR strategy maintains its advantage in latency performance primarily owing to its risk-aware mechanism, which proactively identifies potentially unstable network nodes and chooses reliable paths.

Figure 5 illustrates how path risk assessments vary across four routing strategies under different node failure rates. The experimental results show that throughout the testing process, the RASR strategy maintains the lowest path risk value throughout the entire testing period. Under the baseline condition of a 3% node failure rate, its path risk assessment value is only 1.617. As the failure rate gradually rises to 6%, 9%, 12%, and 15%, the risk values are 1.566, 1.555, 1.529, and 1.483, respectively. Under the stringent 15% failure rate condition, the RASR strategy reduces path risk values by 7.5%, 8.0%, and 8.5% compared with the shortest path strategy, minimum delay path strategy, and maximum bandwidth path strategy, respectively. Moreover, the risk values of all strategies exhibit a gradual downward trend.

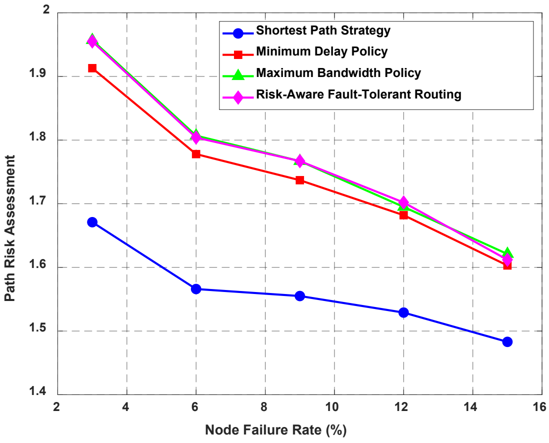

Figure 5. Comparison of Link Risk Assessment Among Algorithms Under Different Node Failure Rates

Figure 6 illustrates the variation in network throughput under various node failure rates for the four routing strategies. As shown in the experimental results of Figure 6, the throughput of all three traditional strategies shows a pronounced downward trend as the node failure rate increases.

In contrast, the RASR strategy demonstrates exceptional stability and superiority in throughput performance. Although it maintains lower throughput levels throughout testing, its decline curve remains relatively flat compared with the other three benchmark strategies. Throughput drops only from 28,158.282 at a 3% disruption rate to 26,049.659 at a 15% disruption rate—significantly lower than the performance degradation of traditional strategies. Under the stringent 15% failure rate condition, the RASR strategy's throughput surpasses both the shortest path and minimum delay path strategies. The relatively flat throughput decline curve of the RASR strategy indicates its robust performance stability in adverse network environments.

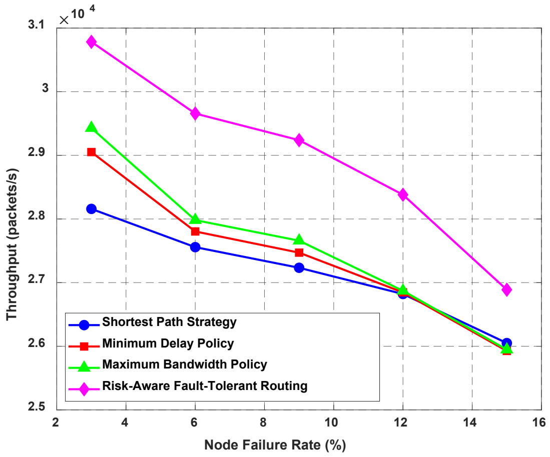

Figure 6. Comparison of throughput performance across algorithms under varying node failure rates

Figure 7 illustrates how path reliability varies across four routing strategies under different node failure rates. As shown in the experimental results of Figure 7, traditional benchmark strategies exhibit significant reliability deficiencies compared with RASR amid network failures. Owing to their lack of comprehensive network risk assessment capabilities, these traditional strategies fail to identify and avoid potential failure nodes and unreliable links effectively. Therefore, the selected paths face a high risk of transmission failure when the network is subjected to attacks.

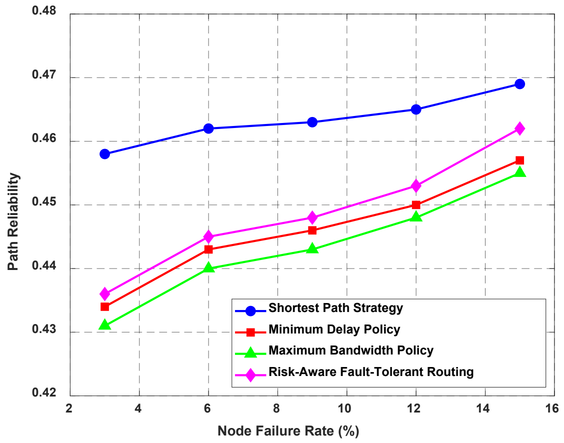

Figure 7. Comparison of Path Reliability Among Algorithms Under Different Node Failure Rates

In contrast, RASR demonstrates significant performance advantages in path reliability. Throughout the testing process, the RASR strategy consistently maintains the highest path reliability level. Under the stringent conditions of a 15% disruption rate, the RASR strategy achieves path reliability improvements of 2.6%, 3.0%, and 1.5% compared with the shortest path strategy, minimum delay path strategy, and maximum bandwidth path strategy, respectively. This outcome clearly demonstrates that the RASR strategy can more accurately identify and select truly reliable transmission paths in adverse network environments.

3.2.3 Adaptive Analysis of RASR Strategies for Different Network Demand Scenarios

The aforementioned experimental result validates the significant advantages of the RASR strategy over traditional routing strategies in terms of fault tolerance performance. However, real-world network environments feature diverse application demands, with varying performance requirements for routing strategies across different network scenarios. To further evaluate the practicality of the RASR strategy, this section presents an in-depth analysis specifically examining its adaptability across different network demand scenarios.

In the experiment, we designed four typical network demand scenarios: latency-sensitive, throughput-priority, high-reliability scenarios, and balanced. For each scenario, the corresponding performance objective was optimized by adjusting the weighting parameters within the RASR policy. Simultaneously, the node failure rate was maintained within a range of 3% to 15% to afford an observation of the policy's performance under varying fault intensities.

To quantify the comprehensive performance Cp across different scenarios, we employed a normalized comprehensive performance metric. This metric holistically evaluates multiple dimensions, including latency, throughput, packet loss rate, and path reliability. Its value ranges from 0 to 1, with higher values indicating superior overall performance. The calculation formula is as follows：

$$C_p = w_1 \times d^s_{(p_{sd})} + w_2 \times T^s_{avg} + w_3 \times R^s_{sd} \\ + w_4 \times reliability^s_{sd} \qquad (17)$$

where $d^s_{(p_{sd})}$ denotes the standardized delay metric, T^s_{avg} is the standardized throughput metric, R^s_{sd} is the standardized reliability metric, and reliability's sd signifies the standardized risk metric.

Figure 8 illustrates the comprehensive performance variations of the RASR strategy across four distinct network demand scenarios. The experimental results provide in-depth insights into the scenario adaptability characteristics of the strategy.

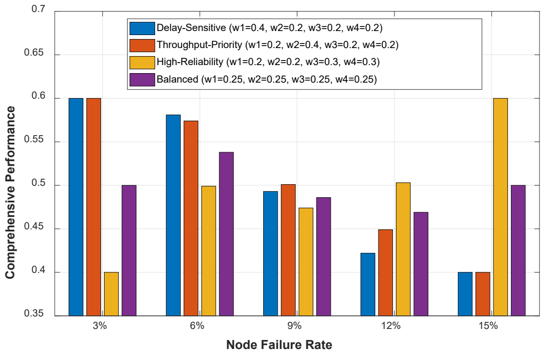

Figure 8. Comprehensive Performance of Risk-Aware Secure Routing Strategies Across Different Network Demand Scenarios

The experimental results demonstrate that the RASR strategy exhibits excellent adaptability to different network optimization objectives. In delay-sensitive network scenarios, the strategy's performance gradually declines from 0.600 at a 3% disruption rate to 0.400 at a 15% disruption rate. Although the performance degrades, it is relatively stable overall. In throughput-priority scenarios, the performance declines from 0.600 to 0.400, exhibiting a similar trend to that observed in latency-sensitive scenarios. Conversely, in balanced scenarios, the strategy achieves optimal stability, with the comprehensive performance metric value consistently hovering around 0.500, making it virtually unaffected by changes in node failure rates. Notably, the RASR strategy exhibits unique performance advantages in high-reliability network scenarios.

3.2.4 Melting Experiment

To verify the effectiveness of each component within the node risk value R(e) calculation module in improving the risk-aware fault-tolerant routing strategy, we also conducted ablation tests under network node failure rates of 3%, 6%, 9%, 12%, and 15%. The historical failure rate component and traffic load factor component were removed from the node risk value R(e) calculation formula in each scenario. The resulting routing strategies were then compared with the complete RASR routing strategy across various evaluation metrics. In ablation experiment 1, the historical failure rate factor was excluded from node risk value R(e) calculations, modifying (1) to the following:

$$R(e) = I(v) \times \frac{\deg(v)}{\sum_{e' \in E_v} bw(e')} \tag{18}$$

We replaced the original R(e) with the R(e) obtained using this new formula, calculated a new path from the source node to the destination node using the same routing policy, and used this new path as a baseline path for comparison.

In Melting Experiment 2, when calculating the average risk value R(e) for each node, we excluded the flow load factor from the equation. Thus, (1) is modified as follows:

$$R(e) = I(v) \times \left(1 + P_{fail}(v)\right) \tag{19}$$

We replaced the original R(e) with the R(e) obtained using this new formula, calculated a new path from the source node to the destination node using the same routing policy, and used this new path as a baseline path for comparison. The results are shown in Figure 9.

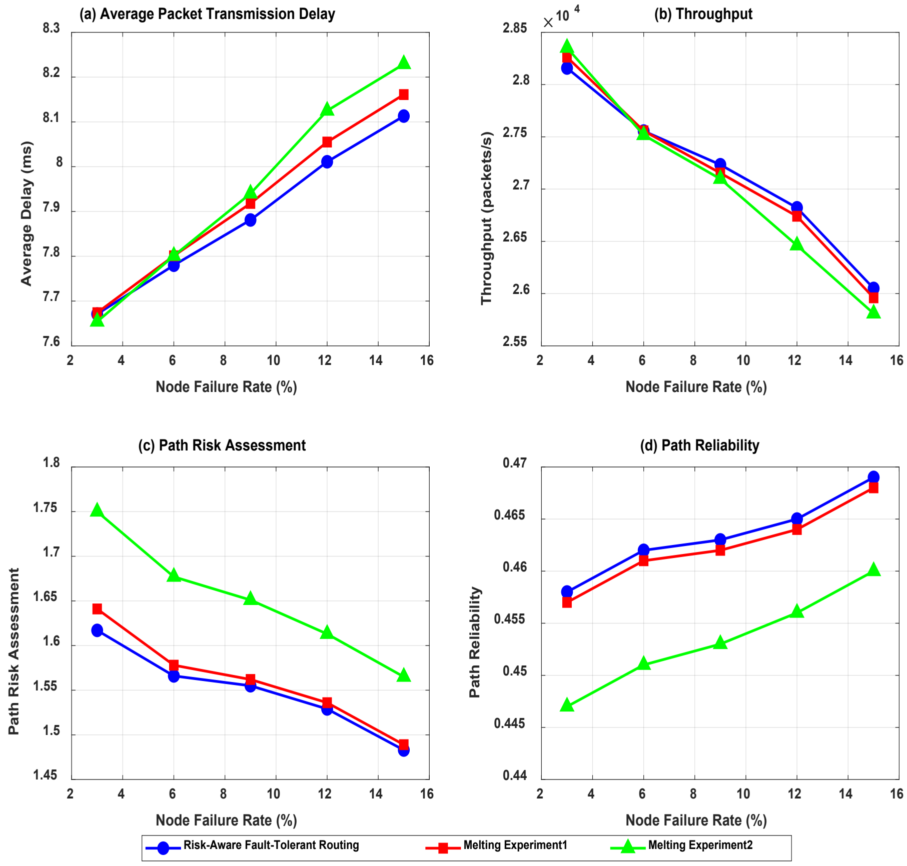

Figure 9. Ablation experiment results: (a) Average packet transmission delay varies with node failure rate; (b) Throughput varies with node failure rate; (c) Path Risk Assessment with Variation in Node Failure Rate; (d) Path Reliability as a Function of Node Failure Rate

A comparative analysis across four performance metrics reveals that the complete RASR strategy achieves optimal overall performance across all test scenarios. As shown in Figure 9(a), the average packet transmission delay of the complete strategy steadily increases from 7.674 ms at a 3% disruption rate to 8.113 ms at a 15% disruption rate. In contrast, both Ablation Experiment 1 and Ablation Experiment 2 result in significantly poorer delay performance than the complete strategy, with Ablation Experiment 2 reaching a peak delay of 8.229 ms at the 15% disruption rate. As shown in Figure 9(b), regarding throughput performance, the complete strategy maintains a relatively high throughput of 26049.659 at a 15% failure rate. In contrast, Ablation Experiment 1 and Ablation Experiment 2 drop to 25959.572 and 25809.187, respectively, with a more pronounced overall decline. This result indicates that the absence of both factors negatively affects network transmission efficiency under severe node failure rates. As shown in Figure 9(c), the complete strategy demonstrates optimal risk control capability in path risk assessment metrics, with its risk assessment value gradually decreasing from 1.617 to 1.489. At the same time, both ablation versions demonstrate relatively weaker risk control. Although Ablation Experiment 1 approaches the performance of the complete strategy, it consistently lags. Ablation Experiment 2's risk assessment value drops from 1.750 to a mere 1.565, indicating that the traffic load factor plays a crucial role in risk identification. As shown in Figure 9(d), regarding path reliability metrics, the complete strategy improves from 0.458 to 0.469, while ablation experiment 1 decreases from 0.457 to 0.468, and ablation experiment 2 only rises from 0.447 to 0.460. Their performance consistently lags significantly behind the complete strategy.

4. Conclusions

This study proposes a GNN-based RASR mechanism to address the lack of risk perception and fault tolerance capacities in power communication networks under complex attack environments. This study successfully designs a solution that integrates critical node identification, risk detection, quantitative assessment, and intelligent routing. This method overcomes the deficiencies in path risk perception of current routing algorithms and enables adjusting the routing strategies in real time based on network state changes. Experimental results demonstrate that under complex attack conditions, the RASR algorithm improves network survivability significantly. Additionally, it demonstrates excellent adaptability and flexibility in managing differentiated service demands for heterogeneous traffic types—including delay-sensitive, bandwidth-sensitive, and reliability-sensitive traffic. Even though RASR significantly increases security and fault tolerance, network throughput can still be optimized. Therefore, future research will concentrate on improving the current strategy.

Author Contribution

Conceptualization, Y.Z. (Yanjun Zhao), Y.Z. (Yue Zhang), X.Z., and L.L.; methodology, Y.Z. (Yanjun Zhao), Y.Z. (Yue Zhang), X.Z., L.L., X.W., and K.A.; software, Y.Z. (Yanjun Zhao), and Y.Z. (Yue Zhang); validation, L.L., X.W., and K.A.; formal analysis, Y.Z. (Yanjun Zhao), Y.Z. (Yue Zhang), and X.Z.; investigation, Y.Z. (Yanjun Zhao) and X.Z.; resources, Y.Z. (Yue Zhang); data curation, Y.Z. (Yue Zhang); writing—original draft preparation, Y.Z. (Yanjun Zhao), Y.Z. (Yue Zhang), and L.L.; writing—review and editing, Y.Z. (Yanjun Zhao), X.W., and K.A.; visualization, Y.Z. (Yue Zhang); supervision, Y.Z. (Yanjun Zhao) and X.Z.; project administration, K.A.; funding acquisition, K.A. All authors have read and agreed to the published version of this manuscript.

Acknowledgments

This research was funded by the Science and Technology Project of Inner Mongolia Power (Group) Co., Ltd. (No.2025-4-12).

Data Availability Statement

Data will be made available on request.

Ethical Approval

Not applicable

Competing Interest

The authors have no relevant financial or non-financial interests to disclose.

References

[1] Lin X, Yao Y, Hu B, et al. Enhancing power communication network security: A comprehensive cyber risk visual analytics framework with real-time risk assessment. Sust. Energy Grids Netw. 2024; 38:101325.

[2] Wen H, Xu, A, Qi H. Application of quantum key distribution in intelligent security operation and maintenance of power communication networks. Result Phys. (2023); 54:107041 https://doi.org/10.1016/j.rinp.2023.107041

[3] Somasundaram K, Kanna RP. Scalable hierarchical balanced clustering-based routing with multipath authentication for secured data transmission in large-scale multicast group communications. Expert Syst. Appl. 2025; 286:128149.

[4] K R MR, Katiravan J. Dynamic trusted cross-layer IDS for secured communications in wireless networks using routing algorithm and FT-CNN. J. Intell. Fuzzy Syst. 2024; 46:6171-6183.

[5] Zhang J, Yan Z, Wang H, et al. CCRPS: Customized cross-domain routing with privacy preservation and stable quality-of-experience based on deep reinforcement learning. Inf. Sci. 2025; 716:122255. https://doi.org/10.1016/J.INS.2025.122255

[6] Chen Y, Gu A, Cui L, et al. MTEAL: Network routing optimization of SD-WAN traffic engineering integrating multi-dimensional QoS metrics. J. Netw. Comput. Appl. 2025; 242:104272. https://doi.org/10.1016/J.JNCA.2025.104272

[7] Zhang F, Shi Y, Xu G, et al. Heuristic community path awareness based routing algorithm in opportunistic Networks. Ad Hoc Netw. 2025; 179:104005. https://doi.org/10.1016/J.ADHOC.2025.104005

[8] Meng Q, Liu L, Zhou D, Tang H, Zhang R, Liu X, Yan D. Application of Artificial Bee Colony Algorithm in Power Communication Network Routing Optimization Simulation. In Proceedings of the 2023 International Conference on Communication Network and Machine Learning, Zhengzhou, China, 27–28 October 2023; https://doi.org/10.1145/3640912.3640921

[9] Jin Z, Xu H, Kong Z, et al. A resilient routing strategy based on deep reinforcement learning for urban emergency communication networks. Comput. Netw. 2025; 257:110898.

[10] Bai J, Sun J, Wang Z, et al. An adaptive intelligent routing algorithm based on deep reinforcement learning. Comput. Commun. 2024; 216:195-208.

[11] Guo Y, Huang Z, Ding M, et al. PROM: A persistent routing optimization method based on supervised learning. J. Netw. Comput. Appl. 2025; 42:104223.

[12] Xiao L, Li S, Wen Q, et al. Load balancing routing algorithm of industrial wireless network for digital twin. Comput. Netw. 2025; 258:111059.

[13] He H, Li Y, Cheng K, Jiao Z, Guo H, Hou X. Research on Invulnerable Routing optimization in Power Communication Backbone Network based on Link-Risk Equalization. In 2023 5th International Academic Exchange Conference on Science and Technology Innovation (IAECST), 8–10 December 2023, Guangzhou, China. https://doi.org/10.1109/IAECST60924.2023.10503476

[14] Tian R, Gu J, Hou Z. Design of Network Routing Optimization Algorithm for Electric Power Communication System. In 2023 International Conference on Telecommunications, Electronics and Informatics (ICTEI), Lisbon, Portugal, 11-13 September 2023, https://doi.org/10.1109/ICTEI60496.2023.00063

[15] Cai J, Wu XS, Sun P. et al. Parameter optimization method for antimisalignment of inductive power transfer system based on a genetic algorithm. J. Power Electron. 2021; 21:1888–1899. https://doi.org/10.1007/s43236-021-00322-9

[16] Sun T, Wu J, Wang X, Zhou W, Li Z. A Risk Balanced Routing Optimization Method for Power Communication Private Networks. In 2023 3rd International Conference on Intelligent Power and Systems (ICIPS), Shenzhen China, 20–22 October 2023. https://doi.org/10.1109/ICIPS59254.2023.10405298

[17] Cheppali P, Selvakumar M. Hybrid optimal parent selection based energy efficient routing protocol for Low-Power and lossy networks (RPL) routing. Expert Syst. Appl. 2025; 277:127011. https://doi.org/10.1016/J.ESWA.2025.127011

[18] Arat F, Akleylek, S. Security-aware RPL: Designing a novel objective function for risk-based routing with rank evaluation. Comput. Netw., 2025; 260:111122.

[19] Lin Z, Zeng Z, Yu Y, et al. Graph Attention Residual Network Based Routing and Fault-Tolerant Scheduling Mechanism for Data Flow in Power Communication Network. Comput. Mater. Continua 2024; 81:1641-1665.

[20] Xiang, K., Fan, L., Shen, R. et al: Topology derivation of a single-phase bridgeless three-level PFC converter based on graph theory. J. Power Electron. (2025). https://doi.org/10.1007/s43236-025-01135-w

[21] Moreno Y, Pastor-Satorras R, Vespignani A. Epidemic outbreaks in complex heterogeneous networks. Eur. Phys. J. B 2002; 26:521-529.

[22] Xia F, Liu T, Wang J, Zhang W, Li H. Listwise approach to learning to rank: theory and algorithm. In Proceedings of the 25th international conference on Machine learning, Helsinki, Finland, 5–9 July 2008. https://doi.org/10.1145/1390156.1390306.