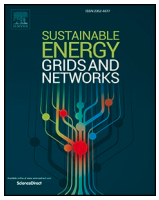
Sustainable Energy, Grids and Networks 43 (2025) 101927

Contents lists available at ScienceDirect

Sustainable Energy, Grids and Networks

journal homepage: www.elsevier.com/locate/segan



Power system resilience enhancement using graph learning: A comprehensive robustness and antifragility approach

Kasra Shafiei *, Saeid Ghassem Zadeh *, Mehrdad Tarafdar Hagh

Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz 51666-16471, Iran

ARTICLE INFO

Keywords:
Power system
Resilience
Comprehensive robustness
Antifragility
Graph learning

ABSTRACT

The increasing vulnerability of power systems to extreme events underscores the need for enhanced resilience strategies. Resilience-based approaches fail to address the complexities of large-scale disruptions, necessitating a paradigm shift toward comprehensive robustness (CR) and antifragility. This study presents a novel graph learning-based framework for improving power grid resilience by modeling electrical networks as weighted multigraphs. The proposed method systematically identifies critical vulnerabilities, optimizes structural configurations, and strengthens connectivity to mitigate cascading failures. By integrating CR metrics, this research ensures that power systems adapt and are resilient in response to vulnerabilities. Extensive simulations on IEEE networks validate the approach, demonstrating resilience improvements of up to 74 % in the IEEE 118-bus system. Similar enhancements are observed in other IEEE test cases, depending on the reconfiguration strategy against malicious and random attacks. Furthermore, the study introduces antifragility principles to power systems that enhance resilience under adverse conditions. The findings contribute to developing adaptive and resilient grid infrastructures capable of sustaining operational integrity in vulnerable environments.

1. Introduction

1.1. Motivation

The increasing occurrence of extreme vulnerabilities in electric grids due to natural disasters and cyberattacks has led to widespread power outages, emphasizing the need for enhanced power system resilience. Traditional *N-1* design criteria for power networks are often inadequate in addressing severe events, necessitating advanced strategies to mitigate vulnerability.

Recent advancements in power systems, particularly graph learning techniques, offer a promising approach to improving power grid robustness. By modeling power networks as weighted multigraphs, it becomes possible to identify critical vulnerabilities and reconfigurations and enhance system robustness. However, existing resilience enhancement strategies primarily focus on reliability rather than comprehensive robustness (CR) and antifragility, limiting their effectiveness in extreme conditions.

This study leverages graph learning-based methodologies to address these challenges and improve power grid resilience. The proposed framework identifies critical nodes, applies strategic edge augmentation, and employs topological reconfiguration to mitigate the impacts of attacks. Using CR metrics and graph-based structural optimization strategies such as critical node identification and optimal edge addition, this study translates resilience theory into practical solutions that measurably improve network robustness and enable adaptive reconfiguration under targeted and random disruptions.

1.2. Literature review

The global transition in the energy sector during the 21st century plays a critical role in ensuring the reliability, resilience, and security of modern power system operations [1]. Achieving these goals requires the development of advanced and intelligent power infrastructures [2]. Large-scale outages not only incur substantial recovery costs but also pose significant threats to economic stability worldwide. Traditional *N-1* contingency criteria, while once sufficient, are increasingly inadequate in the face of growing risks such as natural disasters and cyber-physical attacks [3].

A resilient power system ensures uninterrupted power supply during normal conditions, enables rapid recovery following disturbances, minimizes the risk of equipment damage, and reduces vulnerability to natural disasters and cyberattacks [4]. To address these challenges, it is

* Corresponding authors.
E-mail addresses: k.shafiei@tabrizu.ac.ir (K. Shafiei), g_zadeh@tabrizu.ac.ir (S.G. Zadeh).

https://doi.org/10.1016/j.segan.2025.101927
Received 28 March 2025; Received in revised form 7 July 2025; Accepted 9 August 2025
Available online 13 August 2025

Nomenclature

q	Number of nodes that have failed and been removed from the network
$s(q)$	Evaluate the integrity of the network after these q nodes are removed
N'	Size of the largest connected component
η	Number of edges adjacent to the node
γ	Scaling factor
$\sigma\ (s, t \mid e)$	Shortest paths between nodes s and t that pass through edge e
$\sigma\ (s, t)$	Total number of shortest paths between s and t
k_i	Total number of nodes connected to node i
e_i	Number of edges linking the neighboring nodes of node i
d_{ij}	Shortest route between node i and$j$.
$N = n$	Number of total nodes
$E = e$	Number of edges
$G\ (0)$	Size of the largest connected subgraph before any attack
$G(q)$	Size of the largest connected subgraph after k attacks
$\sqrt{WiWj}$	Maximum power transfer between a generator (Wi) and a load (Wj) node pair
F	External force
σ	elastic deformation
σ_c	critical elastic deformation
qc	Critical threshold network
$q,\ q_l$ *and* $q_{l\text{-}1}$	Fractions of the removed nodes
$1 - G(q)$	Level of network degradation
q_{cI}	Critical threshold of the modified network
$G_I(q)$	Energy level of the improved network resilience after adding edge (I, j),
$G_O(q)$	Energy level of the original network
$q_\omega,\ q_1$	Fractions of the removed nodes
$C_{c,c}$	Critical giant component of the modified network

essential to anticipate potential outages caused by extreme events across various scenarios [5]. Enhancing system resilience and adaptability requires structural reconfiguration and the adoption of advanced network strategies. In parallel, power markets have emerged as key enablers in promoting resilience, often focusing on economic optimization, such as mitigating price volatility, encouraging investment in robust infrastructure, and managing demand during outages [6,7]. Novel approaches increasingly integrate renewable energy sources [8], energy storage systems [9], and electric vehicles [10] to support flexible, market-driven resilience models. Moreover, the incorporation of hybrid distributed generation units, like photovoltaic arrays and wind turbines, into distribution networks improves voltage stability, lowers power losses, and reduces operational costs, contributing to a more resilient system [11].

Network robustness refers to a system's ability to maintain operational performance despite attacks, faults, or disruptions. As a foundational concept in network analysis, it has garnered considerable attention, particularly in the context of complex infrastructures such as power grids. Advances in defining and measuring robustness—using a range of metrics and modeling approaches—have enabled significant progress in enhancing network design, management, and security. However, many challenges and open questions remain. As emerging technologies introduce new layers of complexity and uncertainty, understanding how different network topologies, connection patterns, and interaction dynamics influence overall resilience continues to be a critical area of research [12].

Vulnerabilities in power systems can lead to service interruptions or even complete network failures, often resulting in significant economic and operational losses. As a result, designing resilient networks with high robustness against random faults and targeted attacks has become a key priority for power system planners and policymakers. The dynamic behavior of networked systems has received increasing attention in recent research efforts [13], with a strong focus on enhancing structural robustness [14] and developing reliable network models [15]. These studies provide valuable insights into the underlying structure of power networks and introduce practical strategies for assessing and improving their resilience.

Network attacks are generally classified into two main categories: malicious and random. Malicious attacks [16] deliberately target the most critical components of a network, such as high-degree nodes or key edges [17], often with the intent of causing maximum disruption through strategic sabotage. In contrast, random attacks occur without specific targeting and typically result from unexpected component failures due to wear, aging, or unforeseen technical faults [18].

In the study of malicious attack scenarios, researchers typically distinguish between two primary types of damage: direct structural destruction, also known as simple malicious attacks [14] and cascading failures [19]. The first involves deliberately removing critical nodes or connections, leading to immediate fragmentation and potential overloads in the remaining network. Such attacks can severely disrupt power flow and create congestion, particularly when high-centrality components are compromised. Numerous studies have explored strategies to assess and mitigate this damage in critical infrastructures like electric power systems [14].

The second model, the cascading failure effect, is where the failure of overloaded components triggers successive breakdowns throughout the network [20,21]. Various modeling approaches have been developed to simulate this phenomenon and evaluate system responses. These efforts have expanded the understanding of network resilience and led to methods to reinforce systems against widespread collapse [22,23].

While these two failure types are often treated separately, real-world power systems operate in highly interconnected and complex environments where multiple disturbances can occur simultaneously. As highlighted in [24–26], both direct structural loss and cascading failures may impact a single system at the same time. Therefore, enhancing CR, the ability of a network to withstand types of disruption, is essential. Improving CR ensures power networks are more resilient to both targeted malicious attacks and the secondary effects of cascading failures.

Topological analysis serves as a fundamental approach in identifying critical nodes within complex network theory, particularly in the context of power systems. One notable strategy involves defensive islanding algorithms [27], which aim to enhance grid resilience by segmenting the network into smaller, stable, and self-sufficient sub--networks, or islands, in response to severe disruptions. This islanding process can be interpreted as a detection problem [28], where the goal is to identify vulnerable components and isolate them to prevent cascading failures that could otherwise lead to widespread system collapse.

While such protective methods can improve network availability and help contain disturbances, they are insufficient to ensure full system dependability. To address these limitations, a high-availability subgraph approach has been proposed [29], offering a more robust structural framework to maintain operational integrity under adverse conditions.

A more advanced methodology improves power system resilience by detecting topological attacks and optimizing load restoration in abnormal situations, such as cyberattacks and natural disasters, using machine learning for intrusion detection for topological reconstruction. This enables pre-event and post-event strategies, such as microgrid formation [30]. However, the focus remains primarily on recovery and fault detection, often neglecting antifragility and comprehensive robustness (CR) across diverse failure scenarios.

Recent studies on power network resilience and vulnerability have introduced optimization models and advanced algorithms to improve network connectivity and accessibility. These include optimizing backup and operational paths using linear constraint models, strengthening weak edges through traversal-tree-based analysis, and enhancing node connectivity with dual-tree-based consolidation techniques. Such methods reduce computational complexity, boost resistance to random disruptions, and improve resilience while maintaining cost-efficiency [31–33].

Furthermore, efforts have been made to reinforce the robustness of cyber-physical systems with weak interdependencies and to assess the vulnerability of transmission networks using adjacent graph models. These approaches help detect structural weaknesses and improve resilience against cascading failures [34,35].

In analyzing power network vulnerability and resilience, various multi-strategy frameworks and clustering-based models have been proposed to identify critical nodes and optimize post-disaster restoration. These approaches include frameworks designed to enhance the seismic resilience of substations, techniques for subnet division and power dispatch in multi-source grids, and integrated evaluations of reliability, robustness, and overall resilience of power system topologies. Collectively, these strategies aim to improve network performance under extreme and uncertain conditions [36–42].

In parallel, research on targeted attacks and branch contingencies has introduced weighted topological models and triangle counting techniques to accurately locate vulnerable components and reinforce system resilience against potential disruptions [43–45]. Together, these developments provide a comprehensive toolkit for vulnerability assessment by integrating theoretical advancements with practical applications, ultimately strengthening the resilience of critical infrastructure against a wide range of threats [46–48].

Significant advancements have also been made in leveraging deep reinforcement learning (DRL) and graph-based methods to enhance the resilience of power distribution systems, particularly against extreme weather events, cyberattacks, and operational uncertainties. Novel DRL-based frameworks have been proposed to optimize grid hardening strategies for hurricane resilience, employing Markov decision processes to maximize life-cycle resilience by considering multiple stochastic events, thus surpassing traditional methods that target single hazards [49]. Multi-agent DRL approaches have been developed to coordinate shunt resources and microgrid formation, improving load restoration and system robustness under disaster scenarios by enabling adaptive decision-making in dynamic environments [50,51].

Additionally, DRL paradigms have been introduced to enhance the resilience of electric vehicle charging stations against cyber-attacks, while graph autoencoder-based methods have been developed to detect power attacks in electrified transportation systems, leveraging graph neural networks to identify anomalous patterns with high accuracy [52–54]. Comprehensive reviews and graph-based metrics, alongside resource allocation models based on modularity concepts, have further advanced the field by providing structured frameworks to quantify and enhance resilience, addressing high-impact, low-probability events in cyber-physical systems and optimizing distributed energy resource placement for fault isolation and service continuity [55,56]. Ensembled DRL methods have been proposed to reconfigure distribution systems during outages, maximizing critical load supply through microgrid formation and outperforming traditional model-based approaches in scalability and adaptability [57]. These DRL- and graph-driven innovations collectively offer scalable, model-free solutions that enhance the adaptability and resilience of power systems under complex and unpredictable conditions.

However, despite these advancements, existing DRL and graph-based approaches remain primarily focused on recovery and fault detection, often overlooking critical aspects such as network reconfiguration and CR under both malicious and random failure scenarios. Moreover, many of these methods rely on simplified or unweighted models. In contrast, the present study addresses these limitations by introducing a graph learning-based framework that models power grids as weighted multigraphs. This approach enables the precise identification of critical nodes and edges and enhances resilience based on the CR metric through optimal edge augmentation.

1.3. Research gaps

Despite notable progress in advancing power system resilience, many existing approaches face fundamental limitations. These challenges highlight the need for a paradigm shift toward frameworks that enhance resilience and promote the antifragility of power systems in the face of diverse and evolving failure scenarios. One critical gap lies in the absence of comprehensive models that simultaneously capture the functional interdependencies and the structural complexities inherent in modern power grids. This deficiency has hindered the development of scalable, practical solutions suitable for real-world applications. By leveraging graph learning techniques to systematically identify vulnerabilities and optimize network configurations, while integrating CR and antifragility metrics, it becomes possible to bridge these gaps and enable the design of more adaptive, resilient grid infrastructures. Table 1 presents a comparative analysis of this study against previous research, highlighting existing shortcomings and positioning the current work within the context of resilience-focused innovations.

Despite significant advancements in enhancing power system resilience and network robustness, several critical gaps remain unaddressed:

- Existing vulnerability frameworks primarily address random attacks but cannot quantify and improve resilience against malicious attacks. This gap hinders the development of the resilience of power systems that maintain functionality under malicious attacks.
- Many existing algorithms are constrained by theoretical frameworks that lack practical implementation in large-scale, real-world power systems. There is a gap in translating theoretical insights into scalable and deployable solutions that address the operational complexities of modern power networks.
- The application of the graph method based on complex networks for analyzing and enhancing the resilience of power systems remains underexplored, limiting the ability to identify and reinforce critical components efficiently.
- Unweighted graph models fail to capture the dynamics of power grids. There is a need for weighted multigraph approaches to provide a more accurate and detailed understanding of system vulnerabilities and their impact on network stability.

Addressing these gaps is essential to developing resilience and antifragility of power systems that are adaptive and capable of robustness to increasingly malicious and random attacks.

1.4. Contributions

The strategy for enhancing power system resilience is structured around four fundamental pillars, as depicted in Fig. 1: Robustness, Adaptation, Reconfiguration, and Antifragility. These pillars collectively contribute to the stability and security of the power system by integrating structural robustness, adaptation, and reconfiguration mechanisms.

Robustness focuses on fortifying the power system against various threats, including malicious attacks, random failures, and extreme weather events. The power system can withstand adversities and maintain operational continuity by implementing reinforcement strategies and strengthening critical components.

Adaptation involves adaptive network reconfiguration, graph learning-based complex network adjustments, and vulnerability response mechanisms. These strategies enable real-time adjustments, ensuring the system can dynamically respond to disturbances and

Table 1
Comparison of this study with various studies.

Number of Ref.	Power network model	Complex network	Graph method	Resilience metrics		Comprehensive Robustness	Antifragility	Vulnerability		Year
				Evaluation	Enhancement			Malicious attack	Random attack	
[31]	×	×	✓	✓	✓	×	×	×	×	2024
[32]	×	✓	✓	✓	✓	×	×	×	✓	2024
[33]	×	✓	✓	×	×	×	×	×	✓	2024
[34]	✓	✓	×	✓	✓	×	×	×	✓	2023
[35]	✓	✓	✓	✓	×	×	×	×	×	2019
[36]	✓	×	✓	✓	✓	×	×	×	×	2024
[37]	✓	✓	✓	✓	✓	×	×	×	✓	2023
[38]	✓	×	✓	✓	✓	×	×	×	✓	2022
[39]	✓	✓	×	✓	✓	×	×	×	✓	2024
[40]	✓	✓	✓	×	×	×	×	×	×	2022
[41]	✓	✓	✓	✓	✓	×	×	×	✓	2022
[42]	✓	×	✓	✓	✓	×	×	×	✓	2024
[43]	×	✓	✓	✓	×	×	×	✓	✓	2023
[44]	✓	✓	✓	✓	×	×	×	✓	✓	2020
[45]	✓	✓	×	✓	×	×	×	×	✓	2022
[46]	×	×	×	✓	×	×	×	×	✓	2023
[47]	×	✓	✓	×	×	×	×	×	✓	2023
[48]	×	×	✓	✓	✓	×	×	×	✓	2022
[49]	✓	×	×	✓	✓	×	×	×	✓	2021
[50]	✓	×	×	✓	✓	×	×	×	✓	2021
[51]	✓	×	✓	✓	×	×	×	×	×	2022
[52]	✓	×	×	✓	✓	×	×	✓	×	2024
[53]	✓	×	×	✓	×	×	×	×	×	2023
[54]	✓	×	✓	✓	×	×	×	✓	✓	2024
[56]	✓	×	✓	✓	✓	×	×	×	×	2021
[57]	✓	×	✓	✓	✓	×	×	×	✓	2025
This paper	✓	✓	✓	✓	✓	✓	✓	✓	✓	

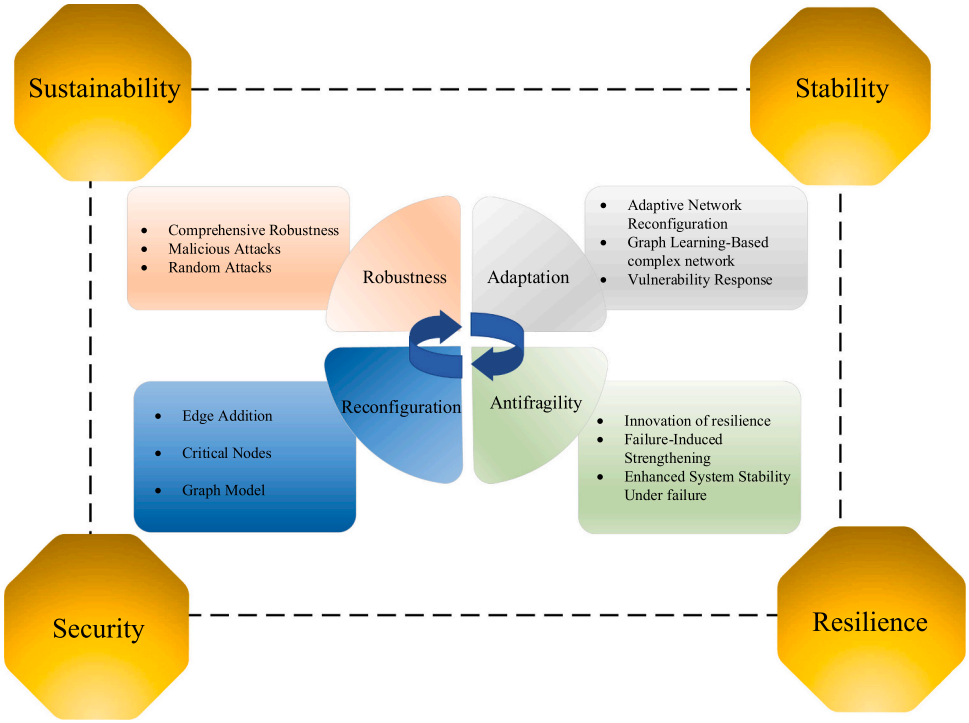


Fig. 1. Classification of Resilience Enhancement Pillars.

mitigate cascading failures. The ability to adjust and restructure the network topology enhances resilience, allowing the system to maintain functionality under various vulnerability conditions.

Reconfiguration is a crucial pillar involving edge addition, critical node identification, and graph-based structural optimization. The power system can reorganize its topology through these methods, improving connectivity and resilience against disruptions. Unlike conventional approaches that rely solely on distributed generation, this study leverages graph learning techniques for network reconfiguration and bolstering resilience. Edge augmentation strategies strengthen weak points and reinforce critical nodes, reducing system vulnerability and enhancing overall performance.

Antifragility extends beyond robustness by leveraging system failures as opportunities for improvement. Key aspects include innovation

in resilience, failure-induced strengthening, and enhanced system stability under failure conditions. By adopting these mechanisms, the power system can evolve and improve its ability to handle vulnerability.

The contributions of this study are as follows:

- A novel graph learning-based framework is proposed in which power grids are modeled as weighted multigraphs, allowing for precise analysis of network robustness and resilience. Using graph-theoretical metrics such as betweenness centrality and degree centrality, the framework systematically identifies critical nodes and edges that significantly influence system resilience. The placement of additional transmission lines is optimized using the posteriorly adding (PA) algorithm, which enhances resilience by strategically reconfiguring the network based on robustness metrics.
- The concept of comprehensive robustness (CR) is integrated into the framework to quantify and improve power system resilience against both random and malicious attacks. Unlike conventional approaches that focus primarily on random failures, the proposed methodology evaluates network performance under diverse attack scenarios, addressing key gaps in existing resilience assessment models. The CR-based enhancements effectively mitigate structural vulnerabilities and support the development of more robust power system infrastructures.
- The resilience framework is extended beyond conventional definitions by incorporating graph-based reconfiguration, allowing the power system to maintain functionality under adverse conditions. Network reconfiguration strategies restructure the topology in response to failures, reinforcing weak components through optimal edge addition and critical node identification. This approach leads to improved structural robustness and enhanced system performance under various failure scenarios.
- Extensive simulations on IEEE standard test networks validate the proposed approach, demonstrating significant resilience improvements. Effectiveness in power grid applications is showcased by optimizing network structure and reducing vulnerability points, visualized through weighted multigraph representations highlighting critical nodes and optimal edge placements.

The remainder of this paper is structured as follows:

Section 2 introduces the conceptual framework. Section 3 outlines the mathematical formulations. Section 4 presents numerical results. Section 5 summarizes the findings and concludes the study.

2. Antifragility and the innovation of resilience

Recent technological advancements have significantly contributed to enhancing the resilience of power systems against a range of threats, including natural disasters, cyberattacks, and major equipment failures. Key technologies that support grid stability include islanding and black-start capabilities, cybersecurity protocols, wide-area monitoring and control systems, demand-side management, electric vehicle integration, renewable energy sources, and energy storage systems.

As power systems grow increasingly complex, the demand for innovative and adaptive technologies becomes more urgent. Traditional resilience strategies primarily focus on withstanding disruptions and restoring functionality. In contrast, the emerging concept of antifragility introduces a transformative shift: systems recover from disturbances and adapt and strengthen as a result. This perspective challenges conventional design by framing failure as an opportunity for improvement.

Antifragility suggests that some systems withstand disruptions and uncertainties and improve and strengthen in adversity. This transformative approach challenges conventional resilience strategies by emphasizing adaptation and growth rather than recovery.

Fig. 2 illustrates the evolution from resilience to antifragility, highlighting the shift toward a more dynamic and flexible energy system.

An antifragile system not only endures uncertainties but also adapts, improves, and evolves when exposed to unpredictable challenges, often surpassing its original performance expectations. Although some studies have explored fragility modeling within energy systems, this field remains relatively underdeveloped. There is a clear need for further research to fully understand and apply antifragility concepts in designing future power infrastructures [58].

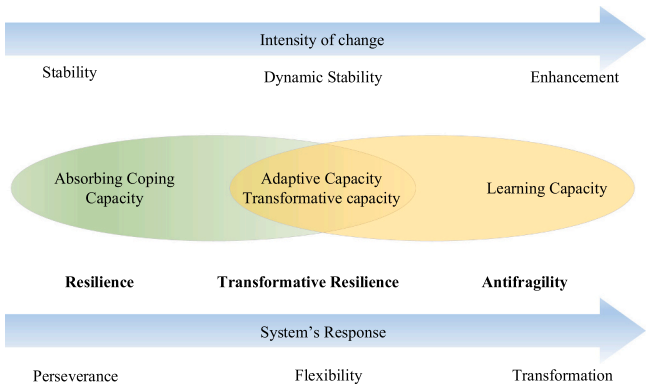


Fig. 2. Resilience, Transformative Resilience, and Antifragility.

A key enabler of this transition is learning, as continuous improvement and innovation emerge from resilience-driven strategies. By shifting focus from mere recovery to adaptive transformation, antifragility introduces a new paradigm for achieving sustainability and operational efficiency in modern power systems [59].

2.1. Future perspective of power systems resilience

Power system infrastructures are transforming significantly through two main development strategies: Greenfield and Brownfield projects. These approaches differ in design, implementation methods, and strategic objectives, yet both play essential roles in enhancing system resilience.

The Greenfield approach focuses on building entirely new infrastructure. For example, developing a new power plant with state-of-the-art technologies enables higher reliability, sustainability, and resilience [60]. This method provides the flexibility to integrate modern innovations without being constrained by legacy systems, making it ideal for meeting long-term energy and stability goals.

In contrast, the Brownfield approach, often called power system restructuring, targets modernizing existing infrastructure. This strategy strengthens the resilience of aging systems by incorporating advanced technologies and adapting to increasingly severe operational challenges, such as natural disasters or cyber-physical threats. While Brownfield projects are generally more cost-effective and quicker to implement, they can face significant hurdles, including compatibility issues, scalability limitations, and legacy system constraints.

Recognizing the distinctions between these two approaches is critical for stakeholders in the energy sector. A hybrid strategy that balances Greenfield innovation with Brownfield upgrades can effectively reduce system vulnerabilities and support the development of a more adaptive, robust, and resilient power grid.

A comparative overview of the strengths and limitations of Greenfield and Brownfield strategies is presented in Fig. 3.

2.2. Complex network

Over the past few decades, complex networks have emerged as powerful tools for analyzing and understanding intricate systems across various domains, including power systems [61]. Their ability to model and evaluate the dynamic interactions within large-scale infrastructures has made them indispensable in resilience-focused research.

In practical scenarios, the functionality and stability of a network can

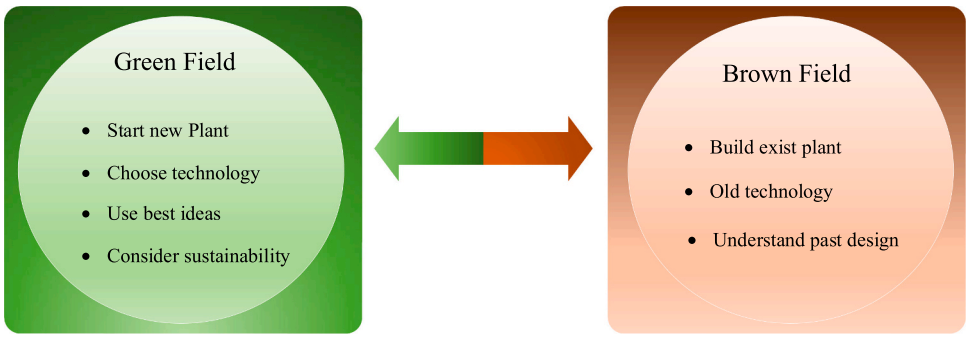


Fig. 3. Greenfield vs Brownfield.

be significantly compromised when specific components are attacked or fail. Random failures and malicious attacks can disrupt network resilience, leading to cascading outages and widespread network interruptions. In power grids, such cascading failures occur when localized disruptions, such as line faults or cyber intrusions, propagate through the system, triggering large-scale blackouts [62,63].

Various strategies have been developed to target network vulnerabilities by disrupting key structural elements. One of the most impactful methods involves eliminating highly influential nodes, which often play a central role in maintaining resilience. This approach typically relies on topological indicators such as degree and centrality to determine node importance [64]. To intensify the impact of such attacks, hierarchical frameworks have been proposed that rank and target groups of nodes based on their structural significance, thereby maximizing disruption to network resilience [65].

The structural integrity of a network also depends heavily on specific subnetwork patterns. Multi-string structures, which create redundant or alternative paths between critical components, are especially vital in preserving resilience under adverse conditions [66]. Power networks, as a subset of complex systems, present unique challenges. Core nodes, such as control centers and major substations, form intricate interaction patterns that play a pivotal role in grid resilience. These systems typically have short path lengths and relatively high clustering coefficients, characteristics that are closely linked with performance degradation under stress [67].

Although power networks do not perfectly follow scale-free degree distributions, they still contain several critical nodes of disproportionate importance. These nodes make the network especially vulnerable to targeted attacks [68]. The removal of such pivotal elements can cause severe cascading effects, far beyond what would result from random node failures. Therefore, topology-based identification of critical nodes is vital in understanding system behavior, diagnosing vulnerabilities, and ensuring secure and grid resilience [67,69].

2.3. Critical node identification

Identifying critical nodes within complex networks is fundamental to understanding network behavior and enhancing overall system resilience. In the context of power systems, accurately detecting these pivotal nodes is especially important due to their direct influence on resilience, robustness, and vulnerability to disruptions.

Conventional methods for critical node identification are generally divided into two main categories[70]:

- Global property-based approaches assess the overall structure of the network to determine node importance. Common metrics include closeness centrality and betweenness centrality, which provide high-resolution rankings by evaluating a node's influence across the entire network. However, these methods often involve high computational complexity, making them less practical for large-scale power networks [71].
- Local property-based approaches focus on neighborhood-level characteristics, offering more efficient computations. Metrics such as degree centrality [72] and the clustering coefficient [13] are widely used in this category. While these techniques are computationally lightweight, their lower accuracy can limit effectiveness, particularly in systems like power grids where precision in identifying critical nodes is essential

2.4. Graph learning

Networks serve as intuitive and effective representations of system structures, offering valuable insights into the complex interdependencies that define real-world systems. As a result, extracting meaningful information and uncovering hidden patterns within networks has become a growing area of research interest.

The structural properties of a network can often reflect its dynamic behavior. Metrics such as node degree [73], assortativity [15,74], and the shortest path length [16] are commonly used to characterize network features and evaluate performance. However, despite their usefulness, these methods can be computationally intensive, especially when applied to large-scale networks, making them less practical for large-volume analysis.

Graph learning techniques [75–77] have emerged as a promising alternative. These methods enable efficient analysis and interpretation of complex network structures by reducing their dimensional complexity while retaining key topological information.

Graph learning transforms a network into a low-dimensional vector space at its core, allowing for scalable computation and deeper structural analysis. Given a network represented by an $N \times N$ adjacency matrix, graph learning encodes each node as a vector in a d-dimensional space. This process produces an $N \times d$ matrix that captures the network's structure in a continuous and compact numerical form. By embedding discrete relationships into continuous representations, graph learning significantly improves the efficiency and flexibility of network-based analysis.

3. Formulations

A power grid can be effectively modeled as a complex network, where generator and load buses are nodes, and transmission lines represent the edges connecting them [78]. When all transmission lines are treated equally, the network is considered unweighted. However, if variations in line weights are introduced based on cost, capacity, or other operational criteria, the network becomes weighted [79,80].

The vulnerability of a power grid is typically linked to unexpected events, such as faults or attacks, and is often measured by the resulting loss in overall network performance. Accurately modeling these disruptions is essential for assessing and improving grid resilience. One widely used approach relies on topological modeling, which focuses purely on the structural configuration of the network without incorporating power flow. This perspective enables the evaluation of structural

vulnerability by simulating random and targeted attacks, particularly on nodes and lines with high betweenness centrality or high degree. By analyzing the impact of such disruptions, the topological model provides critical insights into the robustness of the grid under various failure scenarios.

3.1. Robustness evaluation by vulnerability metrics

Power systems are inherently vulnerable to random failures and targeted attacks, making it essential to assess their structural weaknesses systematically. In this research, a graph learning framework grounded in complex network theory is employed to evaluate and enhance the resilience of power grids. Specifically, vulnerability metrics are introduced and applied to benchmark systems, including the IEEE 14-, 24-, 39-, and 118-bus networks.

The giant component index is a key measure for assessing power grid vulnerability. These metrics provide insights into the grid's transmission efficiency and structural integrity [44].

The ability of a power grid to withstand malicious or random attacks is a crucial measure of its robustness. A central challenge for system operators and planners is determining whether the network can maintain resilience under attacks. In this context, evaluating network robustness becomes a key aspect of resilience analysis.

To quantitatively capture robustness, a numerical index R is used to measure the evolution of the largest connected component (LCC) as the network degrades, following the method defined in [14].

$$R = \frac{1}{N}\sum_{q=1}^{N} s(q) \tag{1}$$

As disruptions occur, the network may fragment into multiple disconnected parts. Only nodes within the largest connected subcomponent are considered operational, emphasizing the importance of maintaining a cohesive core during failures.

3.2. Degree of node

In an undirected and unweighted graph $G= (N, E)$, the degree of a node x refers to the number of edges directly connected to it [44].

$$x_n = \sum\nolimits_{e\in E} \eta_e^n \tag{2}$$

Analyzing the distribution of node degrees provides important insights into the topological structure of a network. The function p(x) describes the degree distribution, which represents the probability that a randomly selected node has degree x.

In real-world networks, degree distributions frequently follow established statistical models such as Poisson, Gaussian, exponential, or power-law distributions. Among these, the power-law distribution is particularly relevant in the context of power grids. In this type of distribution, the likelihood of encountering a node with degree x declines polynomially as x increases. In other words, nodes with high degrees are rare, while those with low degrees are more common.

Networks exhibiting this pattern are called scale-free networks, where the term "scale-free" denotes the consistent mathematical relationship between degree and probability across all scales. Mathematically, this can be expressed as:

$$p(x) = x^{-\gamma} \tag{3}$$

3.3. Betweenness centrality

Betweenness centrality is a key metric that quantifies the extent to which a node lies on the shortest paths between other nodes in a network. In power systems, nodes with high betweenness centrality function as critical intermediaries for power transfer across the grid. Because they facilitate connectivity between different network regions, their failure or removal can cause significant disruptions and fragmentation.

This metric is not limited to nodes; it can also be applied to edges, assessing how essential a transmission line is to overall network flow. In this case, edge betweenness centrality measures the fraction of all shortest paths between node pairs that pass through a specific edge. It reflects the edge's structural importance in maintaining efficient communication and power flow across the network. The betweenness centrality of an edge can be mathematically expressed as follows [81]:

$$BC(e) = \sum_{s,t\in V} \frac{\sigma(s,t|e)}{\sigma(s,t)} \tag{4}$$

Understanding and evaluating betweenness centrality helps identify vulnerable elements in the grid, providing insight into potential failure points and supporting the development of more robust and resilient network designs.

3.4. Clustering coefficient

The clustering coefficient is a key metric to evaluate the degree of interconnectedness among a node's immediate neighbors. Specifically, it quantifies how many possible connections between a node's adjacent nodes exist. For a given node i, the clustering coefficient is defined as the ratio of the number of existing edges between its neighbors to the total number of potential edges that could exist among them [82].

$$C_i(G) = \frac{2e_i}{k_i(k_i-1)} \tag{5}$$

This metric does not account for the distances between nodes; rather, it focuses solely on the local connection pattern within the neighborhood of each node. The clustering coefficient is commonly used to compare local cohesiveness across different networks, but it can also provide meaningful insights when analyzing a single network.

Understanding the distribution of clustering coefficient values across the network helps summarize the overall degree of clustering. A clustering coefficient closer to 1 indicates a more tightly connected and locally robust network structure, which is especially relevant for systems like power grids, where localized redundancy contributes to overall stability and resilience [83].

3.5. Path length

The path length, denoted as $D(G)$, represents the average shortest distance between all pairs of nodes within a network [84]. This metric offers insight into the network's overall structure, particularly the degree of separation between its elements. A shorter average path length indicates more efficient communication and transmission, crucial for systems such as power grids, where timely and reliable flow is essential.

The path length for a network G is calculated using the following formula:

$$D(G) = \frac{2}{N(N-1)}\sum_{i=1}^{N}\sum_{j=i+1}^{N} d_{ij} \tag{6}$$

Higher $D(G)$ suggest a more dispersed network, where nodes are less directly connected and communication requires traversing more intermediate links [85]. As such, path length is widely used to evaluate the efficiency and resilience of different network configurations [86].

3.6. Critical giant component

The critical giant component, often called the largest connected component (LCC), represents the largest subset of nodes in a fully interconnected network. This component plays a central role in determining the performance of a network. Its size is commonly analyzed analytically and numerically as a function of progressively removing

nodes or edges from the network.

As nodes or edges are eliminated randomly or through targeted strategies, the network gradually fragments, eventually reaching a critical threshold at which the structure breaks down. Beyond this point, the size of the giant component rapidly declines, reflecting a significant loss in overall connectivity and operational capacity.

This phase transition, marked by a sharp reduction in the size of the LCC, serves as a key indicator of the network's vulnerability and resilience [62]. The size of the giant component is mathematically expressed as [44]:

$$S(q) = \frac{G(q)}{G(0)} \tag{7}$$

The behavior of the critical giant component during node or edge removal clearly indicates the network's performance threshold. As the size of this component shrinks, it signals a degradation in the network's ability to function cohesively. Therefore, monitoring the evolution of the LCC under both random failures and targeted attacks is essential for quantifying structural robustness. This analysis helps identify critical points at which the network undergoes fragmentation, offering valuable insight into its resilience limits and guiding the evaluation of potential vulnerabilities under failure scenarios.

3.7. Weighted graph

In power systems, failures can lead to the fragmentation of the grid into multiple disconnected sub-networks, severely compromising operational stability. Identifying and reinforcing critical nodes is essential to mitigating these failures and enhancing the overall resilience of the system [87].

To address this challenge, this paper proposes a critical node identification method that evaluates nodes based on operationality features. The method prioritizes nodes using weighted betweenness centrality as a key metric, ensuring that nodes are ranked according to their influence on the system's structural integrity. The weighted nature of the graph is representative of load variations, power flow, capacity, or other operational factors, making the evaluation more representative of real-world conditions. The metric is defined mathematically as [37]:

$$B_e(n) = \frac{1}{2}\sum_{i\in C_j\in L}\sqrt{W_i W_j}\sum_{m\in f(n)}\left|P^{ij}(m,n)\right| \tag{8}$$

This weighted framework allows for a more nuanced understanding of network vulnerability and supports the development of targeted strategies to safeguard the grid against large-scale disruptions.

3.8. Attack strategies for network resilience testing

Different attack strategies are employed to assess the performance of the proposed method, each based on rankings of specific node importance. Evaluating the grid's performance under various disruption scenarios provides valuable insight into its vulnerability and supports the development of more effective resilience-enhancing strategies.

- Random Attack (RA): In this approach, nodes are removed in a completely random sequence, reflecting the unpredictable nature of real-world failures. Such scenarios may result from natural disasters, equipment aging, or unexpected technical malfunctions, where no specific target is involved.
- Malicious Attack: This strategy simulates intentional disruptions, such as cyberattacks or physical sabotage, by targeting nodes in descending order of their degree centrality; that is, the most highly connected nodes are attacked first. Since these nodes often play a pivotal role in maintaining the structural and functional integrity of the network, their removal can cause extensive fragmentation and performance degradation [86,88].

3.9. Topological efficiency of power grid reconfigurations

A key aspect of power system resilience is the network's ability to withstand and adapt to extreme events, exhibiting not just robustness but antifragility. In the aftermath of such events, the immediate objective is to initiate defensive actions using available resources to prevent cascading failures and maintain system stability. Strategies like network reconfiguration and islanding, particularly by adding transmission lines, can help contain the disturbance. These techniques enable rapid detection and response to disruptions, ultimately improving grid resilience. In this context, resilience refers to the network's ability to absorb shocks and continue functioning under failure conditions[18,89,90].

This study examines network resilience through a novel approach that draws an analogy to physical elastic systems. In mechanics, resilience is the ability of a material to absorb and release energy during elastic deformation, quantified by elastic potential energy. Following this concept, resilience in complex networks is modeled as the ability to recover structure and performance after node or edge failures:

$$E_p = \int_{\sigma=0}^{\sigma_c} -Fd\sigma \tag{9}$$

External forces represent disturbances such as attacks or failures, and elastic deformation corresponds to the degradation of the network. In this framework, the proportion of removed nodes q acts as the external force, while the fraction of failed nodes 1−G(q) reflects the elastic deformation. G(q) denotes the relative size of the giant connected component (GCC). This analogy suggests that, like an elastic body, a network may partially or fully maintain its original structure after a disturbance. Following this concept, resilience of the network is modeled as the ability to maintain robustness and performance after node or edge failures:

$$E_p = \int_{1-G(q)=0}^{1-G(q)=1} -qd(1-G(q)) = \int_{G(q)=0}^{G(q)=1} qdG(q) = \int_{q=0}^{q=1} G(q)\Big)dq \tag{10}$$

Since Eq. (10) lacks a closed-form solution, it must be evaluated using numerical integration. Two approximation methods are employed:

$$E_p = \frac{1}{N}\sum_{1}^{q=\frac{1}{N}} G(q) \tag{11}$$

$$E_p = \frac{1}{N}\sum_{1}^{q_l=\frac{1}{N}} \frac{G(q_l)+G(q_{l-1})}{2} \tag{12}$$

Eq. (11) applies the rectangle method, while Eq. (12) uses trapezoidal approximation. However, for consistency and ease, this paper adopts the rectangle method.

As illustrated in Fig. 4, the 24-node test network highlights the most efficient structural connections and identifies central nodes with relatively low influence. By systematically removing the most critical nodes, specifically nodes 9, 10, 16, and 21, a new network configuration emerges, consisting of isolated nodes, weakly connected components (weak cores), and a critical giant component, providing a clear basis for evaluating the impact of failures and the role of structural reconfiguration.

The addition of one, two, or three optimal edges, specifically (18–20), (3–19), and (8–13), respectively, leads to measurable improvements in both network resilience and the critical threshold, as quantified by:

$$\Delta q_c = q_{CI} - q_C \tag{13}$$

Establishing a connection between the weak cores and the critical giant component (Fig. 4) emphasizes that strategically reconfiguring the network, particularly by integrating optimal edges, can significantly improve structural robustness. By reinforcing vulnerable

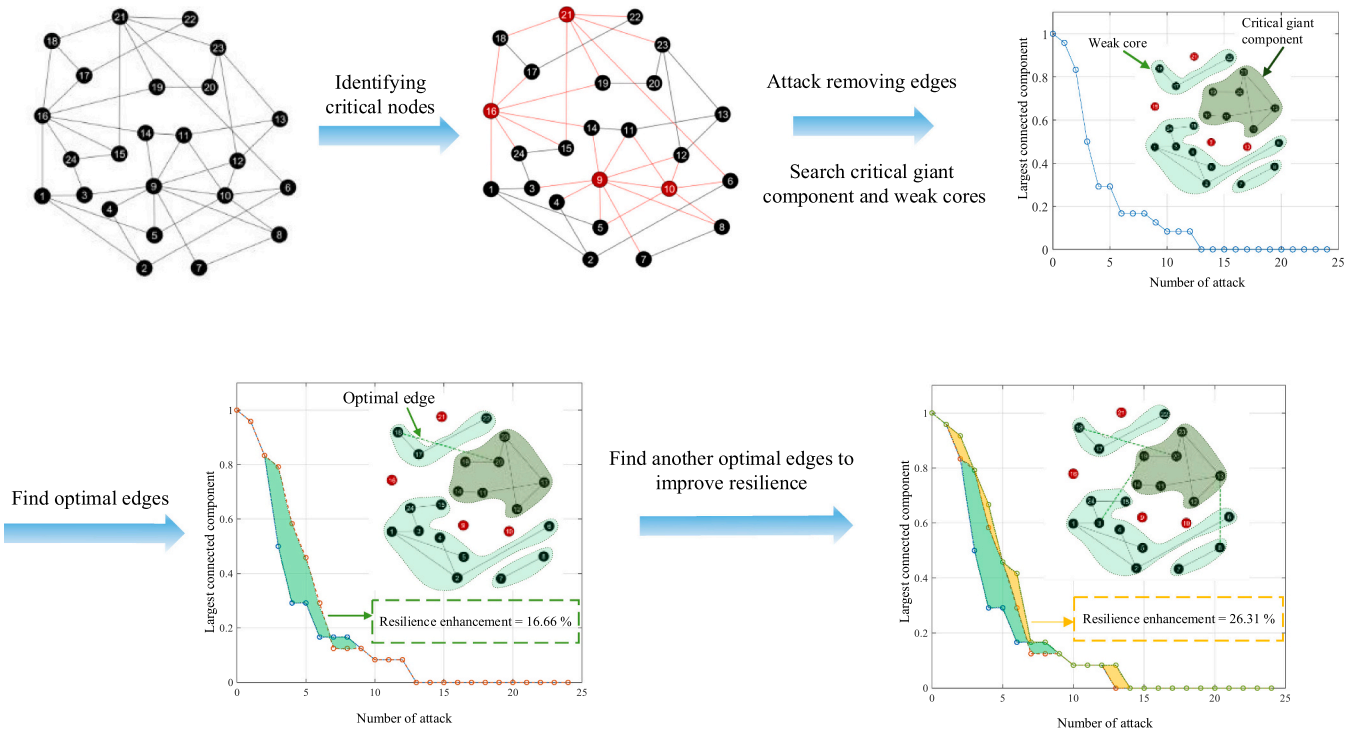


Fig. 4. Weak cores and optimal edges.

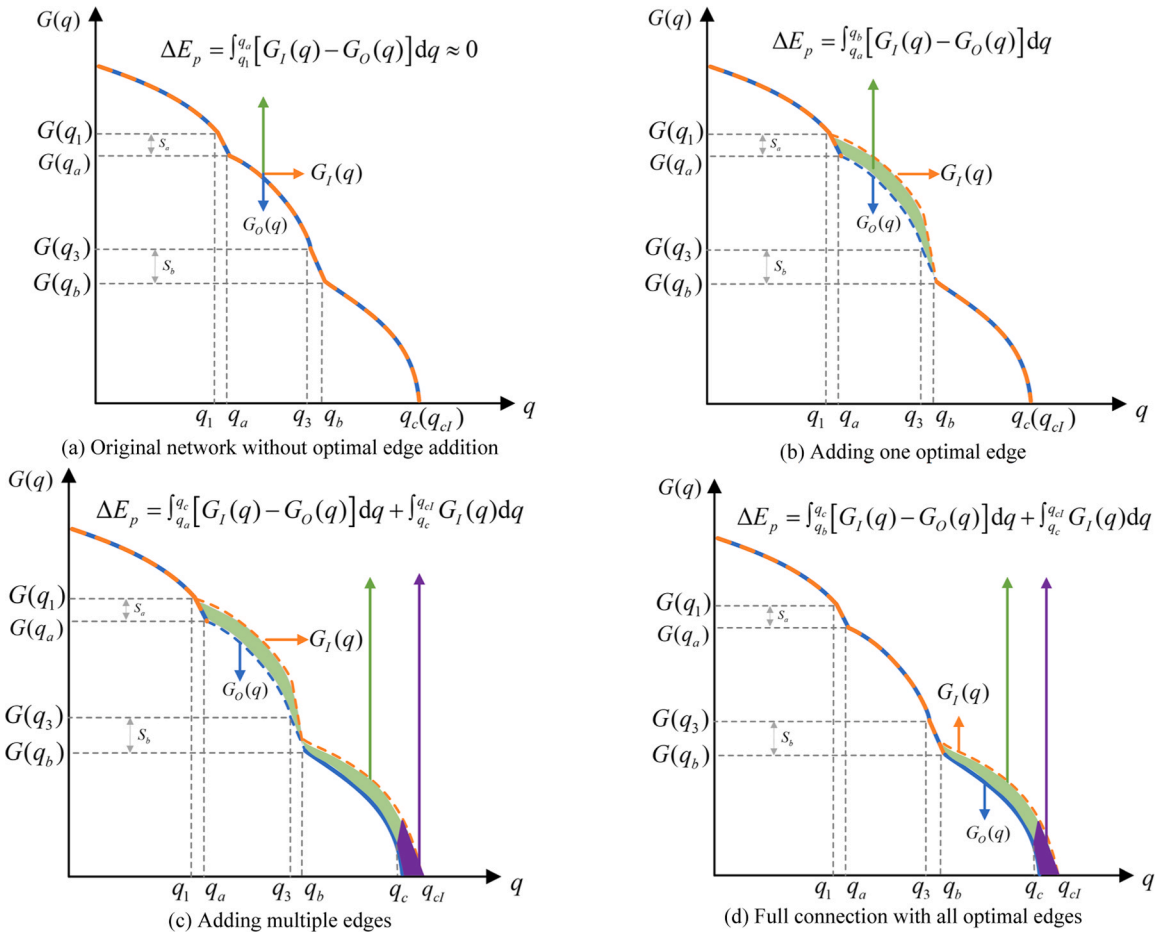


Fig. 5. Enhancement of resilience by 4 possible ways.

subcomponents and maintaining the integrity of the largest connected structure, the proposed method offers a practical and scalable approach to enhancing power grid resilience under random and targeted failure scenarios.

3.10. Enhancing resilience through edge addition

This study explores how the targeted addition of optimal edges can improve the resilience of power networks. The selection of these edges follows specific strategies, such as reinforcing connections within the largest connected component or establishing links between weak cores and the LCC. Once added, the effect of each edge on overall network resilience is evaluated using the resilience metric. The amount of resilience improves in results from edge addition can be quantified using Eq. (14).

$$\Delta E_p = \int_{q=0}^{q=1} [G_I(q) - G_O(q)]dq \tag{14}$$

Resilience improvements resulting from the addition of optimal edges are analyzed using four distinct approaches [91], as illustrated in Fig. 5. The first scenario, considered the baseline (Case i), involves no edge additions and is evaluated using Eq. (15), as depicted in Fig. 5a.

$$\Delta E_p^{i,ii} = \int_{q=0}^{q=1} [G_I(q) - G_O(q)]dq = \int_{q_1}^{q_a} [G_I(q) - G_O(q)]dq \approx 0 \tag{15}$$

Case (ii) involves adding a single edge between a weak core and the giant component, as shown in Fig. 5b. In Case (iii), additional edges are introduced between multiple weak cores and the giant component (Fig. 5c). Finally, Case (iv) incorporates all optimal edges connecting the weak cores to the giant component, as illustrated in Fig. 5d.

$$\Delta E_p^{iii} = \int_{q=0}^{q=1} [G_I(q) - G_O(q)]dq = \int_{q_a}^{q_b} [G_I(q) - G_O(q)]dq \tag{16}$$

$$\Delta E_p^{iv} = \int_{q=0}^{q=1} [G_I(q) - G_O(q)]dq = \int_{q_a}^{q_c} [G_I(q) - G_O(q)]dq + \int_{q_c}^{q_{cI}} G_I(q) \tag{17}$$

Comparing Eq. (17) in Case (iv) with Eq. (16) in Case (iii), as illustrated in Figs. 5d and 5c, respectively, clearly show that the resilience improvement in Case (iv) surpasses that of Case (iii). The findings suggest that the most effective placement of an edge is between a weak core and the largest connected component (LCC).

3.11. Optimizing robustness using the PA algorithm

A minimal and effective set of structural edges is identified to address the challenge of optimizing network robustness. This solution is derived using a unified theoretical framework supported by the proposed resilience indices, which are designed to capture the structural characteristics of network resilience. To implement this, we introduce a posteriorly adding (PA) algorithm that strategically adds edges to enhance resilience, particularly within IEEE standard test networks.

The overall procedure is illustrated in the flowchart in Fig. 6. By sequentially adding the optimal edges identified through the PA algorithm, the network's resilience can be systematically and effectively improved.

The computational complexity of the robustness-enhancement approach is $O(2\alpha K(M+N) + log(M+N))$, where M is the number of edges, α ($\alpha \ll N$) is the number of edges to be added, and K ($K \ll M$) is the number of largest connected components. In practice, K remains small because the sizes of finite components follow a power-law distribution [90]. This favorable scaling ensures our method remains efficient even for large networks.

The proposed methodology used Python with the NetworkX library to model weighted multigraphs, compute centrality metrics, and execute the PA algorithm for optimal edge addition. Analyses were conducted on IEEE 14, 24, 39, and 118-bus test systems.

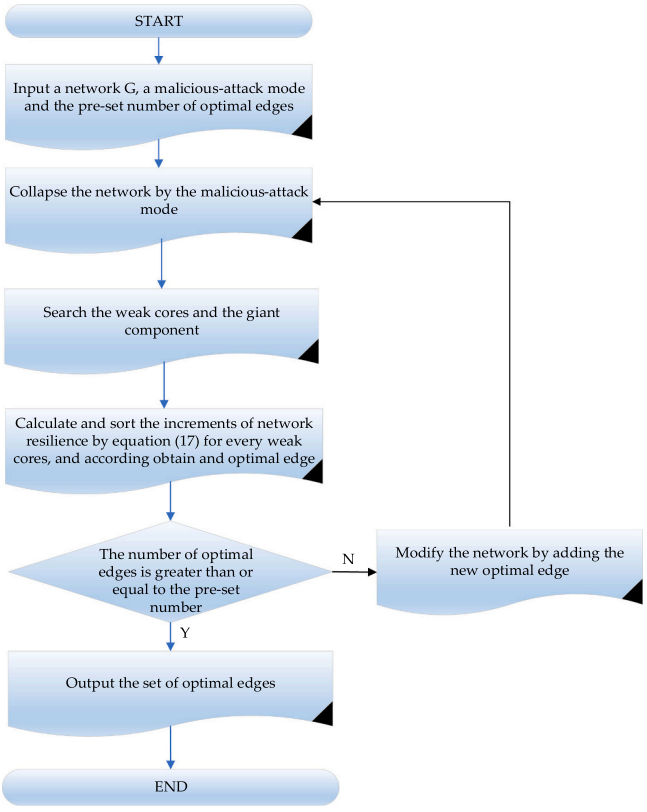


Fig. 6. The flowchart of the model.

4. Numerical results and discussion

This section presents the numerical results of the proposed resilience enhancement framework and evaluates its effectiveness through a series of various case studies. The performance of the graph learning-based approach is assessed using standard IEEE test systems, demonstrating the benefits of optimal edge augmentation and structural reconfiguration strategies.

Key resilience indicators, including betweenness centrality and the size of the largest connected component, are analyzed before and after applying the proposed optimizations to quantify the improvements in network robustness. The simulation results illustrate significant resilience enhancements across various attack scenarios, including malicious and random failures.

4.1. Improve structural resilience

4.1.1. Structural resilience enhancement in the IEEE 14-bus network

To evaluate and enhance the resilience of power networks against malicious attacks, the IEEE 14-bus network (Fig. 7a) is analyzed using a graph-based approach derived from complex network theory. This network comprises 14 nodes (buses) and 24 edges (transmission lines), as illustrated in Fig. 7b.

The process of enhancing network resilience begins with the identification of critical nodes through graph-theoretical methods. Nodes with the highest degree centrality, those whose failure has the greatest impact on network robustness, are identified and removed along with their corresponding edges. As illustrated in Fig. 7c, removing these nodes can significantly compromise the network's structural integrity, leading to severe fragmentation and forming three isolated subnetworks: one LCC and two weak cores (Fig. 7d).

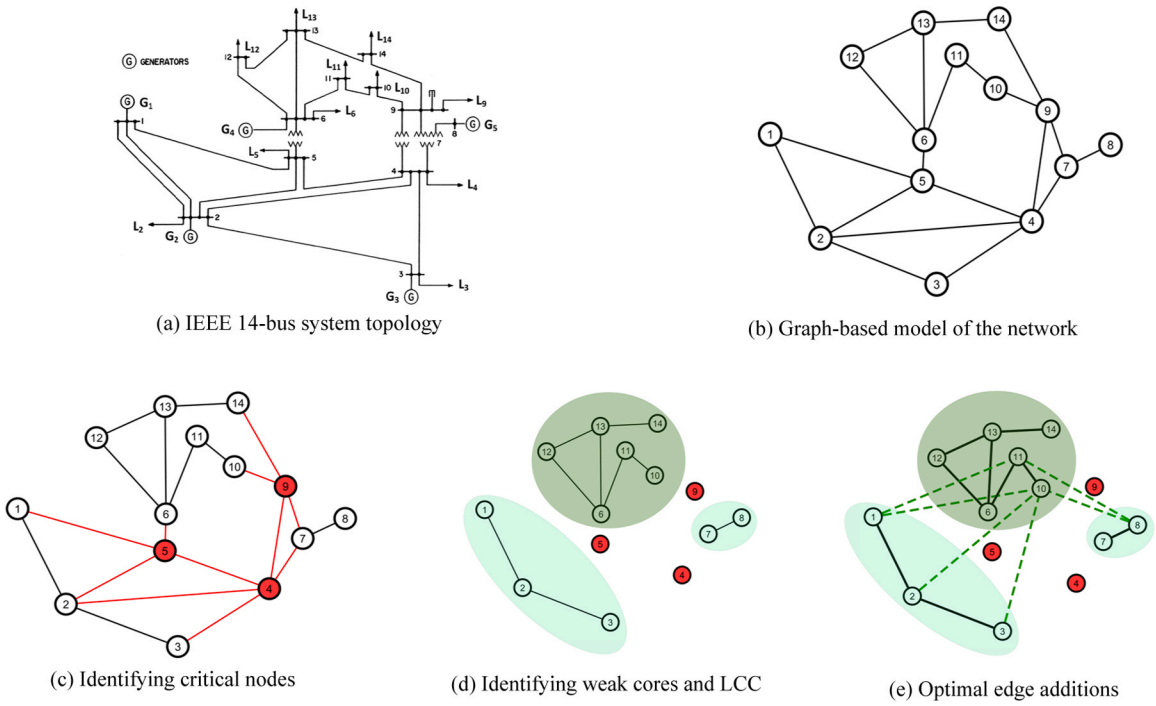


Fig. 7. Resilience enhancement of the IEEE 14-bus network by identifying critical nodes and adding optimal edges.

To mitigate the adverse effects of these disruptions, the PA algorithm is employed to determine the optimal placement of additional edges that enhance network resilience. As illustrated in Fig. 7e, these optimally added edges, marked by green dashed lines, effectively reconnect the fragmented network, enhancing resilience and maintaining structural integrity.

The quantitative impact of the proposed enhancements is substantial. In Case I, adding a single optimal edge yields a 9.61 % improvement in resilience against malicious attacks. With further optimization in Case III, involving the addition of six edges, network resilience increases by 38.46 %. These improvements are illustrated in Fig. 8a.

Resilience evaluations are performed iteratively by removing one critical node at a time, then reanalyzing the network topology to identify the next most vulnerable component and quantify its impact on overall system resilience. In parallel, an alternative evaluation is conducted without modifying the network topology, focusing on a fixed set of predefined critical nodes. This approach is particularly suitable for assessing network resilience under random failure conditions, as depicted in Fig. 8b.

A notable advantage of the fixed-node analysis lies in its relevance to scenarios where certain nodes are inherently more exposed due to their geographic location or operational importance. As shown in Fig. 8b, even without reconfiguring the network, the strategic addition of optimal edges under fixed-node failure conditions leads to a remarkable 52 % improvement in resilience. These results emphasize the effectiveness of the proposed methodology in addressing both targeted and random disruptions while significantly enhancing the structural integrity of the power system.

Table 2 summarizes the optimal edges added to the IEEE 14-bus system and the corresponding resilience improvement based on the

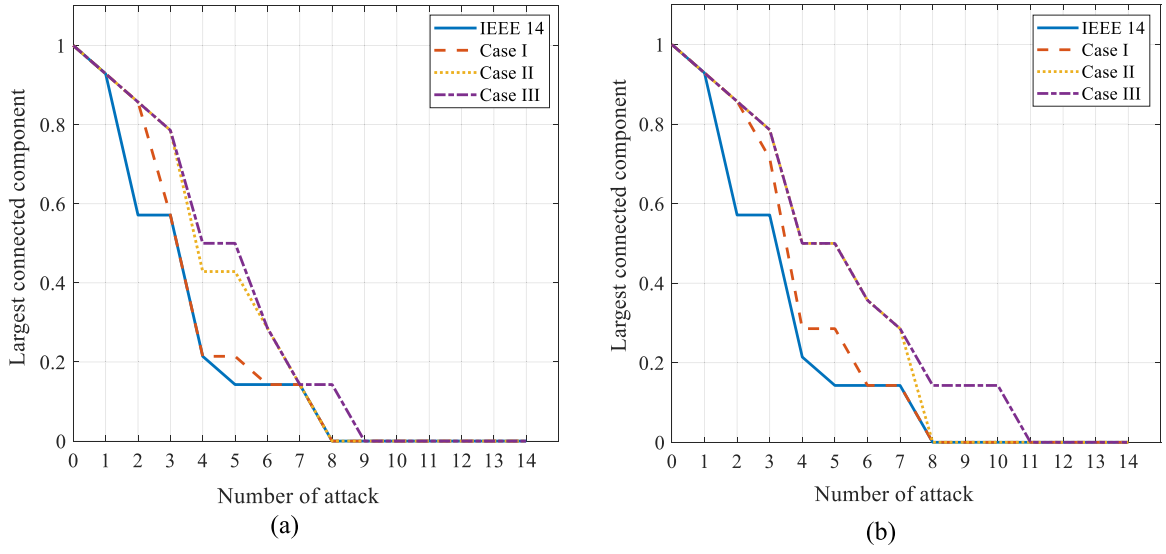


Fig. 8. Evaluation of IEEE 14-bus resilience improvement based on the robustness against (a) malicious, (b) random attack.

Table 2
IEEE 14 information on optimal edge addition.

Number of cases	ID of the optimized Edges	Improve CR against malicious attacks (%)	Improve CR against random attacks (%)
Case I	(1−11)	9.61	17.30
Case II	(1−11), (2−10), (8−10), (3−10)	30.77	40.38
Case III	(1−11), (2−10), (8−10), (3−10), (1−10), (8−11)	38.46	51.92

robustness of both malicious and random attack scenarios. The results underscore the critical role of strategic edge augmentation in enhancing the network's CR across a range of failure conditions.

4.1.2. Structural resilience enhancement in the IEEE 24-bus network

The IEEE 24-bus network, shown in Fig. 9a, serves as a case study for evaluating and enhancing resilience under targeted attack scenarios. Modeled using a graph-theoretical approach grounded in complex network theory, the network comprises 24 nodes and 38 edges (Fig. 9b).

The resilience enhancement process begins with identifying critical nodes whose failure would lead to significant structural degradation. These nodes are identified using graph-theoretical metrics, particularly degree centrality, as shown in Fig. 9c. Removing these high-impact nodes and their corresponding transmission lines results in visible network fragmentation.

Following the simulated targeted attacks, the network is divided into one LCC and three weak cores (Fig. 9d), substantially reducing structural integrity. To address this, the PA algorithm is applied to strategically determine and insert optimal edges that restore connectivity and enhance resilience. The resulting network reconfiguration, including the newly added edges, is illustrated in Fig. 9e, demonstrating a clear improvement in structural robustness.

In Case I, adding a single optimal edge results in a 16.66 % improvement in network resilience. Extending this approach to Case V, which includes ten additional edges, further increases resilience by 44.63 %. To provide a comprehensive assessment, resilience, and CR are evaluated iteratively. Following removing each critical node, the network topology is updated, and the next most vulnerable component is identified to measure its effect on system resilience. In parallel, an alternative evaluation is conducted where the topology remains unchanged, and resilience is assessed based on a fixed set of predefined critical nodes. This method is beneficial for analyzing network robustness under geographical or operational constraints, as shown in Fig. 10b. which, even without reconfiguring the network, the strategic placement of optimal edges leads to a remarkable 120 % improvement in resilience against random-node failures. These findings demonstrate the effectiveness of the proposed method in significantly reinforcing the anti-fragility of the power network under diverse failure conditions.

Table 3 comprehensively summarizes the optimal edge additions implemented in the IEEE 24-bus network. The findings indicate that targeted edge expansion significantly improves network CR.

4.1.3. Structural resilience enhancement in the IEEE 39-bus network

The IEEE 39-bus system serves as a key case study for evaluating and improving the structural resilience of power networks under failure event scenarios. This network includes 10 generators, 39 buses, and 46 transmission lines, as illustrated in Fig. 11a. Its corresponding graph-based representation is shown in Fig. 11b, highlighting the intricate interconnections among network components.

Nodes with the highest degree centrality, those functioning as major transmission hubs, are identified and analyzed for their impact on system performance. As depicted in Fig. 11c, the removal of these critical nodes results in significant structural degradation, marking them as high-priority targets in resilience analysis.

Simulating targeted attacks leads to noticeable fragmentation within the network, forming one LCC and four weak cores, as shown in Fig. 11d.

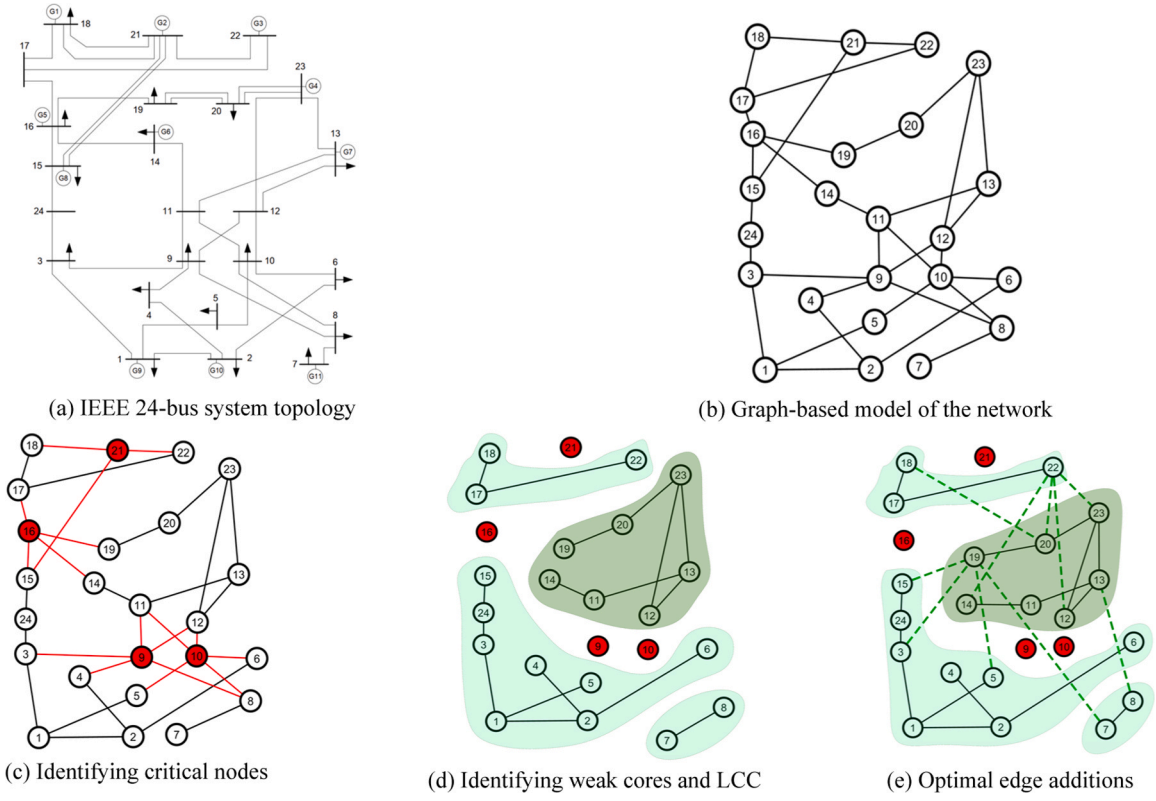


Fig. 9. Resilience enhancement of the IEEE 24-bus network by identifying critical nodes and adding optimal edges.

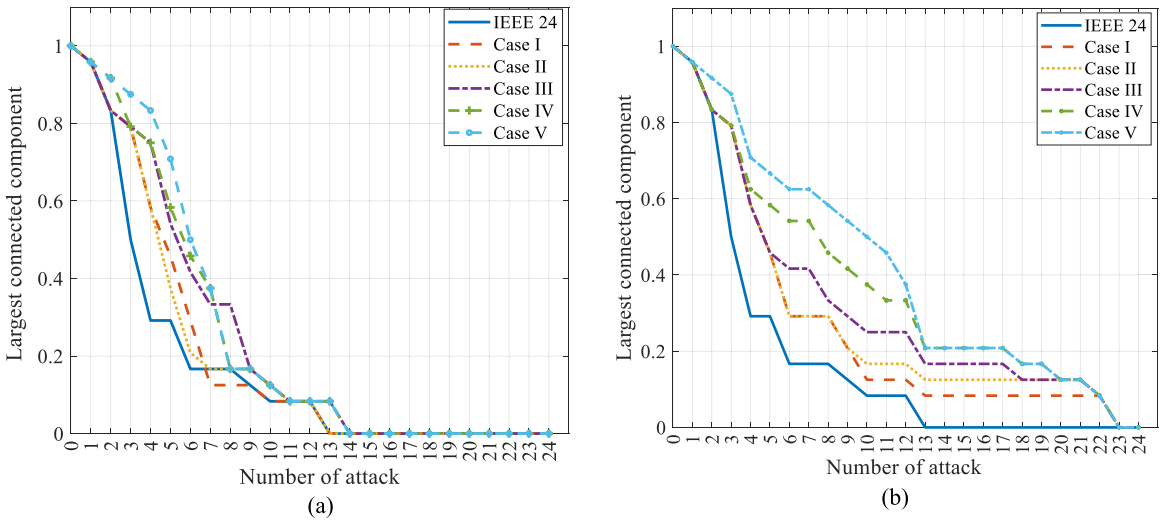


Fig. 10. Evaluation of IEEE 24-bus resilience improvement based on the robustness against (a) malicious, (b) random attack.

Table 3
IEEE 24 information on optimal edge addition.

Number of cases	ID of the optimized Edges	Improve CR against malicious attacks (%)	Improve and CR against random attacks (%)
Case I	(18–20)	16.66	44.34
Case II	(Case I), (22–20), (22–23)	16.66	54.78
Case III	(Case II), (3–19), (22–12)	36.84	72.17
Case IV	(Case III), (22–14), (5–19)	37.72	98.25
Case V	(Case IV), (7–19), (8–13), (15–19)	44.73	119.99

This disruption reduces system connectivity and increases the likelihood of cascading failures. To address this, the PA algorithm is applied to determine and insert optimal edges that reconnect fragmented components. The resulting enhancement is visualized in Fig. 11e, where the added edges (represented by green dashed lines) reinforce key pathways and improve overall network resilience.

Quantitative analysis shows that adding a single edge (Case I) increases network resilience by 7.45 %. Extending this approach to Case V, which includes sixteen additional edges, results in a substantial 90.5 % improvement. These enhancements are visualized in Fig. 12a, demonstrating how strategic edge placement strengthens the network against malicious attacks.

A complementary evaluation is performed where the network topology remains unchanged, and resilience is assessed based on a fixed

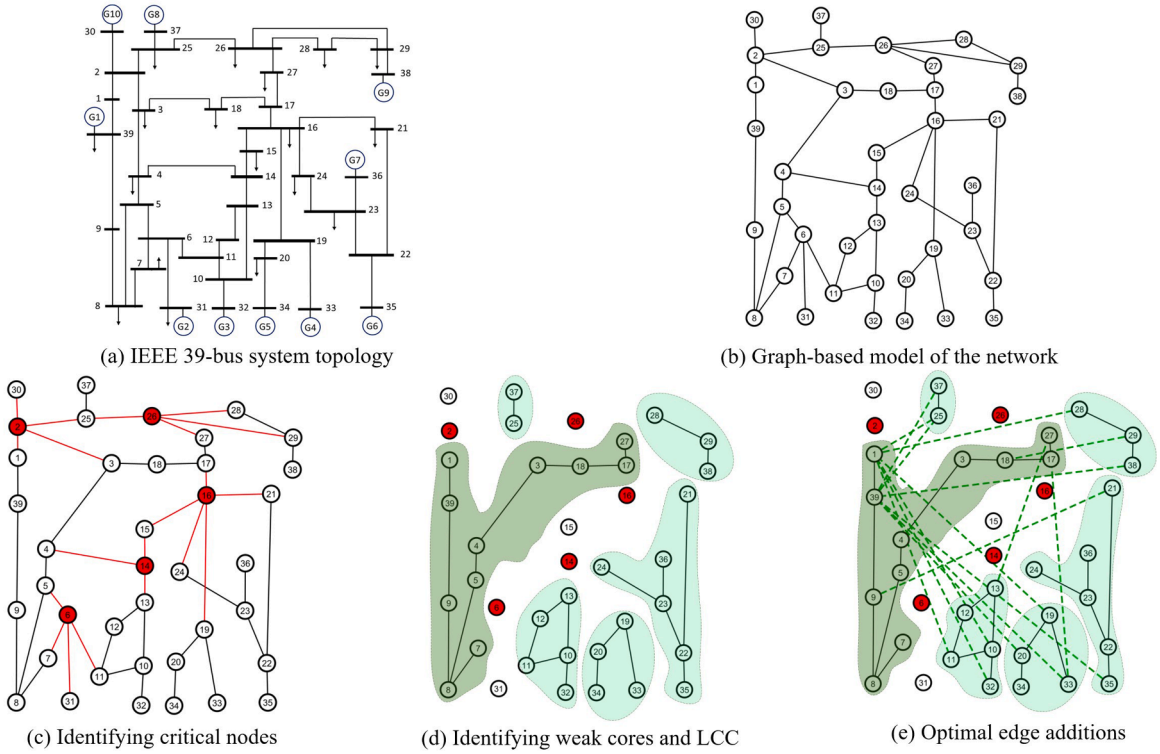


Fig. 11. Resilience enhancement of the IEEE 39-bus network by adding optimal edges.

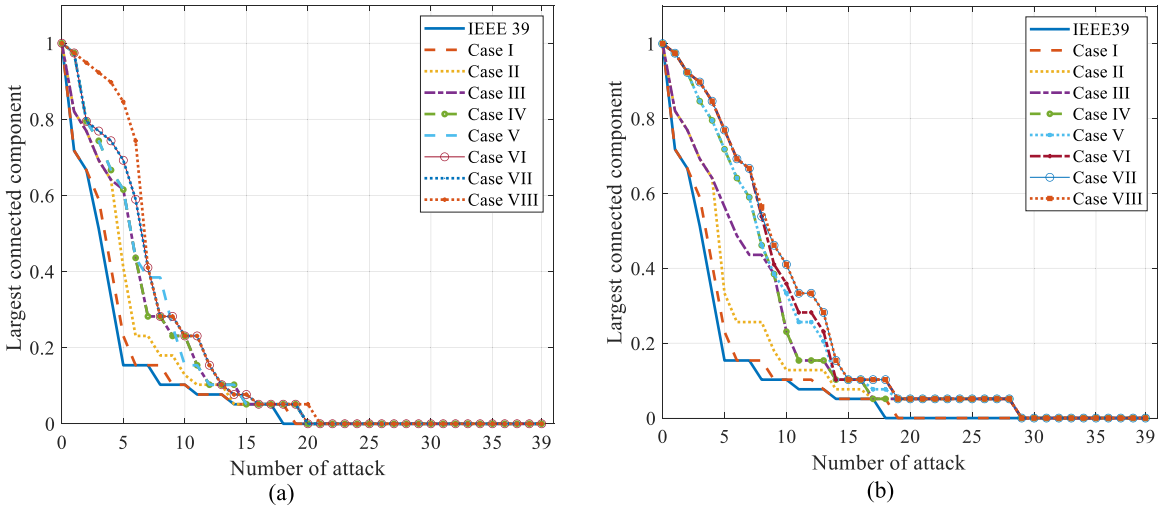


Fig. 12. Evaluation of IEEE 39-bus resilience improvement based on the robustness against (a) malicious, (b) random attack.

set of random nodes. This method allows for analyzing network robustness under operational and geographical constraints, as illustrated in Fig. 12b.

A key insight from this assessment is the system's ability to improve resilience even without major reconfiguration. As shown in Fig. 12b, the strategic addition of optimal edges under fixed-node failure scenarios leads to an impressive 131 % increase in CR. This outcome underscores the effectiveness of the proposed method in reinforcing structural integrity and enhancing resilience.

Table 4 summarizes the optimal edge additions applied to the IEEE 39-bus system and their corresponding contributions to improving CR. The results demonstrate the effectiveness of targeted edge reinforcement in enhancing resilience.

4.1.4. *Structural resilience enhancement in the IEEE 118-bus network*

The IEEE 118-bus test system offers a comprehensive yet simplified representation of the American Electric Power grid in the U.S. Midwest. This network includes 19 generators, 35 synchronous condensers, 186 transmission lines, 9 transformers, and 91 load points. Due to its structural complexity, the system incorporates numerous voltage control devices and is designed for robustness, typically achieving convergence in just a few iterations under fast decoupled power flow analysis. The topology of the network and corresponding graph-based model of the network are shown in Figs. 13a and 13b, respectively.

The resilience enhancement process begins by identifying critical nodes and components with the highest potential to compromise system integrity. Using graph-theoretical analysis, particularly degree centrality, these high-impact nodes are detected based on their role in power transmission. As shown in Fig. 13c, the failure or removal of these nodes leads to a significant decline in network stability, increasing the risk of cascading failures and widespread fragmentation.

Under the simulated targeted attack scenario, the network experiences severe disintegration, forming the LCC and thirteen weak cores (Fig. 13d). This level of disruption presents serious challenges to system robustness and highlights the need for robust resilience strategies. The strategic placement of these new connections, illustrated as green dashed lines in Fig. 13e, contributes to restoring connectivity and enhancing the CR of the power system.

Quantitative analysis shows that, in Case I, adding a single optimal edge yields a modest 2.85 % increase in network resilience. However, expanding the optimization to Case V, which includes fifty additional edges, leads to a substantial 73.64 % improvement. These enhancements are illustrated in Fig. 14a. After each critical node is removed, the network topology is updated, the next most vulnerable node is identified, and its impact on system resilience is quantified. In parallel, an alternative evaluation is conducted without modifying the network structure. This secondary approach focuses on a fixed set of critical nodes, enabling resilience assessment under geographic and operational constraints, as depicted in Fig. 14b. Optimizing edge placement without reconfiguring the network results in a remarkable 123 % increase in resilience under failure conditions. This outcome underscores the effectiveness of the proposed method in reinforcing structural integrity and enhancing resilience.

Table 5 presents a detailed summary of the optimal edge additions in the IEEE 118-bus system and their corresponding improvements in CR. The results highlight the effectiveness of targeted edge reinforcement in strengthening resilience. By strategically reinforcing weak areas and optimizing overall connectivity, the IEEE 118-bus network significantly increases resilience.

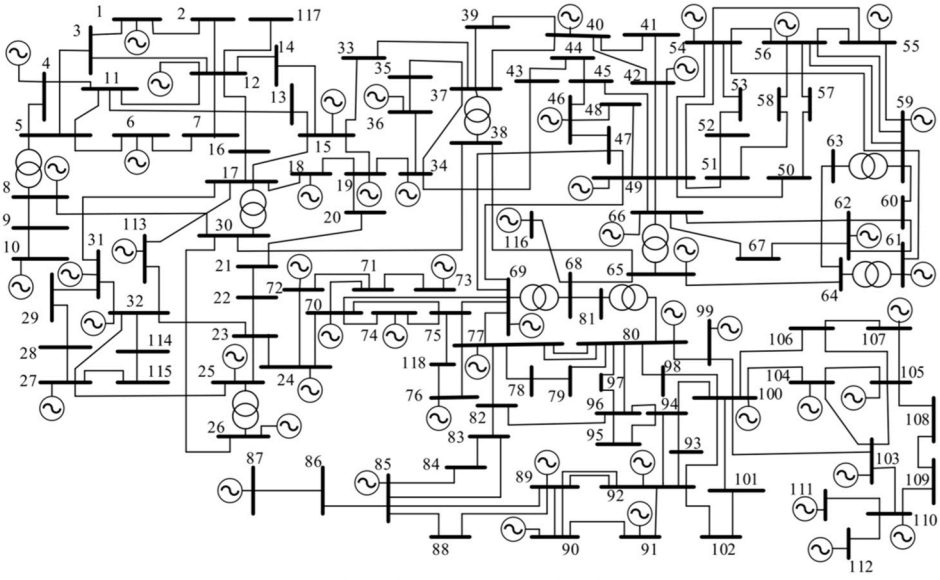
Table 4
IEEE 39 information on optimal edge addition.

Number of cases	ID of the optimized Edges	Improve CR against malicious attacks (%)	Improve and CR against random attacks (%)
Case I	(1−28)	7.52	8.67
Case II	(Case I), (13−27), (33−39)	32.96	47.98
Case III	(Case II), (29−18), (33−17)	51.45	76.887
Case IV	(Case III), (20−39), (35−39)	57.24	101.74
Case V	(Case IV), (38−39), (11−1)	60.70	110.99
Case VI	(Case V), (32−1), (39−25)	71.68	123.14
Case VII	(Case VI), (1−25), (37−39)	71.68	130.07
Case VIII	(Case VII), (9−21), (10−1), (19−1)	90.18	130.65

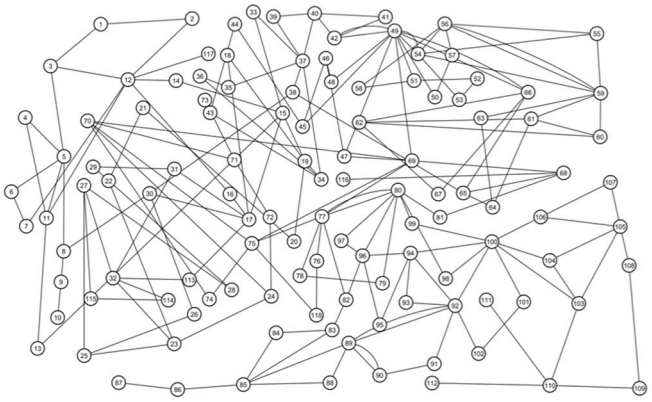
4.2. *Improve the resilience of weighted multigraph*

This section presents the results of resilience enhancement based on weighted multigraph modeling. Unlike unweighted graph-based approaches, weighted multigraphs offer a more realistic representation of power system dynamics by incorporating edge weights, which reflect operational characteristics.

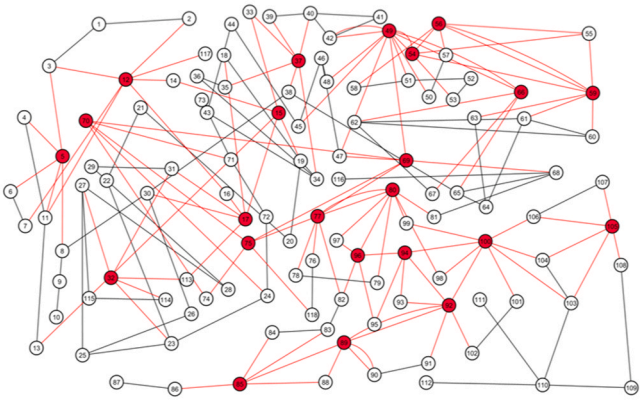
This analysis employs weighted betweenness centrality as a key metric to evaluate resilience improvements. This measure captures the proportion of shortest paths passing through a given node, weighted by



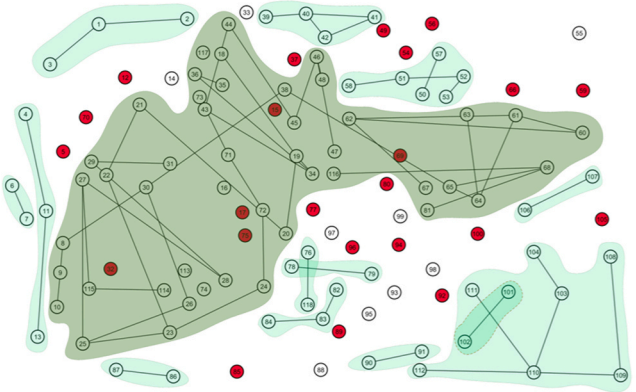
(a) IEEE 118-bus system topology



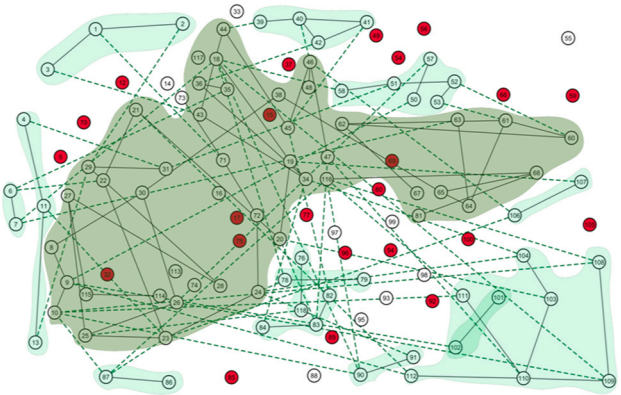
(b) Graph-based model of the network



(c) Identifying critical nodes



(d) Identifying weak cores and LCC



(e) Optimal edge additions

Fig. 13. Identification of critical nodes and resilience improvement in the IEEE 118-bus network by adding optimal edges.

the importance of connected edges, thereby identifying critical components that play a central role in maintaining network connectivity. Nodes 4, 5, 6, and 9, as shown in Fig. 15a, are operating near their maximum capacity, indicated by the darker coloring that represents the weighted sum of the lines connected to these nodes. These nodes represent potential failure points where disruptions could propagate rapidly through the network.

Following the addition of optimal edges, identified in previous sections, the weighted values of nodes 4, 5, 6, and 9 are reduced, as illustrated in Fig. 15b. This decrease reflects a more balanced load distribution across the network, effectively alleviating the critical stress on these key nodes.

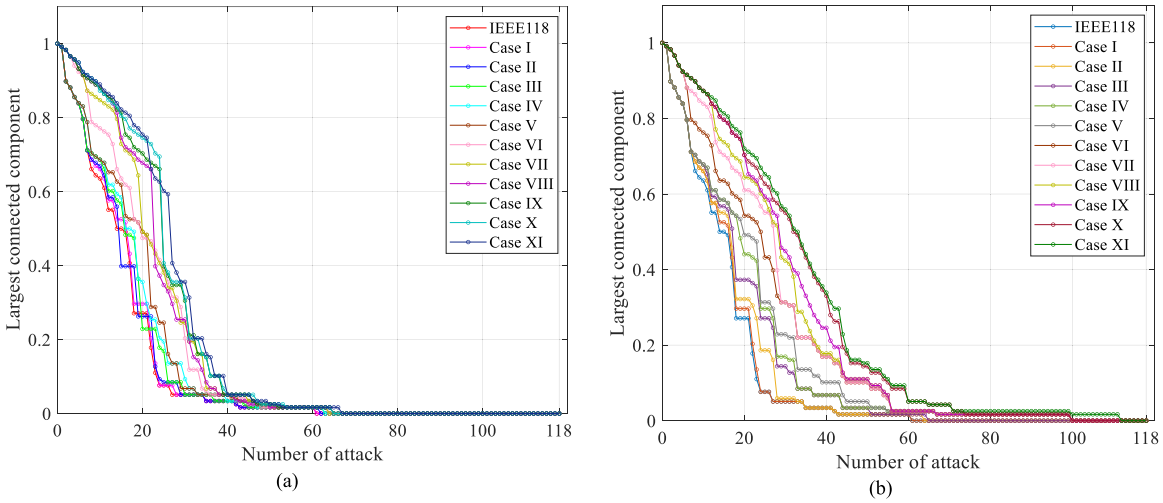


Fig. 14. Evaluation of IEEE 118-bus resilience improvement based on the robustness against (a) malicious, (b) random attack.

Table 5
IEEE 118 information on optimal edge addition.

Number of cases	ID of the optimized Edges	Improve CR against malicious attacks (%)	Improve and CR against random attacks (%)
Case I	(2−29)	2.86	2.69
Case II	(Case I), (1−71), (3−43), (4−31), (11−23)	2.47	9.14
Case III	(Case II), (13−29), (6−35), (6−22), (7−63), (7−18)	8.58	21.38
Case IV	(Case III), (87−10), (87−116), (87−23), (82−45), (83−20)	14.59	32.66
Case V	(Case IV), (83−47), (84−34), (118−25), (78−18), (78−24)	20.31	40.85
Case VI	(Case V), (90−10), (90−116), (90−18), (91−24), (106−46)	40.07	66.44
Case VII	(Case VI), (106−23), (107−19), (50−9), (57−26), (51−31)	50.57	77.78
Case VIII	(Case VII), (52−60), (53−61), (58−18), (39−44), (40−46)	54.27	88.27
Case IX	(Case VIII), (41−45), (42−36), (112−21), (112−9), (110−47)	64.99	97.25
Case X	(Case IX), (109−18), (109−26), (108−10), (108−116), (103−20)	68.47	115.16
Case XI	(Case X), (104−34), (104−24), (111−10), (111−116), (102−9)	73.63	122.73

The effectiveness of this approach is further validated across other test cases. Figs. 15c–15h demonstrate similar applications of the methodology to the IEEE 24-, 39-, and 118-bus systems. These results confirm the framework's ability to identify and mitigate critical vulnerabilities within weighted multigraph models. The proposed approach systematically enhances resilience based on robustness by reinforcing connectivity and reducing the risk of fragmentation.

An AC power flow analysis was performed using the Pandapower framework to validate structural improvements from an operational perspective. The simulations were conducted under peak load conditions. Figs. 16(a)-16(d) illustrate the power flow results for all network lines before and after adding optimized lines.

The power flow analysis results of the 14-bus network lines demonstrate that the addition of optimal lines has significantly reduced the loads of lines in the network, as shown in Fig. 16(a). These results align with the findings from the weighted multigraph analysis, which indicated that adding optimal lines would reduce critical points. Power flow analysis further confirms that no lines are overloaded after the additions. In most cases, the load on the original lines has decreased.

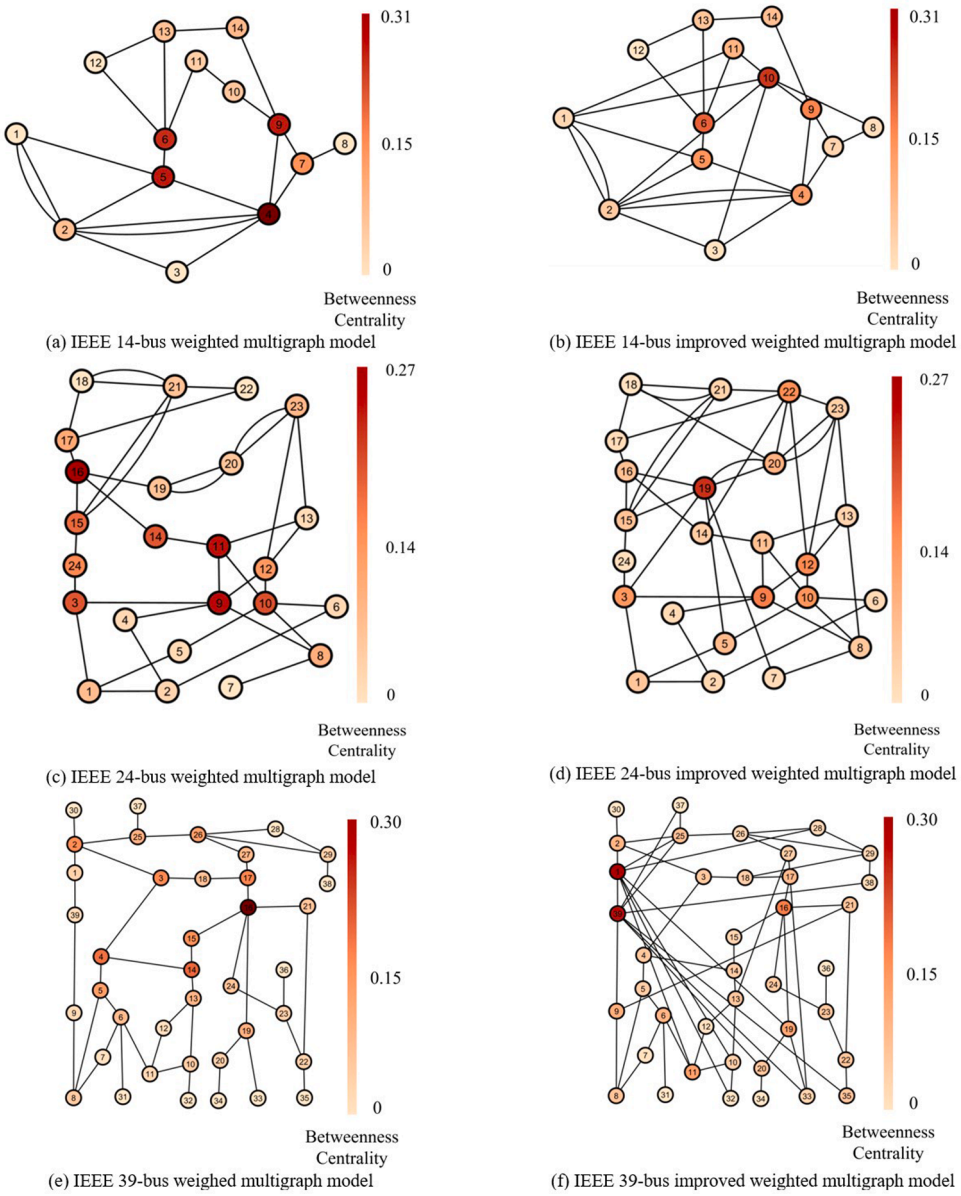
A similar result is observed in the 24-bus network, where the integration of optimal lines has considerably lowered the load on the original lines, as illustrated in Fig. 16(b). In the 39-bus network, power flow analysis revealed that 15 out of 46 original lines were initially overloaded due to structural and operational complexities, as illustrated in Fig. 16(c). Nevertheless, after the optimized lines were added, the number of overloaded lines was reduced to nine. This number can be further decreased by adjusting line capacities, depending on the network's operational conditions. Notably, most remaining lines exhibit lower loading levels than the initial scenario.

Finally, in the large-scale and complex 118-bus network, where the original configuration includes 186 lines with 28 overloaded, adding 50 optimal lines reduced the number of overloaded lines to 2. In most remaining cases, the loading levels of original lines significantly decreased, as shown in Fig. 16(d).

Power-flow analysis evaluates the steady-state behavior of an electrical network, calculating voltages, active and reactive power flows, and branch loadings, based on transmission line capacities and operational conditions. To maintain system security and prevent overloads, operators may employ corrective actions such as generator re-dispatch, transformer tap adjustments, reactive compensation, or load curtailment within security-constrained optimal power-flow frameworks. These strategies are essential components of energy management and operational planning in modern power systems.

A detailed comparison of the resilience improvements achieved in the IEEE 14, 24, 39, and 118-bus networks following applying the proposed framework under malicious attack scenarios is shown in Fig. 17. The results are illustrated in Figs. 17a–17d. Specifically, the optimized network structures exhibit substantial resilience gains, with the IEEE 14-bus network achieving a 36.71 % improvement, the IEEE 24-bus network a 28.62 % improvement, the IEEE 39-bus network a 21.64 % improvement, and the IEEE 118-bus network a 22.22 % improvement. These improvements are driven by the systematic identification and reinforcement of critical nodes and edges, identified through weighted betweenness, which reduce network vulnerability to targeted disruptions. The proposed method bolsters resilience against target attacks and contributes to developing antifragile power systems.

Table 6 summarizes the quantitative resilience metrics across the evaluated networks before and after applying the proposed framework.



(a) IEEE 14-bus weighted multigraph model
(b) IEEE 14-bus improved weighted multigraph model
(c) IEEE 24-bus weighted multigraph model
(d) IEEE 24-bus improved weighted multigraph model
(e) IEEE 39-bus weighed multigraph model
(f) IEEE 39-bus improved weighted multigraph model

Fig. 15. Effect of adding optimal edges in a weighted multigraph network to enhance resilience.

Key metrics such as robustness, average path length, and clustering coefficient are used to demonstrate the improvements in resilience.

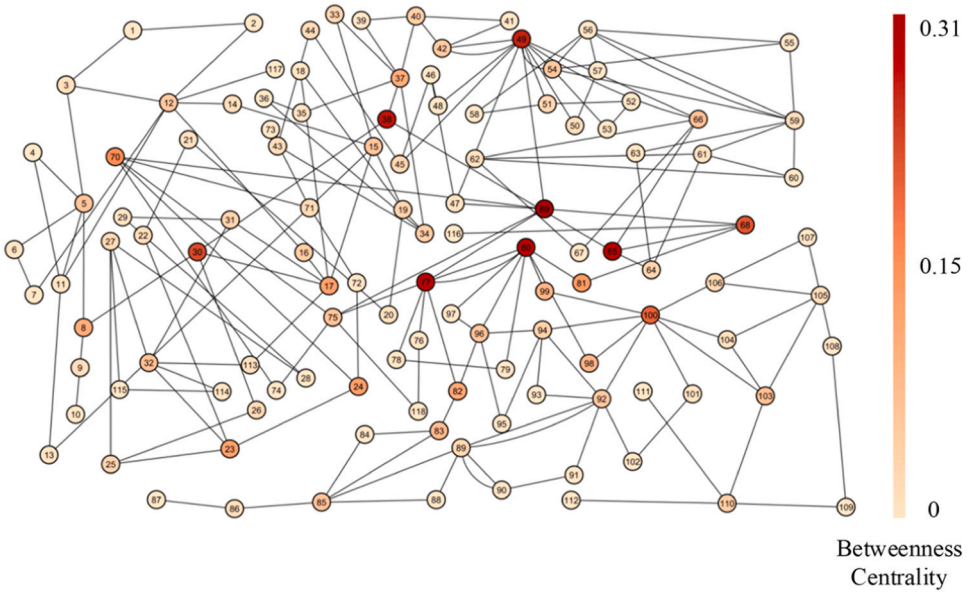
Reducing average path length reflects a more cohesive and efficient network structure, enhancing resilience by enabling faster and more reliable connectivity even during disruptions. Similarly, an increase in the clustering coefficient, which indicates the degree of local interconnectedness, suggests improved structural cohesion. This rise in clustering reflects stronger resilience, as the network becomes better equipped to maintain functionality through alternative pathways when facing failures.

Fig. 18 illustrates the percentage of node removals at which the number of links in the IEEE 14-, 24-, 39-, and 118-bus networks drops to zero under malicious attack scenarios. In the original network configurations, connectivity is lost when approximately 50 % of nodes are attacked in the IEEE 14-bus network, 50 % in the IEEE 24-bus network, 43 % in the IEEE 39-bus network, and 51 % in the IEEE 118-bus network.

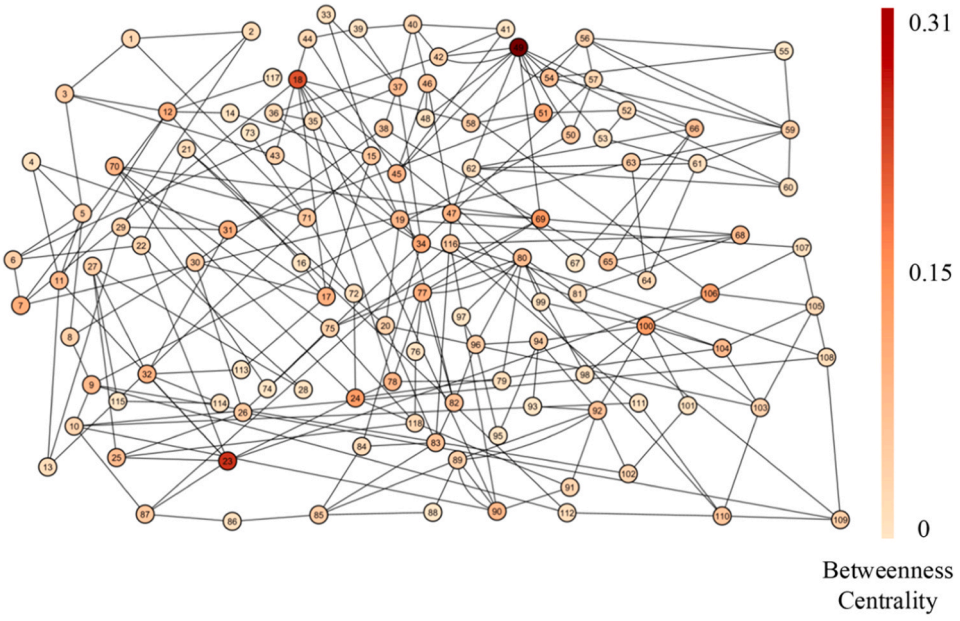
In contrast, enhanced through targeted edge additions and structural reinforcement, the improved networks demonstrate notable resilience. Connectivity is maintained until 57 % of nodes are removed in the IEEE 14-bus network, 54 % in the IEEE 24-bus network, 51 % in the IEEE 39-bus network, and 56 % in the IEEE 118-bus network. These improvements are achieved by reinforcing critical nodes and connecting weak cores to the LCC. The results highlight the effectiveness of the proposed framework in delaying network fragmentation and enhancing CR, contributing to the development of more resilient power systems capable of withstanding severe disruptions.

4.3. Practical implications and discussion

The proposed graph learning-based framework marks a significant advancement in enhancing power system resilience. By using structural robustness, reconfiguration, and the conceptual foundation of anti-fragility, this framework enables the design of networks capable of withstanding and adapting to various disruptions. Simulation results across standard IEEE test systems confirm its effectiveness. For instance, in the IEEE 24-bus network, adding a single optimal transmission line led to a 16.66 % increase in robustness against malicious attacks and a



(g) IEEE 118-bus weighed multigraph model



(h) IEEE 118-bus improved weighted multigraph model

Fig. 15. (*continued*).

44.34 % improvement under random failures. When three optimal lines were added, robustness against random failures increased to 54.78 %. These results substantially outperform previous methods. For example, in [38], adding a single optimal line resulted in only a 5.71 % increase in robustness, and adding three lines led to just a 9.43 % improvement. This comparison demonstrates the superior performance and efficiency of the proposed approach, which achieves greater resilience gains with fewer structural modifications.

While traditional methods often focus on identifying vulnerabilities, such as fragile lines or critical points [34,81], the proposed framework moves beyond assessment by offering network reconfiguration strategies. Modeling the grid as a weighted multigraph more accurately captures operational dynamics and enables more detailed structural analysis.

In contrast to reactive approaches, such as graph autoencoder-based techniques used for detecting false data injection in cyber-physical systems [54], this study evaluates improvements in network resilience before and after structural reconfiguration by simulating malicious and random attacks. While the proposed framework is demonstrated using attack scenarios (malicious and random), it is not confined to these models. The flexible methodology can be extended to analyze high-impact, low-probability (HILP) events, such as floods, earthquakes, or targeted cyberattacks, by incorporating spatial impact models, probabilistic hazard maps, or real-world failure data. This adaptability enables its application in various resilience assessments and planning studies.

The proposed methodology introduces a targeted, performance-driven optimization strategy based on recent developments in graph-

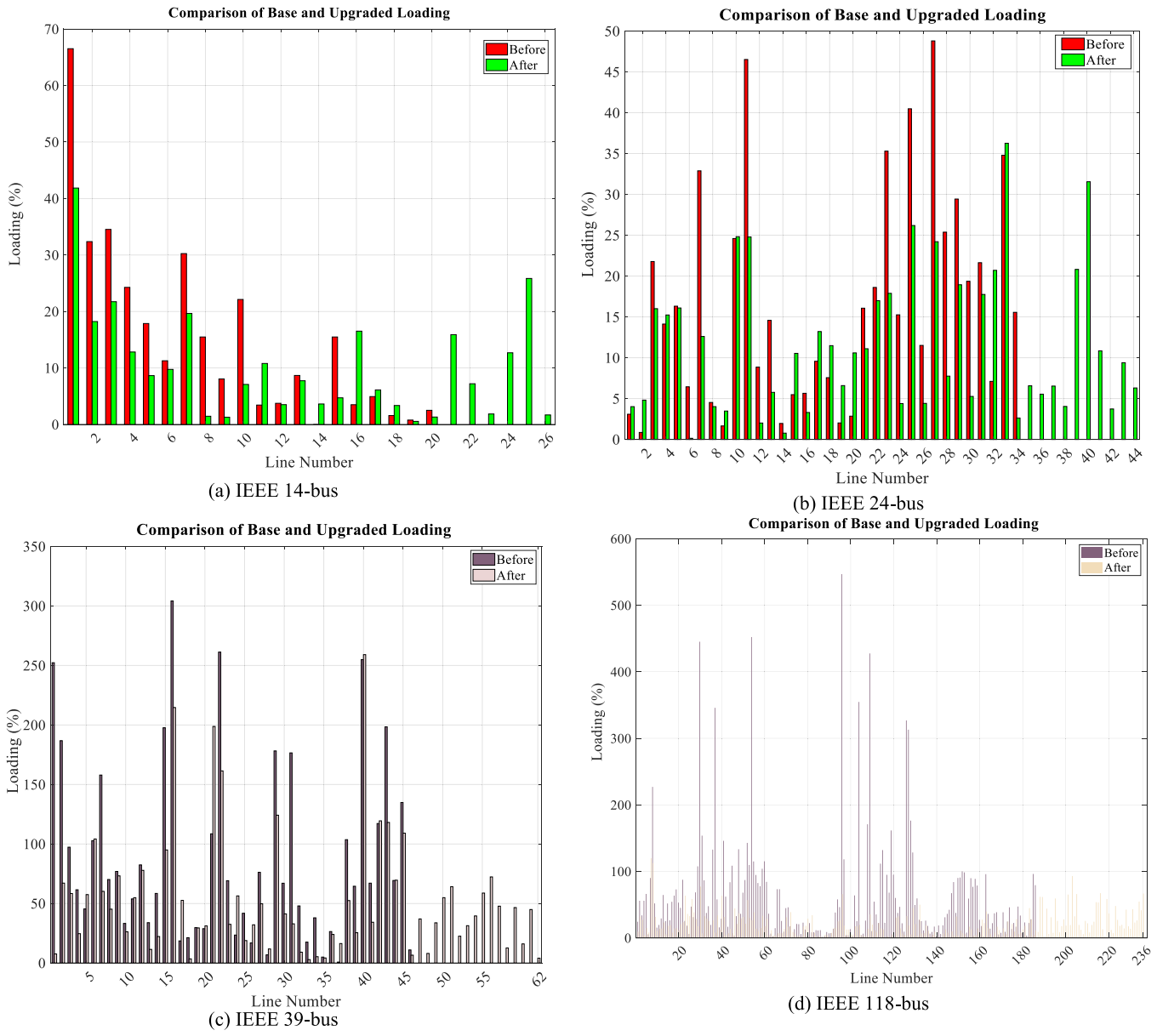


Fig. 16. Power flow before and after line additions.

based resilience metrics [55]. By leveraging weighted betweenness centrality, it prioritizes reinforcements where they are most impactful, delivering measurable improvements in resilience that surpass conventional metric-based methods. This framework offers a more resilient and scalable reconfiguration strategy than modularity-based resource allocation models, focusing on distributed energy resources and switching schemes for microgrid formation [56]. Rather than relying on fixed operational scenarios, it adaptively reshapes network topology to enhance resilience under diverse conditions and failure types.

As power systems become increasingly complex, driven by integrating renewable energy, distributed generation, and digital technologies, future research must focus on a deeper understanding of cyber-physical interactions. Advanced methods such as reinforcement learning, graph neural networks (GNNs), and multi-layer modeling of interconnected infrastructures can significantly improve the accuracy of resilience assessment and enhance the overall robustness of power networks.

Moreover, translating this framework into real-world applications will require careful consideration of economic factors, regulatory policies, and the standardization of resilience metrics across the energy sector. The concept of antifragility, introduced in this study as a transformative addition to resilience, lays the foundation for grid systems that survive attacks and emerge resilient and more adaptable with every challenge they encounter.

5. Conclusion

A novel framework based on graph learning was proposed to enhance the resilience of power systems by integrating the principles of comprehensive robustness (CR) and antifragility. By modeling electrical grids as weighted multigraphs, the framework enables the identification of critical nodes and edges and guides optimal structural reconfiguration through strategic edge augmentation. The resilience metrics applied to IEEE standard test systems, including 14, 24, 39, and 118-bus networks, demonstrated substantial improvements in network comprehensive robustness. Unlike traditional resilience approaches focusing solely on recovery or random fault tolerance, the proposed method provides a unified strategy that strengthens network structure against random and

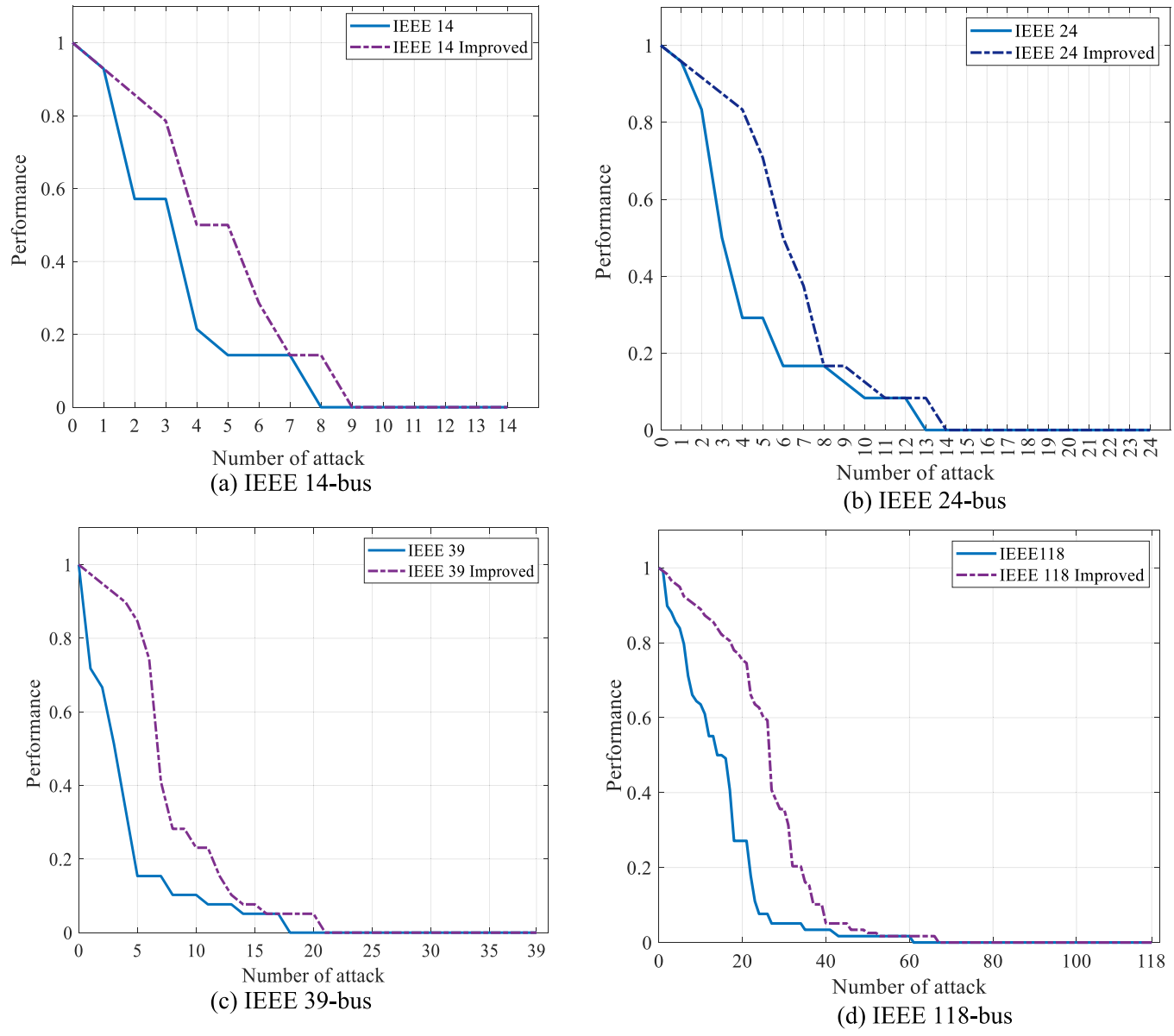


Fig. 17. Improved network resilience based on robustness.

Table 6
Quantitative values of resilience metrics.

Network	Node	Edge	Min degree	Max degree	Resilience based on the robustness	Path length	Cluster coefficient
IEEE 14 bus	14	20	1	6	26.43 %	2.37	0.367
IEEE 14 bus Improved	14	26	2	7	36.71 %	2.04	0.374
IEEE 24 bus	24	34	1	5	19.8 %	3.214	0.035
IEEE 24 bus improved	24	44	2	7	28.62 %	2.500	0.065
IEEE 39 bus	39	46	1	6	11.36 %	4.941	0.074
IEEE 39 bus improved	39	62	1	8	21.64 %	3.231	0.135
IEEE 118 bus	118	186	1	12	12.8 %	6.309	0.165
IEEE 118 bus improved	118	236	1	12	22.22 %	3.962	0.119

malicious attacks. Moreover, the incorporation of antifragility concepts allows power systems not only to withstand disruptions but also to improve performance through reconfiguration. Quantitative analysis across unweighted and weighted multigraph models confirmed the effectiveness of this method in enhancing the resilience of power systems. Metrics such as path length, clustering coefficient, and betweenness centrality showed measurable improvements after implementing the proposed strategies. Overall, the proposed framework provides a scalable solution for designing and enhancing the resilience of power systems capable of adapting to evolving threats and operational challenges.

CRediT authorship contribution statement

Kasra Shafiei: Writing – original draft, Validation, Software, Data curation, Conceptualization. **Mehrdad Tarafdar Hagh:** Resources,

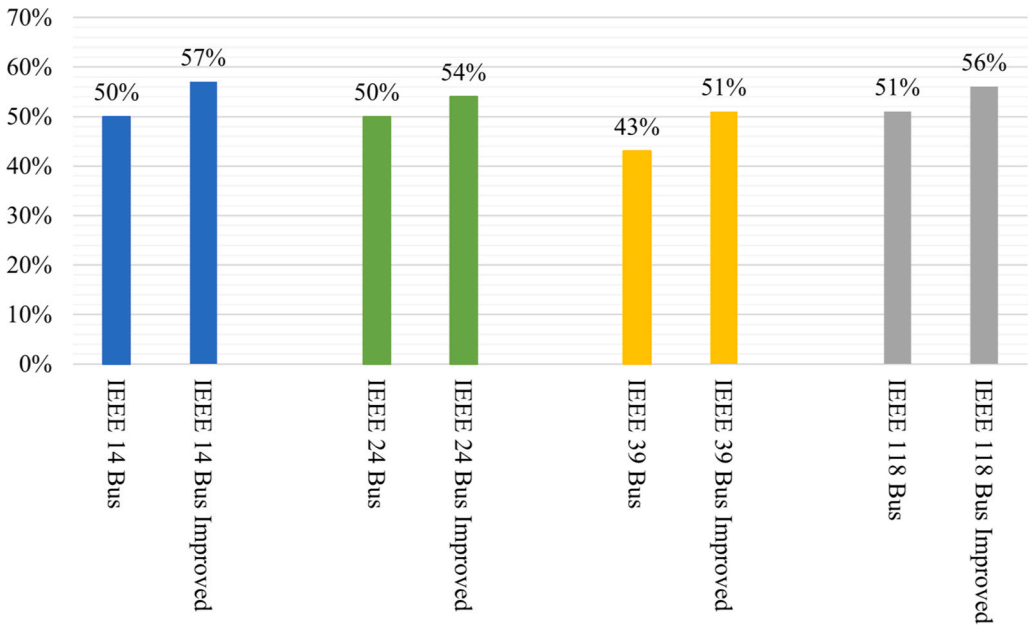


Fig. 18. Percentage of attacked nodes when the number of links reaches zero.

Formal analysis. **Saeid Ghassem Zadeh:** Writing – review & editing, Validation, Supervision, Methodology, Investigation.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] M. Panteli, C. Pickering, S. Wilkinson, R. Dawson, P. Mancarella, Power system resilience to extreme weather: fragility modeling, probabilistic impact assessment, and adaptation measures, IEEE Trans. Power Syst. 32 (5) (2016) 3747–3757.
[2] Z. Bie, Y. Lin, G. Li, F. Li, Battling the extreme: a study on the power system resilience, Proc. IEEE 105 (7) (2017) 1253–1266.
[3] S. Chen, Q. Chen, Q. Xia, H. Zhong, C. Kang, N− 1 security assessment approach based on the steady-state security distance, IET Gener. Transm. Distrib. 9 (15) (2015) 2419–2426.
[4] X. Dong, H. Lin, R. Tan, R.K. Iyer, Z. Kalbarczyk, Software-defined networking for smart grid resilience: opportunities and challenges, Proc. 1st ACM Workshop CyberPhys. Syst. Secur. (2015) 61–68.
[5] Y. Wang, C. Chen, J. Wang, R. Baldick, Research on resilience of power systems under natural disasters—A review, IEEE Trans. Power Syst. 31 (2) (2015) 1604–1613.
[6] M. Yan, Y. He, M. Shahidehpour, X. Ai, Z. Li, J. Wen, Coordinated regional-district operation of integrated energy systems for resilience enhancement in natural disasters, IEEE Trans. Smart Grid 10 (5) (2018) 4881–4892.
[7] E. Shittu, J.R. Santos, Electricity markets and power supply resilience: an incisive review, Curr. Sustain. /Renew. Energy Rep. 8 (4) (2021) 189–198.
[8] K. Shafiei, A. Seifi, M.T. Hagh, A novel multi-objective optimization approach for resilience enhancement considering integrated energy systems with renewable energy, energy storage, energy sharing, and demand-side management, J. Energy Storage 115 (2025) 115966.
[9] K. Shafiei, S.G. Zadeh, M.T. Hagh, Planning for a network system with renewable resources and battery energy storage, focused on enhancing resilience, J. Energy Storage 87 (2024) 111339.
[10] A. Loni, S. Asadi, Power system resilience: the role of electric vehicles and social disparities in mitigating the us power outages, Smart Grids Sustain. Energy 9 (1) (2024) 23.
[11] Y. ATEŞ, T. Gökçek, A.Y. ARABUL, Impact of hybrid power generation on voltage, losses, and electricity cost indistribution networks,", Turk. J. Electr. Eng. Comput. Sci. 29 (3) (2021) 1720–1735.
[12] S. Freitas, D. Yang, S. Kumar, H. Tong, D.H. Chau, Graph vulnerability and robustness: a survey, IEEE Trans. Knowl. Data Eng. 35 (6) (2022) 5915–5934.
[13] D.J. Watts, S.H. Strogatz, Collective dynamics of 'small-world'networks, Nature 393 (6684) (1998) 440–442.
[14] C.M. Schneider, A.A. Moreira, J.S. Andrade, Jr, S. Havlin, H.J. Herrmann, Mitigation of malicious attacks on networks, Proc. Natl. Acad. Sci. 108 (10) (2011) 3838–3841.
[15] M.E. Newman, Assortative mixing in networks, Phys. Rev. Lett. 89 (20) (2002) 208701.
[16] S. Wang, J. Liu, Robustness of single and interdependent scale-free interaction networks with various parameters, Physica A Statis. Mechanics Appl. 460 (2016) 139–151.
[17] M. Kitsak, et al., Identification of influential spreaders in complex networks, Nat. Phys. 6 (11) (2010) 888–893.
[18] R. Albert, H. Jeong, A.-L. Barabási, Error and attack tolerance of complex networks, Nature 406 (6794) (2000) 378–382.
[19] A.E. Motter, Cascade control and defense in complex networks, Phys. Rev. Lett. 93 (9) (2004) 098701.
[20] P. Crucitti, V. Latora, M. Marchiori, Model for cascading failures in complex networks, Phys. Rev. E 69 (4) (2004) 045104.
[21] Y. Jin, Y. Chen, Z. Lu, Q. Zhang, R. Kang, Cascading failure modeling for circuit systems using impedance networks: a current-flow redistribution approach, IEEE Trans. Ind. Electron. 68 (1) (2020) 632–641.
[22] S. Mizutaka, K. Yakubo, Robustness of scale-free networks to cascading failures induced by fluctuating loads, Phys. Rev. E 92 (1) (2015) 012814.
[23] X. Tang, J. Liu, X. Hao, Mitigate cascading failures on networks using a memetic algorithm, Sci. Rep. 6 (1) (2016) 38713.
[24] H.S. Jeong, J. Qiao, D.M. Abraham, M. Lawley, J.P. Richard, Y. Yih, Minimizing the consequences of intentional attack on water infrastructure, Comput. -Aided Civ. Infrastruct. Eng. 21 (2) (2006) 79–92.
[25] X. Gao, M. Peng, K.T. Chi, H. Zhang, A stochastic model of cascading failure dynamics in cyber-physical power systems, IEEE Syst. J. 14 (3) (2020) 4626–4637.
[26] C. Zhai, H. Zhang, G. Xiao, T.-C. Pan, An optimal control approach to identify the worst-case cascading failures in power systems, IEEE Trans. Control Netw. Syst. 7 (2) (2019) 956–966.
[27] M. Panteli, D.N. Trakas, P. Mancarella, N.D. Hatziargyriou, Boosting the power grid resilience to extreme weather events using defensive islanding, IEEE Trans. Smart Grid 7 (6) (2016) 2913–2922.
[28] X. Zhao, J. Liang, J. Wang, A community detection algorithm based on graph compression for large-scale social networks, Inf. Sci. 551 (2021) 358–372.
[29] A. Alashaikh, T. Gomes, D. Tipper, The spine concept for improving network availability, Comput. Netw. 82 (2015) 4–19.
[30] A. Yaldız, T. Gökçek, Y. Ateş, O. Erdinç, Overview and advancement of power system topology addressing pre-and post-event strategies under abnormal operating conditions,", Sustain. Energy Grids Netw. 40 (2024) 101562.
[31] L. Martins, D. Santos, R. Girão-Silva, T. Gomes, A new linear path pair availability constraint for network design, Networks 84 (3) (2024) 326–344.
[32] W. Wei, G. Sun, Q. Zhang, Large-scale robustness-oriented efficient edge addition through traversal tree-based weak edge identification, Chaos Solitons Fractals 179 (2024) 114470.
[33] W. Wei, Q. Hu, Q. Zhang, Improving node connectivity by optimized dual tree-based effective node consolidation, Reliab. Eng. Syst. Saf. 242 (2024) 109747.
[34] S. Wang, X. Gu, J. Chen, C. Chen, X. Huang, Robustness improvement strategy of cyber-physical systems with weak interdependency, Reliab. Eng. Syst. Saf. 229 (2023) 108837.

[35] T. Zang, S. Gao, T. Huang, X. Wei, T. Wang, Complex network-based transmission network vulnerability assessment using adjacent graphs, IEEE Syst. J. 14 (1) (2019) 572–581.
[36] X. Liu, Q. Xie, A multi-strategy framework to evaluate seismic resilience improvement of substations, Reliab. Eng. Syst. Saf. 245 (2024) 110045.
[37] S. Wang, Q. Dong, A multi-source power grid's resilience enhancement strategy based on subnet division and power dispatch, Int. J. Crit. Infrastruct. Prot. 41 (2023) 100602.
[38] J. Beyza, J.M. Yusta, Characterising the security of power system topologies through a combined assessment of reliability, robustness, and resilience, Energy Strategy Rev. 43 (2022) 100944.
[39] C. Zhang, Y.-F. Li, H. Zhang, Y. Wang, Y. Huang, J. Xu, Distributionally robust resilience optimization of post-disaster power system considering multiple uncertainties, Reliab. Eng. Syst. Saf. 251 (2024) 110367.
[40] J. Wu, F. Wu, K. Lin, Z. Wang, L. Shi, Y. Li, An improved AP clustering algorithm based critical nodes identification for distribution network with high PV penetration, IEEE Access 10 (2022) 124619–124628.
[41] R. Rocchetta, Enhancing the resilience of critical infrastructures: statistical analysis of power grid spectral clustering and post-contingency vulnerability metrics, Renew. Sustain. Energy Rev. 159 (2022) 112185.
[42] M. Xu, G. Li, A. Chen, Resilience-driven post-disaster restoration of interdependent infrastructure systems under different decision-making environments, Reliab. Eng. Syst. Saf. 241 (2024) 109599.
[43] T.N. Alrumaih, M.J. Alenazi, Evaluation of industrial network robustness against targeted attacks, Concurr. Comput. Pract. Exp. 35 (27) (2023) e7855.
[44] P. Panigrahi, S. Maity, Structural vulnerability analysis in small-world power grid networks based on weighted topological model, Int. Trans. Electr. Energy Syst. 30 (7) (2020) e12401.
[45] Y. Zhu, G. Liu, Application of triangle count in branch contingency screening, Int. J. Electr. Power Energy Syst. 135 (2022) 107392.
[46] M. Qi, S. Tan, P. Chen, X. Duan, X. Lu, Efficient network intervention with sampling information, Chaos Solitons Fractals 166 (2023) 112952.
[47] J. Zheng, J. Liu, A new scheme for identifying important nodes in complex networks based on generalized degree, J. Comput. Sci. 67 (2023) 101964.
[48] R. Li, Y. Gao, On the component resilience importance measures for infrastructure systems, Int. J. Crit. Infrastruct. Prot. 36 (2022) 100481.
[49] N.L. Dehghani, A.B. Jeddi, A. Shafieezadeh, Intelligent hurricane resilience enhancement of power distribution systems via deep reinforcement learning, Appl. Energy 285 (2021) 116355.
[50] M. Kamruzzaman, J. Duan, D. Shi, M. Benidris, A deep reinforcement learning-based multi-agent framework to enhance power system resilience using shunt resources, IEEE Trans. Power Syst. 36 (6) (2021) 5525–5536.
[51] Y. Huang, G. Li, C. Chen, Y. Bian, T. Qian, Z. Bie, Resilient distribution networks by microgrid formation using deep reinforcement learning, IEEE Trans. Smart Grid 13 (6) (2022) 4918–4930.
[52] R. Sepehrzad, A. Khodadadi, S. Adinehpour, M. Karimi, A multi-agent deep reinforcement learning paradigm to improve the robustness and resilience of grid connected electric vehicle charging stations against the destructive effects of cyber-attacks, Energy 307 (2024) 132669.
[53] H. Xie, L. Tang, H. Zhu, X. Cheng, Z. Bie, Robustness assessment and enhancement of deep reinforcement learning-enabled load restoration for distribution systems, Reliab. Eng. Syst. Saf. 237 (2023) 109340.
[54] S.R. Fahim, et al., Graph autoencoder-based power attacks detection for resilient electrified transportation systems, IEEE Trans. Transp. Electrification 10 (4) (2024) 9539–9553.
[55] M.H.N. Amiri, F. Guéniat, Towards a framework for measurements of power systems resiliency: comprehensive review and development of graph and vector-based resilience metrics,", Sustain. Cities Soc. (2024) 105517.
[56] S. Mousavizadeh, A. Alahyari, T.G. Bolandi, M.R. Haghifam, P. Siano, A novel resource allocation model based on the modularity concept for resiliency enhancement in electric distribution networks, Int. J. Energy Res. 45 (9) (2021) 13471–13488.
[57] D. Kumar, A. Kumar, A robust approach to resiliency enhancement of distribution system using ensembled deep reinforcement learning, Energy Syst. (2025) 1–40.
[58] D. Coppitters, F. Contino, Optimizing upside variability and antifragility in renewable energy system design, Sci. Rep. 13 (1) (2023) 9138.
[59] R. Dahlberg, Resilience and complexity: conjoining the discourses of two contested concepts, Cult. Unbound 7 (3) (2015) 541–557.
[60] F. Yahya, M. Rafiq, Brownfield, greenfield, and renewable energy consumption: moderating role of effective governance, Energy Environ. 31 (3) (2020) 405–423.
[61] N.L. Dehghani, S. Zamanian, A. Shafieezadeh, Adaptive network reliability analysis: methodology and applications to power grid, Reliab. Eng. Syst. Saf. 216 (2021) 107973.
[62] H. Cetinay, K. Devriendt, P. Van Mieghem, Nodal vulnerability to targeted attacks in power grids, Appl. Netw. Sci. 3 (2018) 1–19.
[63] X. Zhang, D. Liu, H. Tu, C.K. Tse, An integrated modeling framework for cascading failure study and robustness assessment of cyber-coupled power grids, Reliab. Eng. Syst. Saf. 226 (2022) 108654.
[64] J. Thomas, S. Ghosh, D. Parek, D. Ruths, and J. Ruths, "Robustness of network controllability to degree-based edge attacks," in Complex Networks & Their Applications V: Proceedings of the 5th International Workshop on Complex Networks and their Applications (COMPLEX NETWORKS 2016), 2017: Springer, pp. 525-537.
[65] Y. Lou, L. Wang, G. Chen, A framework of hierarchical attacks to network controllability, Commun. Nonlinear Sci. Numer. Simul. 98 (2021) 105780.
[66] G. Chen, Y. Lou, L. Wang, A comparative study on controllability robustness of complex networks, IEEE Trans. Circuits Syst. II Express Briefs 66 (5) (2019) 828–832.
[67] B. Hartmann, How does the vulnerability of an evolving power grid change? Electr. Power Syst. Res. 200 (2021) 107478.
[68] G.A. Pagani, M. Aiello, The power grid as a complex network: a survey, Physica A Statis. Mechanics Appl. 392 (11) (2013) 2688–2700.
[69] R. Albert, I. Albert, G.L. Nakarado, Structural vulnerability of the north American power grid, Phys. Rev. E 69 (2) (2004) 025103.
[70] L. Lü, D. Chen, X.-L. Ren, Q.-M. Zhang, Y.-C. Zhang, T. Zhou, Vital nodes identification in complex networks, Phys. Rep. 650 (2016) 1–63.
[71] L.C. Freeman, "Centrality in social networks: conceptual clarification, in: Social network: critical concepts in sociology, 1, Routledge, *Londres*, 2002, pp. 238–263.
[72] P. Bonacich, Factoring and weighting approaches to status scores and clique identification, J. Math. Sociol. 2 (1) (1972) 113–120.
[73] A.-L. Barabási, R. Albert, Emergence of scaling in random networks, Science 286 (5439) (1999) 509–512.
[74] H.J. Herrmann, C.M. Schneider, A.A. Moreira, J.S. Andrade, S. Havlin, Onion-like network topology enhances robustness against malicious attacks (vol), J. Stat. Mech. Theory Exp. (01) (2011).
[75] Y. Bengio, A. Courville, P. Vincent, Representation learning: a review and new perspectives, IEEE Trans. Pattern Anal. Mach. Intell. 35 (8) (2013) 1798–1828.
[76] S.T. Roweis, L.K. Saul, Nonlinear dimensionality reduction by locally linear embedding, science 290 (5500) (2000) 2323–2326.
[77] H. Bahonar, A. Mirzaei, S. Sadri, R.C. Wilson, Graph embedding using frequency filtering, IEEE Trans. Pattern Anal. Mach. Intell. 43 (2) (2019) 473–484.
[78] Y. Xu, A.J. Gurfinkel, P.A. Rikvold, Architecture of the florida power grid as a complex network, Physica A Statis. Mechanics Appl. 401 (2014) 130–140.
[79] M.E. Newman, Analysis of weighted networks, Phys. Rev. E Stat. Nonlinear Soft Matter Phys. 70 (5) (2004) 056131.
[80] M.E. Newman, Scientific collaboration networks. Ii. shortest paths, weighted networks, and centrality, Phys. Rev. E 64 (1) (2001) 016132.
[81] M.R. Narimani, et al., Generalized contingency analysis based on graph theory and line outage distribution factor, IEEE Syst. J. 16 (1) (2021) 626–636.
[82] A. Kumar, S.S. Singh, K. Singh, B. Biswas, Level-2 node clustering coefficient-based link prediction, Appl. Intell. 49 (2019) 2762–2779.
[83] S. Forsberg, K. Thomas, M. Bergkvist, Power grid vulnerability analysis using complex network theory: a topological study of the nordic transmission grid, Physica A Statis. Mechanics Appl. 626 (2023) 129072.
[84] R. Albert, A.-L. Barabási, Statistical mechanics of complex networks, Rev. Mod. Phys. 74 (1) (2002) 47.
[85] Å.J. Holmgren, Using graph models to analyze the vulnerability of electric power networks, Risk Anal. 26 (4) (2006) 955–969.
[86] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, Z.W. Geem, A critical review of robustness in power grids using complex networks concepts,", Energies 8 (9) (2015) 9211–9265.
[87] J. Li, C. Shi, C. Chen, L. Dueñas-Osorio, A cascading failure model based on AC optimal power flow: case study, Physica A Statis. Mechanics Appl. 508 (2018) 313–323.
[88] A. Abedi, L. Gaudard, F. Romerio, Review of major approaches to analyze vulnerability in power system, Reliab. Eng. Syst. Saf. 183 (2019) 153–172.
[89] F. Morone, H.A. Makse, Influence maximization in complex networks through optimal percolation, Nature 524 (7563) (2015) 65–68.
[90] R. Cohen, S. Havlin, Complex networks: structure, robustness and function, Cambridge university press, 2010.
[91] W. Li, et al., Maximizing network resilience against malicious attacks, Scientific reports 9 (1) (2019) 2261.