

Article

Real-Time Small-Signal Security Assessment of Power Systems Using an Edge-Enhanced Graph Attention Network

Weiran Jiao ^{1,*}, Mingyuan Wang ¹, Qian Sun ¹, Kangli Liu ¹ and Jianfeng Zhao ^{1,2}¹ School of Electrical Engineering, Southeast University, Nanjing 210096, China; 220252993@seu.edu.cn (M.W.); qiansuncn@seu.edu.cn (Q.S.); kangli@seu.edu.cn (K.L.); jianfeng_zhao@seu.edu.cn (J.Z.)² College of Information Science and Technology & Artificial Intelligence, Nanjing Forestry University, Nanjing 210037, China

* Correspondence: vivi@seu.edu.cn

Abstract

Conventional small-signal security assessment requires repeated power flow calculations, system linearization, and eigenvalue analysis, resulting in considerable computational burden for online applications. Moreover, existing data-driven methods generally provide insufficient representation of branch power flows, line operating states, and incomplete PMU measurements. To address these limitations, this paper proposes an edge-enhanced graph attention network (EE-GAT) for real-time small-signal security assessment. The model takes bus voltage magnitude, phase angle, active and reactive power injections, and PMU availability masks as node features, while branch active and reactive power flows and line operating states are incorporated as edge features. An edge-enhanced multi-head attention mechanism is employed to jointly learn node state and branch coupling information, and a global attention readout mechanism is used to construct the system-level representation for secure/insecure classification. Tests on the New England 39-bus and NPCC 140-bus systems show that EE-GAT achieves accuracies of 97.75% and 96.47%, respectively, outperforming XGBoost, LSTM, CNN, GCN, and conventional GAT. The proposed model also maintains superior performance under incomplete PMU measurements and requires only 0.0034 s and 0.0051 s for the corresponding test batches, demonstrating its potential for online small-signal security screening.

Keywords: small-signal security assessment; graph attention network; edge feature enhancement; power system stability; phasor measurement unit



Academic Editor: Roberto Zivieri

Received: 7 July 2026

Revised: 24 July 2026

Accepted: 27 July 2026

Published: 30 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

Power system security refers to the ability of a power system to withstand anticipated disturbances and potential contingencies without interrupting electricity supply or violating operating constraints [1]. Small-signal stability is an important component of dynamic security assessment, reflecting the capability of a power system to maintain synchronism and damp low-frequency oscillations in the face of small disturbances [2,3]. With the large-scale integration of renewable generation, increasing penetration of power electronic devices, and growing complexity of operating conditions, system inertia, power flow distributions, and damping characteristics exhibit stronger uncertainty and time-varying properties. Consequently, small-signal security assessment (SSSA) faces more stringent requirements for real-time performance, robustness, and accuracy. As shown in Figure 1, modern power systems consist of various source and load units, including conventional

generating units, wind farms, photovoltaic plants, substations, and residential, commercial, and industrial loads.

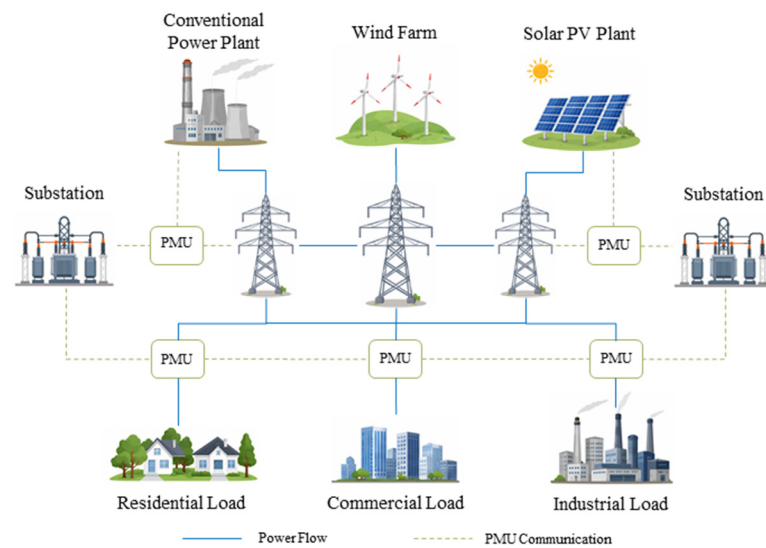


Figure 1. Modern power system with renewable generation and PMU measurements.

Conventional SSSA methods are mainly based on the linearization of power system differential algebraic equations. By constructing the state matrix and calculating its eigenvalues, the frequencies and damping ratios of critical oscillation modes can be obtained, and the security margin can be evaluated according to a damping threshold. These methods have clear physical mechanisms and high analytical accuracy but require complete and accurate dynamic models of generators, exciters, governors, and loads. In practical systems, equipment parameters and controller models may be uncertain or unavailable. Moreover, when multiple operating conditions and $N-1$ contingencies are considered, conventional methods must perform power flow calculation, dynamic simulation, or eigenvalue analysis for many scenarios, resulting in a heavy computational burden and limiting their applicability to real-time online assessment [4–6].

To reduce the computational cost of dynamic security assessment, direct methods such as transient energy functions, Lyapunov function approximation, and the extended equal area criterion have been investigated [4,7]. Although these methods can partly avoid complete time-domain simulations, they still rely on detailed system models and carefully designed physical features. Their applicability and generalization capability may be limited when the system's scale increases, control devices become more diverse, or operating conditions vary significantly.

With the deployment of phasor measurement units (PMUs) and wide-area measurement systems, data-driven security assessment methods have attracted increasing attention [8,9]. Early machine learning methods, such as decision trees, support vector machines, and kernel ridge regression, have been applied to stability boundary fitting and post-fault stability prediction [10–12]. These methods can learn a nonlinear mappings between operating states and security labels from historical or simulated data, thereby reducing dependence on detailed dynamic models. However, they usually rely on manual feature selection and have limited representation ability for high-dimensional PMU measurements, complex operating conditions, and large-scale network topologies.

In recent years, deep learning has been increasingly applied to power system security assessment due to its nonlinear feature extraction capability [13]. Deep autoencoders have been used for security assessment feature learning [14], and convolutional neural networks (CNNs) have been employed for faulted line localization and security status

classification [15]. For SSSA, CNN-based methods usually convert operating points into two-dimensional feature matrices or images and classify them into secure and insecure states [16]. Nevertheless, CNNs are designed for regular grid-structured data, whereas power systems are naturally represented as non-Euclidean graphs composed of buses and transmission lines. Converting power system states into image-like representations may weaken the original bus–branch connectivity and electrical coupling. In contrast, graph neural networks are designed for relational data and can directly preserve these structural characteristics.

Accordingly, graph neural networks (GNNs) have been applied to outage prediction, fault chain prediction, optimal power flow, state estimation, transient stability prediction, and stability contingency screening [17–21]. For small-signal stability-related tasks, residual graph convolutional networks have been used to predict damping ratios and oscillation frequencies [22], and temporal–topological embedding networks have been adopted for power system stability analysis [23]. In addition, GNN-based real-time SSSA methods can use PMU or power flow data to achieve rapid secure/insecure classification and improve training efficiency and robustness against missing measurements [24].

Although existing GNN-based methods can exploit power grid topology, most of them aggregate information mainly based on bus node features, while the impacts of transmission line power flow states, line operating status, and topology variations are not sufficiently modeled. In fact, the $N-1$ small-signal security of an operating condition is related not only to local bus quantities, such as voltages and nodal power injections, but also pre-contingency inter-area power transfers, branch loading patterns, and electrical coupling relationships. These branch-level operating quantities contain useful information for evaluating the vulnerability of the current operating condition to subsequent contingencies. Therefore, incorporating branch features, such as active and reactive power flows and current line operating states, can provide a more complete representation of the pre-contingency operating condition for GNN-based SSSA.

To this end, this paper proposes an Edge-Enhanced Graph Attention Network (EE-GAT) for real-time small-signal security assessment. Graph attention networks (GATs) can adaptively learn the importance of neighboring nodes through the attention mechanism [25]. Based on this mechanism, the proposed EE-GAT explicitly introduces branch active power, branch reactive power, and line operating status into the calculation of attention coefficients. As a result, the model jointly represents bus states, branch operating information, and network connectivity to learn a nonlinear mapping from a pre-contingency operating condition to its corresponding $N-1$ small-signal security label, thereby enabling rapid secure/insecure classification. It should be emphasized that EE-GAT is intended as a rapid security screening and decision support tool rather than an autonomous protection or control system. Operating conditions identified as insecure or close to the security boundary can still be examined through detailed eigenvalue or modal analysis.

The main contributions of this paper are summarized as follows. First, an edge-enhanced graph attention mechanism is developed to explicitly incorporate branch power flows and line operating states into neighborhood information aggregation, enabling the model to represent both nodal operating conditions and electrical coupling relationships. Second, a PMU availability mask is introduced to distinguish truly observed measurements from zero-filled missing measurements, thereby improving robustness under incomplete measurement conditions. Third, a global attention readout mechanism is employed to adaptively aggregate bus-level representations into a system-level representation for real-time small-signal security classification.

The remainder of this paper is organized as follows. Section 2 introduces the formulation of the small-signal security assessment problem and the construction of graph-

structured power system features. Section 3 presents the proposed EE-GAT model, including the edge-enhanced attention mechanism, global attention pooling, and missing measurement handling strategy. Section 4 validates the effectiveness of the proposed method through case studies on the New England 39-bus system and the NPCC 140-bus system. Section 5 discusses the applicability and limitations of the proposed method, and Section 6 concludes the paper.

2. Problem Formulation

2.1. Fundamentals of Small-Signal Security Assessment

In this study, small-signal security refers to the ability of a power system to maintain stable electromechanical oscillations following small disturbances around a feasible steady-state operating point. An operating scenario is regarded as a small-signal case when a valid pre- or post-contingency equilibrium exists and the system can be locally linearized around this equilibrium. The security state is then evaluated using the eigenvalues and damping ratios of the linearized model. For an $N-1$ line outage scenario, the line disconnection itself is a discrete topology change rather than a small disturbance. After the outage, the post-contingency power flow is solved to obtain a new steady-state operating point. If a valid equilibrium exists, small-signal analysis is performed around this point. Therefore, this study assesses the small-signal security of the post-contingency system rather than the large disturbance transient process caused by the outage.

After a power system is subjected to small disturbances around a steady-state operating point, its dynamic behavior can usually be described by the following nonlinear differential algebraic equations

$$\dot{x} = f(x, y, u), \quad (1)$$

$$0 = g(x, y, u), \quad (2)$$

where x denotes the vector of dynamic state variables, y denotes the vector of algebraic variables, and u denotes the vector of input or disturbance variables. By linearizing the differential algebraic equations around the equilibrium point and eliminating the algebraic variable increments, the following reduced state-space model is obtained:

$$\Delta\dot{x} = A\Delta x + B\Delta u, \quad (3)$$

where A is the reduced state matrix and B is the input matrix. Small-signal stability can be evaluated from the eigenvalues of A . The i -th oscillatory eigenvalue is expressed as

$$\lambda_i = \sigma_i \pm j\omega_i, \quad (4)$$

where σ_i and ω_i denote the real and imaginary parts, respectively. The corresponding damping ratio is calculated as

$$\zeta_i = -\frac{\sigma_i}{\sqrt{\sigma_i^2 + \omega_i^2}}. \quad (5)$$

An operating condition is classified as small-signal secure if all critical electromechanical modes have negative real parts and satisfy

$$\zeta_{\min} \geq \zeta_{\min}^{\text{th}}, \quad (6)$$

where $\zeta_{\min}^{\text{th}} = 3\%$ is the damping ratio threshold adopted in this study. Otherwise, the operating condition is classified as insecure.

2.2. Power Grid Graph Modeling and Input Feature Construction

For each operating condition, the input to the proposed EE-GAT is represented as a graph-structured sample consisting of the network topology, node features, and edge features. Specifically, the power system is modeled as a graph

$$\mathcal{G} = (\mathcal{V}, \mathcal{E}), \quad (7)$$

where $\mathcal{V}$ denotes the set of bus nodes and $\mathcal{E}$ denotes the set of transmission line edges. For a power system with N buses and M transmission lines, the complete model input is expressed as

$$\mathcal{I} = (\mathcal{G}, \mathbf{X}, \mathbf{E}) \quad (8)$$

where $\mathcal{G}$ describes the network topology, $\mathbf{X}$ is the node feature matrix, and $\mathbf{E}$ is the edge feature matrix. The node feature matrix is expressed as

$$\mathbf{X} = [\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_N]^T \in \mathbb{R}^{N \times d_x}, \quad (9)$$

and the edge feature matrix is expressed as

$$\mathbf{E} = [\mathbf{e}_{i_1 j_1}^T, \mathbf{e}_{i_2 j_2}^T, \dots, \mathbf{e}_{i_M j_M}^T]^T \in \mathbb{R}^{M \times d_e}, \quad (10)$$

where (i_m, j_m) denotes the m -th transmission-line edge in $\mathcal{E}$ and d_x and d_e denote the dimensions of node and edge features, respectively.

The node-level input features characterize the operating state and measurement availability of each bus. For bus node i , the node feature vector is constructed as

$$\mathbf{x}_i = [V_i, \theta_i, P_i, Q_i, m_i], \quad (11)$$

where V_i is the voltage magnitude of bus i , θ_i is the voltage phase angle, P_i and Q_i are the nodal active and reactive power injections, respectively, and m_i is the PMU availability mask. Specifically, $m_i = 1$ indicates that the measurement at bus i is available, whereas $m_i = 0$ indicates that the measurement is missing. The PMU mask enables the model to distinguish between available measurements and filled missing values, thereby improving its robustness under incomplete measurement conditions.

The edge-level input features characterize the power transfer state and operating status of each transmission line. For branch (i, j) , the edge feature vector is constructed as

$$\mathbf{e}_{ij} = [P_{ij}, Q_{ij}, s_{ij}], \quad (12)$$

where P_{ij} and Q_{ij} are the active and reactive power flows on branch (i, j) , respectively, and s_{ij} denotes the line operating status. Specifically, $s_{ij} = 1$ indicates that the branch is in service, whereas $s_{ij} = 0$ indicates that the branch is disconnected. For each physical branch, the direction of P_{ij} and Q_{ij} is defined according to the reference direction in the original branch data. Consequently, the edge features provide the model with explicit information on transmission corridor loading, power flow direction, and topology variations caused by line outages.

Accordingly, each EE-GAT input sample comprises the current network topology $\mathcal{G}$, the node operating state matrix $\mathbf{X}$, and the branch operating state matrix $\mathbf{E}$. This graph-structured representation enables the model to jointly capture nodal operating conditions, branch power transfers, measurement availability, and topology changes.

2.3. Output Definition and Binary Classification Formulation

The output of the proposed EE-GAT comprises a continuous security probability and the corresponding binary security classification. During supervised training, each operating condition is assigned a ground truth label according to the minimum damping ratio of its critical oscillatory modes.

For the m -th operating condition, the ground truth security label is defined as

$$y_m = \begin{cases} 1, & \zeta_{\min}^m \geq \zeta_{\min}^{\text{th}} \\ 0, & \zeta_{\min}^m < \zeta_{\min}^{\text{th}} \end{cases} \quad (13)$$

where $\zeta_{\min}^m$ denotes the minimum damping ratio among the critical oscillatory modes associated with the m -th operating condition and the considered contingencies and $\zeta_{\min}^{\text{th}}$ denotes the prescribed security threshold. Therefore, $y_m = 1$ represents a secure operating condition, whereas $y_m = 0$ represents an insecure operating condition.

Given the graph-structured input $(\mathcal{G}_m, \mathbf{X}_m, \mathbf{E}_m)$, the objective of EE-GAT is to learn a nonlinear mapping from the current operating condition to the probability that the system is in a small-signal secure state:

$$\hat{y}_m = F_{\Theta}(\mathcal{G}_m, \mathbf{X}_m, \mathbf{E}_m), \quad \hat{y}_m \in [0, 1], \quad (14)$$

where $F_{\Theta}(\cdot)$ denotes the EE-GAT model parameterized by Θ and $\hat{y}_m$ denotes the predicted probability that the m -th operating condition is small-signal secure. A value of $\hat{y}_m$ closer to 1 indicates a higher predicted likelihood of security, whereas a value closer to 0 indicates a higher predicted likelihood of insecurity.

The continuous probability output is converted into the final binary classification result according to

$$\hat{c}_m = \begin{cases} 1, & \hat{y}_m \geq \tau \\ 0, & \hat{y}_m < \tau \end{cases} \quad (15)$$

where τ is the classification threshold, which is set to 0.5 in this study unless otherwise specified. Accordingly, $\hat{c}_m = 1$ indicates that the operating condition is classified as secure, whereas $\hat{c}_m = 0$ indicates that it is classified as insecure.

Therefore, the direct model output is the scalar security probability $\hat{y}_m$, while the final assessment output is the binary security state $\hat{c}_m$.

3. Proposed Model

3.1. Overall Framework

The proposed EE-GAT is designed for real-time small-signal security assessment, aiming to rapidly determine whether a power system satisfies the small-signal security requirement under a given operating point and network topology. As shown in Figure 2, the proposed method consists of two main stages: offline training and online assessment.

In the offline training stage, various operating conditions are first generated by randomly perturbing the load levels and generator outputs. For each operating condition, a power flow calculation is performed to obtain the pre-contingency bus operating states and branch power flow states. Subsequently, $N-1$ small-signal stability analysis is conducted to determine the corresponding security label. Specifically, the pre-contingency operating condition is labeled according to whether the system satisfies the prescribed small-signal security criterion under all considered $N-1$ contingencies. The power system before the occurrence of any contingency is then represented as a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, in which buses are modeled as nodes and transmission lines are modeled as edges. Accordingly, the node feature matrix $\mathbf{X}$ and edge feature matrix $\mathbf{E}$ are constructed using the pre-contingency

operating states and network topology. The node features include bus voltage magnitude, voltage phase angle, nodal active power injection, nodal reactive power injection, and the PMU measurement mask, whereas the edge features include branch active power flow, branch reactive power flow, and line operating status. The EE-GAT model is trained in a supervised manner using these labeled pre-contingency graph samples, enabling it to learn a nonlinear mapping from the current system operating condition to the corresponding $N-1$ small-signal security state.

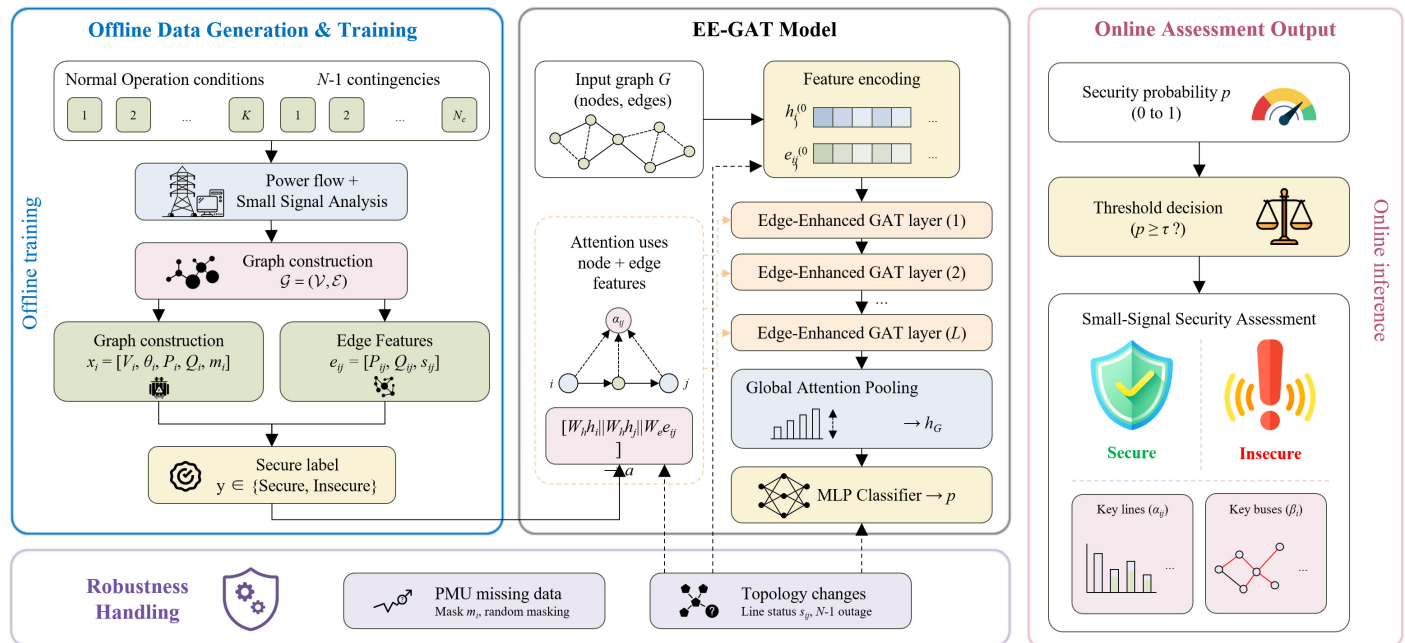


Figure 2. Overall framework of the proposed Edge-Enhanced Graph Attention Network.

In terms of model architecture, EE-GAT consists of an input feature encoding layer, edge-enhanced graph attention layers, a global attention pooling layer, and a security classifier. The input feature encoding layer maps the original node and edge features into a unified hidden feature space. The edge-enhanced graph attention layers simultaneously consider the states of neighboring buses and the corresponding branch states during neighborhood information aggregation and adaptively assign attention weights according to branch power flows and line operating status. Unlike the standard GAT, which computes attention coefficients only based on node features, EE-GAT explicitly incorporates edge features into the attention computation, enabling the model to identify key transmission corridors that have significant impacts on the small-signal security boundary. After multiple layers of edge-enhanced graph attention propagation, each bus node obtains a high-dimensional representation that integrates neighborhood topology, power flow distribution, and line status information.

Because small-signal security assessment is a system-level classification task, a global attention pooling layer is further adopted to aggregate all node representations into a system-level graph representation h_G . This pooling process can adaptively learn the contribution of different buses to the final security classification result, thereby highlighting the effects of critical buses and weak areas. Finally, the graph-level representation is fed into a multilayer perceptron classifier to output the probability $\hat{y}$ that the current operating point is in a small-signal secure state, and the secure/insecure binary classification decision is made according to a predefined threshold.

In the online application stage, the trained EE-GAT no longer requires sequential $N-1$ contingency simulations or eigenvalue calculations. For a real-time operating point, only

the corresponding node features, edge features, and topological relationships need to be constructed. The small-signal security assessment result can then be obtained through a single forward propagation. Therefore, the proposed method improves the online computational efficiency of small-signal security assessment while preserving the physical information embedded in the power grid graph structure. In addition, the learned attention weights provide a basis for subsequent identification of critical buses and critical branches.

The overall offline training and online assessment procedure of the proposed EE-GAT is summarized in Algorithm 1. In the offline stage, labeled graph samples are constructed by combining power flow calculation, $N-1$ contingency analysis, small-signal stability analysis, and security label generation. In the online stage, the trained EE-GAT directly maps the real-time graph features to the security probability, thereby avoiding repeated eigenvalue calculations.

Algorithm 1 Offline Training and Online Assessment Procedure of EE-GAT

Require: Power grid topology $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, operating condition set Ω , contingency set $\mathcal{C}$, damping ratio threshold $\zeta_{\min}^{\text{th}}$

Ensure: Trained EE-GAT model F_{θ} and online security assessment result $\hat{y}$

Offline training stage:

for each operating condition $\omega \in \Omega$ **do**

 Run power flow calculation to obtain bus and branch operating states and calculate the minimum damping ratio $\zeta_{\min}$

 Construct the graph topology $\mathcal{G}$, node feature matrix $\mathbf{X}$ and edge feature matrix $\mathbf{E}$

for each contingency $c \in \mathcal{C}$ **do**

 Update line operating status and run power flow calculation

 Perform small-signal stability analysis and calculate the minimum damping ratio $\zeta_{\min}$

end for

 Assign security label y according to $\zeta_{\min}$ and the threshold $\zeta_{\min}^{\text{th}}$

end for

Train EE-GAT by minimizing the binary cross-entropy loss

Online assessment stage:

Acquire real-time measurements and construct the corresponding node features $\mathbf{X}$, edge features $\mathbf{E}$, and topology $\mathcal{G}$

Obtain the predicted security probability $\hat{y} = F_{\theta}(\mathcal{G}, \mathbf{X}, \mathbf{E})$

Determine the secure/insecure state according to the predefined threshold τ

3.2. Edge-Enhanced Attention Mechanism

A standard graph attention network [25] mainly computes attention weights using the hidden representations of node i and its neighboring node j . The attention coefficient is usually expressed as

$$\alpha_{ij} = \text{softmax}_j \left(\text{LeakyReLU} \left(a^T [W h_i \| W h_j] \right) \right), \quad (16)$$

where W is the node feature transformation matrix, a is the attention vector, and $\|$ denotes vector concatenation. This mechanism can learn the importance of different neighboring

nodes, but it does not explicitly consider the impacts of branch power flows and line status on information transmission between nodes.

To further illustrate how branch operating information is incorporated into the attention calculation, the edge-enhanced attention mechanism is shown in Figure 3. Unlike the standard graph attention mechanism, the proposed EE-GAT introduces the edge feature vector e_{ij} into the attention score calculation, enabling the model to jointly consider node states, branch power flows, and line operating status. At the l -th layer, the unnormalized attention score between node i and its neighboring node j is defined as

$$r_{ij}^{(l)} = \text{LeakyReLU}\left(a^T [W_h h_i^{(l)} \| W_h h_j^{(l)} \| W_e e_{ij}]\right), \quad (17)$$

where $h_i^{(l)}$ and $h_j^{(l)}$ are the hidden representations of nodes i and j at the l -th layer, respectively, W_h is the node feature transformation matrix, and W_e is the edge feature transformation matrix.

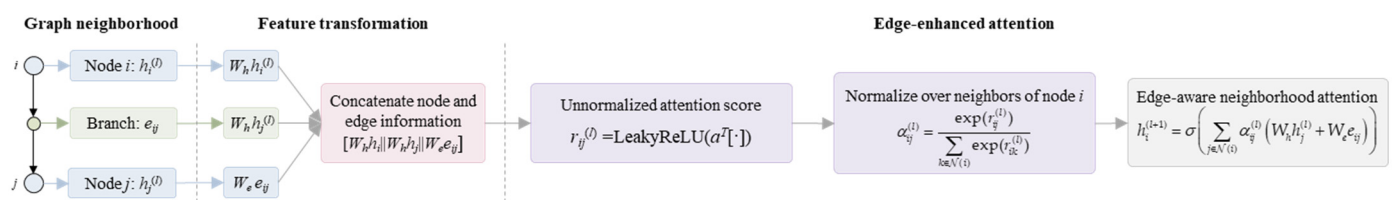


Figure 3. Illustration of the edge-enhanced attention mechanism.

By normalizing over the neighborhood of node i , the edge-enhanced attention weight is obtained as

$$\alpha_{ij}^{(l)} = \frac{\exp(r_{ij}^{(l)})}{\sum_{k \in \mathcal{N}(i)} \exp(r_{ik}^{(l)})}, \quad (18)$$

where $\mathcal{N}(i)$ denotes the set of neighboring nodes of node i .

After obtaining the attention weights, the state of node i is updated by

$$h_i^{(l+1)} = \sigma \left(\sum_{j \in \mathcal{N}(i)} \alpha_{ij}^{(l)} (W_h h_j^{(l)} + W_e e_{ij}) \right), \quad (19)$$

where $\sigma(\cdot)$ is a nonlinear activation function. It can be seen that when aggregating neighboring bus information, EE-GAT considers not only the operating states of neighboring buses but also branch power flows and line status as important factors affecting information transmission.

3.3. Multi-Head Attention Mechanism

To improve the representation capability and training stability of the model, a multi-head attention mechanism is adopted. For the k -th attention head, the updated representation of node i is given by

$$h_{i,k}^{(l+1)} = \sigma \left(\sum_{j \in \mathcal{N}(i)} \alpha_{ij,k}^{(l)} (W_{h,k} h_j^{(l)} + W_{e,k} e_{ij}) \right). \quad (20)$$

The outputs of K attention heads are concatenated as

$$h_i^{(l+1)} = \parallel_{k=1}^K h_{i,k}^{(l+1)}. \quad (21)$$

In the final layer, the outputs of multiple attention heads can also be averaged to obtain a more stable node representation:

$$h_i^{(L)} = \frac{1}{K} \sum_{k=1}^K h_{i,k}^{(L)}. \quad (22)$$

3.4. Global Attention Pooling and Graph-Level Representation

Small-signal security assessment is a system-level classification task, and therefore the hidden representations of all bus nodes need to be aggregated into a graph-level representation. In this paper, a global attention pooling mechanism is adopted to adaptively learn the importance of different buses for system security classification. The pooling weight of node i is defined as

$$\beta_i = \frac{\exp(q^T \tanh(W_p h_i^{(L)}))}{\sum_{r \in \mathcal{V}} \exp(q^T \tanh(W_p h_r^{(L)}))}, \quad (23)$$

where W_p and q are trainable parameters.

The system-level graph representation is obtained as

$$h_G = \sum_{i \in \mathcal{V}} \beta_i h_i^{(L)}. \quad (24)$$

A larger β_i indicates that bus i contributes more to the final small-signal security classification result.

3.5. Security Classifier and Loss Function

The graph-level representation h_G is fed into a multilayer perceptron to obtain the system security probability:

$$p = \text{Sigmoid}(\text{MLP}(h_G)). \quad (25)$$

where $p \in [0, 1]$ denotes the probability that the system is in a small-signal secure state.

The model is trained using the binary cross-entropy loss function:

$$\mathcal{L}_{\text{BCE}} = -\frac{1}{M} \sum_{m=1}^M [y_m \log(p_m) + (1 - y_m) \log(1 - p_m)], \quad (26)$$

where M is the number of training samples, y_m is the ground-truth label of the m -th sample, and p_m is the predicted security probability.

To prevent overfitting, an L_2 regularization term can be introduced during training:

$$\mathcal{L} = \mathcal{L}_{\text{BCE}} + \lambda \|\Theta\|_2^2, \quad (27)$$

where λ is the regularization coefficient and Θ denotes all trainable parameters of the model.

3.6. Handling Missing PMU Measurements and Topology Variations

In practical power systems, incomplete PMU deployment, measurement loss, or communication anomalies may occur. To improve the adaptability of the model to missing measurements, a PMU measurement mask m_i is introduced into the node features. When the measurement of a bus is available, $m_i = 1$; when the measurement is missing, $m_i = 0$, and the missing features are filled by zero filling or mean filling. By randomly masking part of the node measurements during training, the model can learn to perform security assessment under incomplete observation conditions.

For topology variations and $N-1$ line outage scenarios, this paper models them through the line operating status s_{ij} in the edge features. When line (i, j) is in service, $s_{ij} = 1$; when the line is disconnected, $s_{ij} = 0$. In EE-GAT, the line status directly participates in the computation of attention weights. Therefore, the model can dynamically adjust the information transmission strength between nodes according to the line switching status, thereby adapting to small-signal security assessment tasks under different network topologies.

4. Case Studies

4.1. Data Construction

To evaluate the effectiveness of the proposed EE-GAT model for real-time small-signal security assessment, the New England 39-bus system and the NPCC 140-bus system are selected as test systems. The New England 39-bus system comprises 39 buses, 46 branches, and 10 generators, whereas the NPCC 140-bus system comprises 140 buses, 233 branches, and 48 generators. The operating samples and their corresponding small-signal security labels are generated using the MATLAB R2024b-based Power System Toolbox (PST), in which power flow calculations and conventional eigenvalue analyses are performed. All learning-based models, including the proposed EE-GAT, are implemented and trained using the PyTorch 2.2 framework. repeated power flow calculation

During dataset generation, the active power outputs of generators and the active and reactive power demands of loads are independently perturbed within 70–130% of their respective base case values to construct diverse operating conditions. For each generated operating condition, $N-1$ line outage contingencies are sequentially applied to the considered transmission lines. Power flow calculations and small-signal stability analyses are then performed for the resulting post-contingency operating states. The security label of each graph sample is assigned according to the damping ratio criterion defined in Equation (6), with the minimum damping ratio threshold set to $\zeta_{\min}^{\text{th}} = 3\%$. A sample is classified as secure when all critical oscillatory modes satisfy the prescribed damping requirement; otherwise, it is classified as insecure.

The bus and branch operating quantities used as model inputs are obtained from converged power flow calculations, while the corresponding security labels are generated through conventional eigenvalue analysis. Only scenarios for which the power flow converges and a valid pre-contingency or post-contingency equilibrium can be obtained are retained. Cases involving power flow non-convergence, loss of equilibrium, or severe operating limit violations are excluded because they fall outside of the local small-signal assessment domain considered in this study.

After data screening, 7360 valid graph samples were retained for the New England 39-bus system, of which 63.4% were labeled as secure. For the NPCC 140-bus system, 6420 valid graph samples were retained, with secure samples accounting for 42.8%. To mitigate the effects of random data partitioning and model initialization, all experiments were independently repeated five times using different random seeds. In each run, the dataset was stratified into training, validation, and test sets at a ratio of 70%, 15%, and 15%, respectively, and the mean and standard deviation of the five test results were reported. The Adam optimizer [26] was employed with a learning rate of 0.0001 and a batch size of 128.

4.2. Evaluation Metrics

Accuracy (Acc), precision (Pre), recall (Rec), F1-score (F1), and specificity (Sp) are adopted as evaluation metrics to assess the classification performance of different models.

Accuracy measures the proportion of correctly classified samples among all samples and is defined as

$$\text{Acc} = \frac{TP + TN}{TP + TN + FP + FN}. \quad (28)$$

Precision measures the proportion of actually secure samples among the samples predicted as secure and is defined as

$$\text{Pre} = \frac{TP}{TP + FP}. \quad (29)$$

Recall measures the ability of the model to correctly identify actually secure samples and is defined as

$$\text{Rec} = \frac{TP}{TP + FN}. \quad (30)$$

The F1-score jointly considers precision and recall and is defined as

$$\text{F1} = \frac{2 \cdot \text{Pre} \cdot \text{Rec}}{\text{Pre} + \text{Rec}}. \quad (31)$$

Specificity measures the ability of the model to correctly identify actually insecure samples and is defined as

$$\text{Sp} = \frac{TN}{TN + FP}. \quad (32)$$

Here, true positive TP denotes the number of secure samples correctly predicted as secure, true negative TN denotes the number of insecure samples correctly predicted as insecure, false positive FP denotes the number of insecure samples incorrectly predicted as secure, and false negative FN denotes the number of secure samples incorrectly predicted as insecure.

4.3. Analysis on the New England 39-Bus System

The New England 39-bus system contains 39 buses and 10 generators. Although the system's scale is relatively small, it includes typical multi-machine interconnection structures and inter-area power exchange characteristics, making it suitable for preliminarily validating the capability of EE-GAT to identify small-signal security boundaries.

4.3.1. Interpretability Analysis of Attention Weights

To further analyze the physical interpretability of EE-GAT, the edge attention weights α_{ij} and node pooling weights β_i learned by the model on the New England 39-bus system are visualized. Node color intensity represents the magnitude of bus pooling weights, while line thickness represents the magnitude of edge attention weights. Figure 4 shows the attention weight distribution under a typical operating condition.

Figure 4 shows the node pooling and edge attention weights for a representative operating condition in the New England 39-bus system. The nonuniform distribution indicates that EE-GAT adaptively assigns different contributions to buses and branches according to the current operating features and network connectivity. Edge attention weights reflect the relative importance of branch information during neighborhood aggregation, whereas node pooling weights indicate the contributions of learned bus representations to graph-level classification.

These weights are sample-dependent and jointly influenced by node features, branch states, topology, and multi-layer message passing; therefore, they do not correspond directly to any single physical quantity. A high edge attention weight does not necessarily indicate the most heavily loaded branch, nor does a high node pooling weight necessarily coincide with modal participation factors or eigenvalue sensitivities. Moreover, because the input

represents the pre-contingency operating condition while the label is determined from $N-1$ security analysis, the attention map cannot identify the specific outage causing insecurity. Thus, Figure 4 provides only an auxiliary visualization of the information emphasized by EE-GAT rather than a direct causal or physical sensitivity explanation.

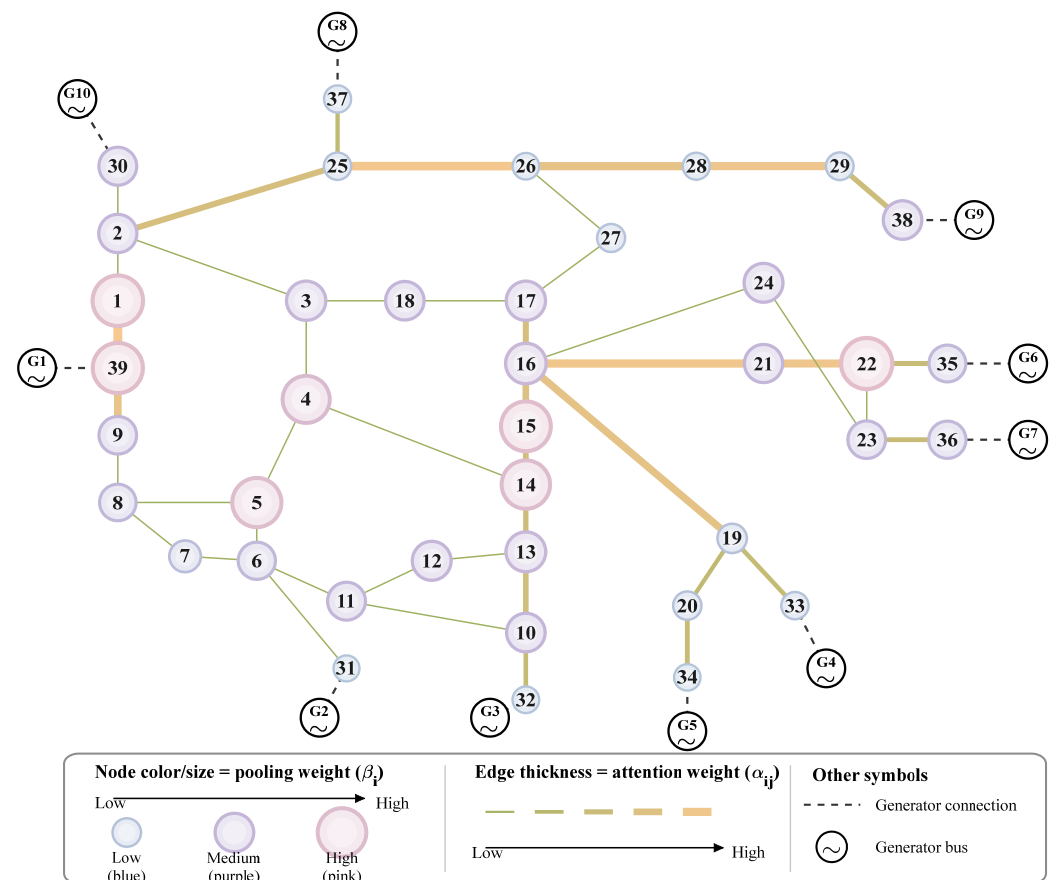


Figure 4. Node pooling and edge attention weights learned by EE-GAT for a representative operating condition in the New England 39-bus system.

4.3.2. Ablation Experiments

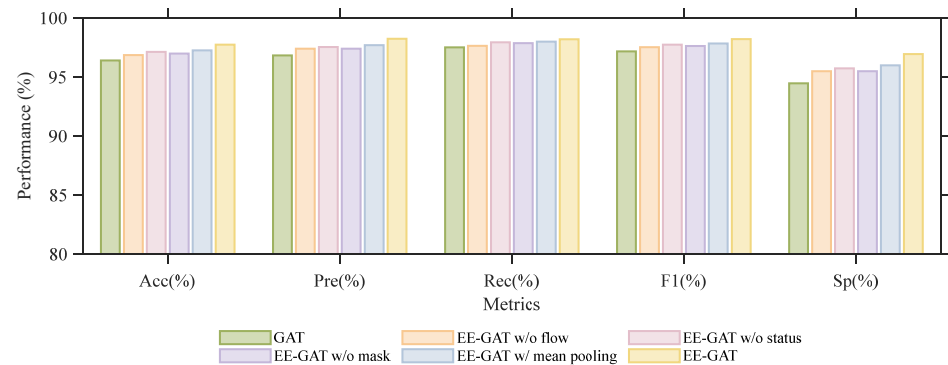
To further verify the effectiveness of different components of EE-GAT, ablation experiments are conducted on the New England 39-bus system. The compared variants include EE-GAT without edge power flow features, EE-GAT without line status features, EE-GAT without PMU masks, EE-GAT using mean pooling instead of global attention pooling, and the full EE-GAT model.

As shown in Table 1 and Figure 5, the complete EE-GAT model achieves the best performance across all evaluation metrics, confirming the effectiveness of the proposed edge-enhanced architecture. Compared with the standard GAT, EE-GAT improves accuracy and specificity by 1.34 and 2.47 percentage points, respectively, indicating that edge information helps the model capture branch power flow redistribution and topology changes under line outages. When branch power flow features or line status features are removed, the model's performance decreases, especially in accuracy and specificity, which demonstrates the importance of active/reactive power flows and topology status in identifying the small-signal security boundary. In addition, removing the PMU mask or replacing global attention pooling with mean pooling also leads to performance degradation, further verifying that missing measurement indicators and attention-based global pooling contribute to the identification of critical buses and key transmission branches.

Table 1. Ablation results of EE-GAT on the New England 39-Bus System.

Model Variant	Acc (%)	Pre (%)	Rec (%)	F1 (%)	Sp (%)
GAT	96.41 ± 0.20	96.84 ± 0.16	97.52 ± 0.17	97.18 ± 0.16	94.48 ± 0.27
EE-GAT w/o flow	96.86 ± 0.20	97.41 ± 0.15	97.65 ± 0.17	97.53 ± 0.16	95.50 ± 0.26
EE-GAT w/o status	97.14 ± 0.19	97.55 ± 0.15	97.95 ± 0.15	97.75 ± 0.15	95.74 ± 0.26
EE-GAT w/o mask	97.00 ± 0.19	97.41 ± 0.14	97.87 ± 0.16	97.64 ± 0.15	95.50 ± 0.24
EE-GAT w/mean pooling	97.27 ± 0.18	97.70 ± 0.13	98.01 ± 0.15	97.85 ± 0.14	96.00 ± 0.23
EE-GAT	97.75 ± 0.17	98.24 ± 0.13	98.21 ± 0.14	98.22 ± 0.13	96.95 ± 0.22

Note: Values are reported as mean ± standard deviation over five independent runs; bold indicates the best result for each metric.

**Figure 5.** Performance comparison of EE-GAT ablation variants on the New England 39-bus system.

4.3.3. Comparative Experiments

Table 2 and Figure 6 present the small-signal security assessment performance of different methods on the New England 39-bus system. XGBoost and LSTM are used as conventional machine learning and sequence learning baselines, respectively. CNN constructs the system operating state as a two-dimensional feature matrix for classification, while GCN performs neighborhood aggregation according to the grid topology. Standard GAT further introduces attention weights among neighboring buses but computes attention only from node features. In contrast, the proposed EE-GAT incorporates branch active power flow, reactive power flow, and line operating status into the attention mechanism, enabling the model to better capture the coupling between bus operating states and transmission line conditions.

Table 2. Comparative results of different methods on the New England 39-bus system.

Model Variant	Acc (%)	Pre (%)	Rec (%)	F1 (%)	Sp (%)
XGBoost	93.54 ± 0.38	94.17 ± 0.25	95.74 ± 0.37	94.95 ± 0.30	89.74 ± 0.44
LSTM	93.38 ± 0.29	94.40 ± 0.19	95.21 ± 0.30	94.80 ± 0.23	90.22 ± 0.32
CNN	94.35 ± 0.32	94.93 ± 0.22	96.22 ± 0.29	95.57 ± 0.25	91.11 ± 0.38
GCN	95.66 ± 0.24	96.38 ± 0.19	96.79 ± 0.20	96.59 ± 0.19	93.70 ± 0.33
GAT	96.41 ± 0.20	96.84 ± 0.16	97.52 ± 0.17	97.18 ± 0.16	94.48 ± 0.27
EE-GAT	97.75 ± 0.17	98.24 ± 0.13	98.21 ± 0.14	98.22 ± 0.13	96.95 ± 0.22

Note: Values are reported as mean ± standard deviation over five independent runs; bold indicates the best result for each metric.

As shown in Table 2 and Figure 6, EE-GAT achieves the best results across all metrics, with an accuracy of 97.75% ± 0.17%, precision of 98.24% ± 0.13%, recall of 98.21% ± 0.14%, an F1-score of 98.22% ± 0.13%, and specificity of 96.95% ± 0.22%. Compared to CNN, GCN, and standard GAT, the accuracy of EE-GAT is improved by 3.40, 2.09, and 1.34 percentage points, respectively. Its specificity is also higher than that of CNN, GCN, and

GAT by 5.84, 3.25, and 2.47 percentage points, respectively, indicating that EE-GAT is more effective in identifying insecure operating states and reducing the risk of misclassifying insecure samples as secure. Compared with XGBoost and LSTM, the graph-based methods generally achieve better performance, which demonstrates the importance of topology information in small-signal security assessment. The superior performance of EE-GAT further demonstrates that branch power flow and line status information provide valuable discriminative features for identifying the small-signal security boundary.

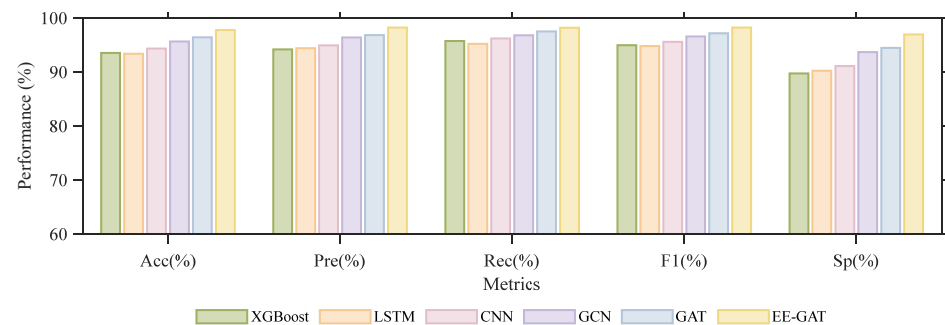


Figure 6. Performance comparison of different methods for small-signal security assessment on the New England 39-bus system.

4.3.4. Robustness Analysis Under Missing PMU Data

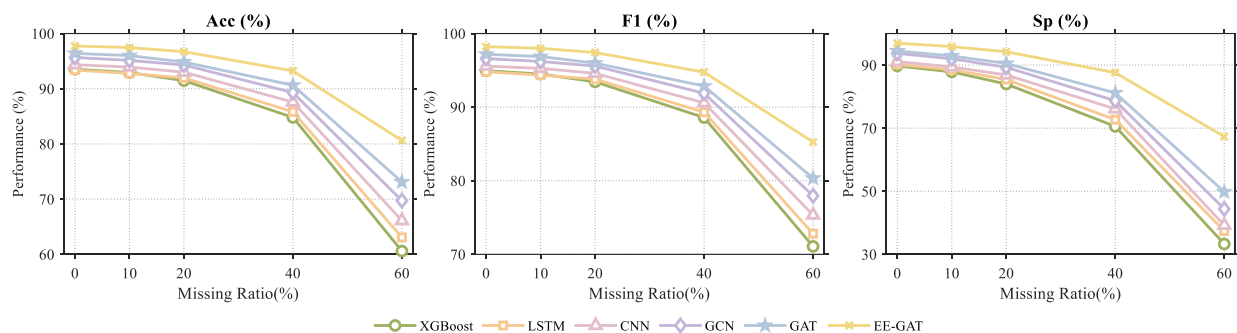
To verify the robustness of the proposed model under incomplete measurement conditions, different missing PMU data ratios are considered on the New England 39-bus system, and the classification performance of XGBoost, LSTM, CNN, GCN, GAT, and EE-GAT is compared. The missing PMU data ratios are set to 0%, 10%, 20%, 40%, and 60%, where 0% represents the complete measurement condition. For buses with missing measurements, the voltage magnitude, voltage phase angle, nodal active power injection, and nodal reactive power injection are filled with zeros, while the corresponding PMU mask is set to zero to explicitly indicate missing bus measurements. For buses with available measurements, the PMU mask is set to 1.

As shown in Table 3 and Figure 7, the classification performance of all models decreases as the missing PMU data ratio increases, while EE-GAT consistently achieves the best results under all missing data conditions. When the missing ratio increases from 0% to 20%, the accuracy, F1-score, and specificity of EE-GAT decrease only from $97.75\% \pm 0.17\%$, $98.22\% \pm 0.13\%$, and $96.95\% \pm 0.22\%$ to $96.71\% \pm 0.74\%$, $97.42\% \pm 0.57\%$, and $94.22\% \pm 1.18\%$, respectively, indicating that the proposed model maintains stable classification performance under moderate PMU data loss. When the missing ratio further increases to 40% and 60%, all models exhibit more pronounced performance degradation and larger standard deviations, especially in specificity, suggesting that severe measurement loss weakens their ability to identify insecure operating states. Under the 60% missing data condition, the specificity values of CNN, GCN, and GAT decrease to $39.23\% \pm 6.81\%$, $44.39\% \pm 6.49\%$, and $49.81\% \pm 6.41\%$, respectively, whereas EE-GAT still maintains a specificity of $67.33\% \pm 5.65\%$. Meanwhile, the accuracy and F1-score of EE-GAT remain at $80.62\% \pm 3.46\%$ and $85.26\% \pm 2.56\%$, respectively, which are higher than those of all compared models. These results demonstrate that the PMU mask helps the model distinguish actual measurements from filled missing values, while the edge-enhanced attention mechanism further utilizes branch power flow and line status information to compensate for partial node measurement loss, thereby improving robustness and insecure sample identification capability under high missing PMU data ratios.

Table 3. Robustness comparison under different missing PMU data ratios on the New England 39-bus system.

Metric	Model	0%	10%	20%	40%	60%
Acc (%)	XGBoost	93.54 ± 0.38	92.93 ± 0.48	91.47 ± 1.05	84.80 ± 2.26	60.59 ± 4.94
	LSTM	93.38 ± 0.29	92.77 ± 0.45	91.97 ± 1.00	85.82 ± 2.15	63.07 ± 4.70
	CNN	94.35 ± 0.32	93.92 ± 0.41	93.00 ± 0.91	87.58 ± 1.96	66.11 ± 4.33
	GCN	95.66 ± 0.24	95.14 ± 0.38	94.30 ± 0.83	89.30 ± 1.80	69.73 ± 3.98
	GAT	96.41 ± 0.20	96.00 ± 0.38	94.83 ± 0.84	90.63 ± 1.80	73.11 ± 3.93
	EE-GAT	97.75 ± 0.17	97.45 ± 0.34	96.71 ± 0.74	93.23 ± 1.58	80.62 ± 3.46
F1 (%)	XGBoost	94.95 ± 0.30	94.50 ± 0.37	93.44 ± 0.80	88.58 ± 1.67	71.08 ± 3.45
	LSTM	94.80 ± 0.23	94.35 ± 0.35	93.80 ± 0.76	89.31 ± 1.59	72.80 ± 3.29
	CNN	95.57 ± 0.25	95.27 ± 0.32	94.59 ± 0.70	90.58 ± 1.47	75.34 ± 3.03
	GCN	96.59 ± 0.19	96.20 ± 0.30	95.58 ± 0.64	91.88 ± 1.34	77.95 ± 2.77
	GAT	97.18 ± 0.16	96.87 ± 0.30	95.98 ± 0.65	92.86 ± 1.35	80.34 ± 2.76
	EE-GAT	98.22 ± 0.13	97.99 ± 0.26	97.42 ± 0.57	94.75 ± 1.21	85.26 ± 2.56
Sp (%)	XGBoost	89.74 ± 0.44	87.85 ± 0.75	83.99 ± 1.62	70.56 ± 3.50	33.29 ± 7.82
	LSTM	90.22 ± 0.32	88.52 ± 0.71	85.44 ± 1.56	72.71 ± 3.37	37.43 ± 7.54
	CNN	91.11 ± 0.38	89.41 ± 0.63	86.88 ± 1.39	76.11 ± 3.01	39.23 ± 6.81
	GCN	93.70 ± 0.33	92.00 ± 0.62	89.29 ± 1.33	78.69 ± 2.88	44.39 ± 6.49
	GAT	94.48 ± 0.27	92.89 ± 0.62	90.51 ± 1.35	81.17 ± 2.89	49.81 ± 6.41
	EE-GAT	96.95 ± 0.22	95.86 ± 0.55	94.22 ± 1.18	87.59 ± 2.54	67.33 ± 5.65

Note: Values are reported as mean ± standard deviation over five independent runs; bold indicates the best result for each metric.

**Figure 7.** Classification performance under different missing PMU data ratios on the New England 39-bus system.

4.4. Analysis on the NPCC 140-Bus System

To further verify the applicability of the proposed method to larger-scale power systems, tests are conducted on the NPCC 140-bus system. The NPCC 140-bus system contains 140 buses and 48 generators, with a larger network scale, more complex topology, richer power flow distributions, and more prominent inter-area oscillation characteristics. Therefore, it is suitable for evaluating the modeling capability and generalization performance of EE-GAT on larger-scale graph-structured data.

4.4.1. Interpretability Analysis of Attention Weights

Figure 8 shows the attention weight distribution learned by EE-GAT on the NPCC 140-bus system. Node color intensity represents the magnitude of bus pooling weights, while line thickness represents the magnitude of edge attention weights.

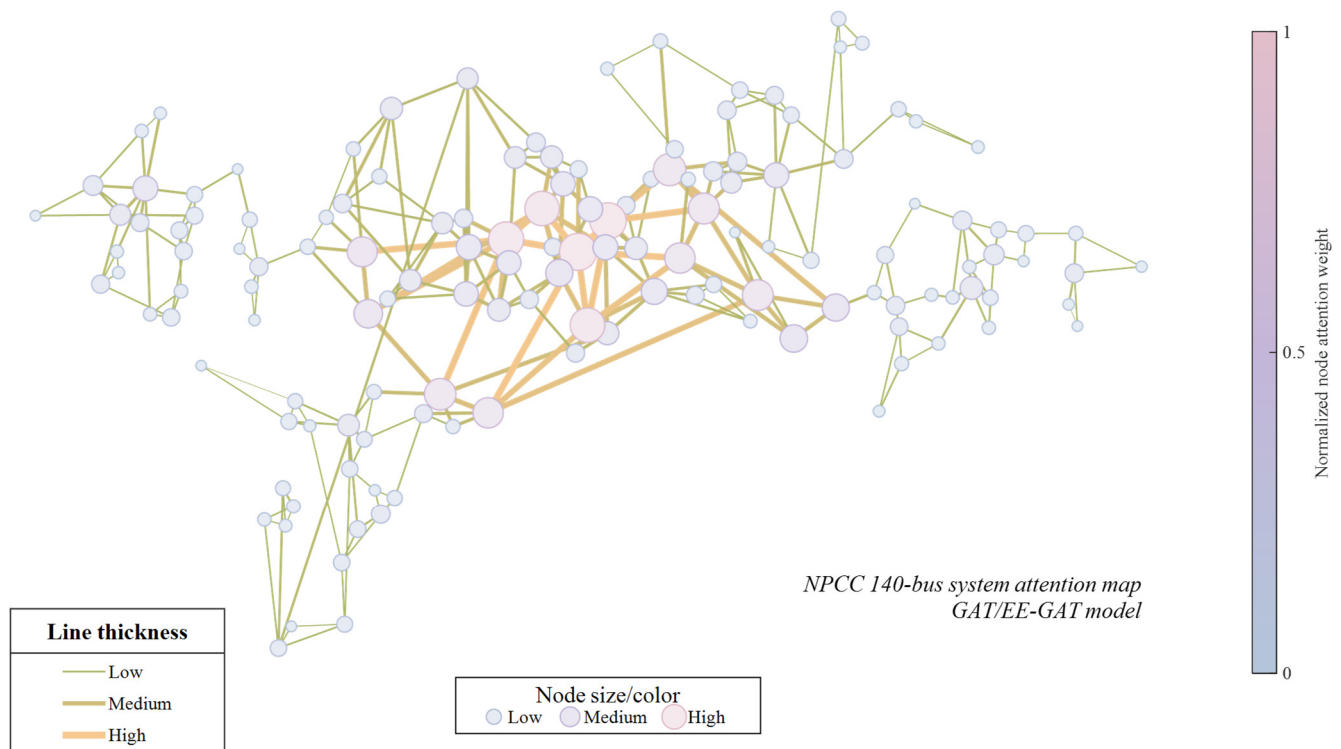


Figure 8. Node pooling and edge attention weights learned by EE-GAT for a representative operating condition in the NPCC 140-bus system.

Figure 8 shows the attention weight distribution for a representative operating condition in the NPCC 140-bus system. Compared with the New England 39-bus system, the weights are distributed over a larger and more complex network, with only a subset of buses and branches receiving relatively high values. This indicates that EE-GAT selectively emphasizes different parts of the graph rather than assigning uniform importance to all components.

These weights are sample-dependent internal coefficients jointly influenced by node states, branch features, network topology, and multi-layer message passing. Therefore, they should not be interpreted as fixed rankings of critical buses or transmission corridors, nor are they expected to coincide directly with branch loading, contingency severity, eigenvalue sensitivity, or modal participation factors. Because the visualized attention map corresponds to the pre-contingency operating condition, it cannot identify the specific $N-1$ outage responsible for an insecure label or describe the associated post-contingency behavior. Figure 8 therefore provides only auxiliary information on the graph components emphasized by EE-GAT, while rigorous physical diagnosis still requires conventional eigenvalue, participation factor, or sensitivity analysis.

4.4.2. Ablation Experiments

To verify the role of the edge-enhanced mechanism in a larger-scale system, ablation experiments are further conducted on the NPCC 140-bus system. Table 4 and Figure 9 present the test results of different model variants.

As shown in Table 4 and Figure 9, the complete EE-GAT model achieves the best performance across all evaluation metrics on the NPCC 140-bus system, with an accuracy of $96.47\% \pm 0.25\%$, precision of $93.57\% \pm 0.47\%$, recall of $98.53\% \pm 0.27\%$, an F1-score of $95.99\% \pm 0.28\%$, and specificity of $94.93\% \pm 0.40\%$. Compared with the standard GAT, EE-GAT improves accuracy and specificity by 1.34 and 1.91 percentage points, respectively, indicating that the edge-enhanced mechanism helps the model capture complex network

topology and branch power flow redistribution more effectively. When the branch power flow features are removed, the accuracy decreases to $95.54\% \pm 0.25\%$, showing that active and reactive power flows provide useful discriminative information for identifying the small-signal security boundary. When the line status feature is removed, the specificity decreases to $93.95\% \pm 0.42\%$, demonstrating the importance of explicit topology information for recognizing insecure samples under $N-1$ contingency conditions. In addition, removing the PMU mask reduces the accuracy and specificity to $95.68\% \pm 0.24\%$ and $93.77\% \pm 0.42\%$, respectively, while replacing global attention pooling with mean pooling reduces them to $96.06\% \pm 0.27\%$ and $94.29\% \pm 0.45\%$. These results further confirm that missing measurement indicators and attention-based global pooling contribute to robust small-signal security assessment in larger-scale power systems.

Table 4. Ablation results of EE-GAT on the NPCC 140-Bus System.

Model Variant	Acc (%)	Pre (%)	Rec (%)	F1 (%)	Sp (%)
GAT	95.13 ± 0.28	91.31 ± 0.52	97.95 ± 0.27	94.52 ± 0.30	93.02 ± 0.46
EE-GAT w/o flow	95.54 ± 0.25	91.98 ± 0.46	98.14 ± 0.26	94.96 ± 0.28	93.59 ± 0.40
EE-GAT w/o status	95.82 ± 0.25	92.41 ± 0.48	98.32 ± 0.26	95.27 ± 0.27	93.95 ± 0.42
EE-GAT w/o mask	95.68 ± 0.24	92.19 ± 0.48	98.22 ± 0.27	95.11 ± 0.27	93.77 ± 0.42
EE-GAT w/mean pooling	96.06 ± 0.27	92.81 ± 0.53	98.42 ± 0.28	95.53 ± 0.30	94.29 ± 0.45
EE-GAT	96.47 ± 0.25	93.57 ± 0.47	98.53 ± 0.27	95.99 ± 0.28	94.93 ± 0.40

Note: Values are reported as mean $\pm$ standard deviation over five independent runs; bold indicates the best result for each metric.

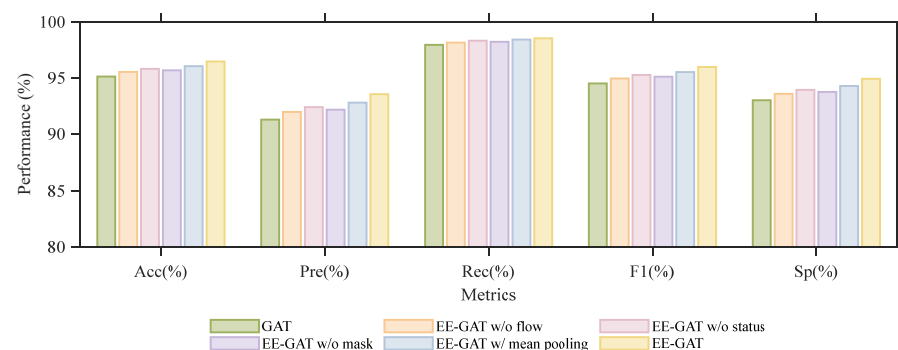


Figure 9. Performance comparison of EE-GAT ablation variants on the NPCC 140-bus system.

4.4.3. Comparative Experiments

Table 5 and Figure 10 present the small-signal security assessment results of different methods on the NPCC 140-bus system. Compared with the New England 39-bus system, the NPCC 140-bus system has a larger network scale, more complex topological connections, richer branch power flow distributions, and more complicated inter-area oscillation characteristics, which place higher demands on the feature extraction and topology modeling capabilities of different methods.

As shown in Table 5 and Figure 10, XGBoost, LSTM, and CNN achieve relatively lower performance because they cannot fully represent the graph-topological coupling characteristics of large-scale power grids. By incorporating grid topology, GCN improves the accuracy to $94.31\% \pm 0.26\%$, while GAT further increases the accuracy to $95.13\% \pm 0.28\%$ by adaptively assigning attention weights to neighboring buses. The proposed EE-GAT achieves the best performance across all evaluation metrics, with an accuracy of $96.47\% \pm 0.25\%$, precision of $93.57\% \pm 0.47\%$, recall of $98.53\% \pm 0.27\%$, an F1-score of $95.99\% \pm 0.28\%$, and specificity of $94.93\% \pm 0.40\%$. Compared with standard GAT, EE-GAT improves accuracy, precision, recall, F1-score, and specificity by 1.34, 2.26,

0.58, 1.47, and 1.91 percentage points, respectively. These results indicate that incorporating branch active power flow, reactive power flow, and line operating status into the attention mechanism enables EE-GAT to better capture branch power flow redistribution and topology variations, thereby improving the identification of small-signal security boundaries in larger-scale power systems.

Table 5. Comparative results of different methods on the NPCC 140-bus system.

Model Variant	Acc (%)	Pre (%)	Rec (%)	F1 (%)	Sp (%)
XGBoost	91.89 ± 0.20	86.21 ± 0.53	96.48 ± 0.53	91.06 ± 0.20	88.45 ± 0.57
LSTM	92.59 ± 0.22	87.28 ± 0.36	96.79 ± 0.31	91.79 ± 0.23	89.44 ± 0.35
CNN	93.14 ± 0.24	88.15 ± 0.43	97.02 ± 0.31	92.37 ± 0.25	90.24 ± 0.40
GCN	94.31 ± 0.26	89.82 ± 0.45	97.78 ± 0.28	93.63 ± 0.28	91.70 ± 0.40
GAT	95.13 ± 0.28	91.31 ± 0.52	97.95 ± 0.27	94.52 ± 0.30	93.02 ± 0.46
EE-GAT	96.47 ± 0.25	93.57 ± 0.47	98.53 ± 0.27	95.99 ± 0.28	94.93 ± 0.40

Note: Values are reported as mean ± standard deviation over five independent runs; bold indicates the best result for each metric.

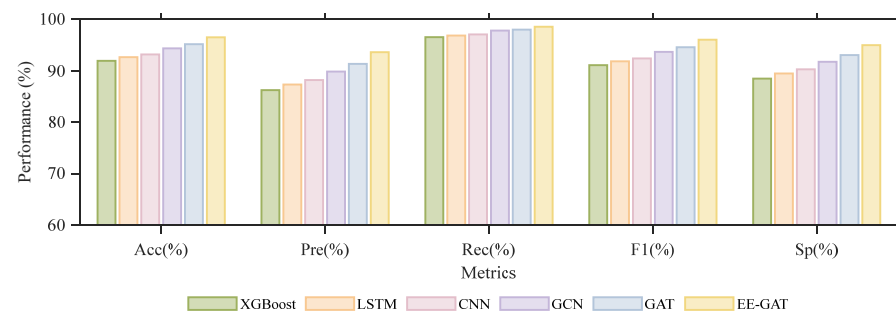


Figure 10. Performance comparison of different methods for small-signal security assessment on the NPCC 140-bus system.

4.4.4. Robustness Analysis Under Missing PMU Data

To verify the adaptability of the proposed EE-GAT under incomplete measurement conditions in larger-scale systems, missing PMU data ratios of 0%, 10%, 20%, 40%, and 60% are set on the NPCC 140-bus system. The classification performance of XGBoost, LSTM, CNN, GCN, GAT, and EE-GAT is compared under different missing data scenarios.

As shown in Table 6 and Figure 11, the classification performance of all models decreases as the missing PMU data ratio increases, and degradation is more pronounced than that observed on the New England 39-bus system. EE-GAT consistently achieves the best performance under all missing data ratios. When the missing ratio increases from 0% to 20%, the accuracy, F1-score, and specificity of EE-GAT decrease from 96.47% ± 0.25%, 95.99% ± 0.28%, and 94.93% ± 0.40% to 94.56% ± 0.62%, 93.99% ± 0.64%, and 91.01% ± 1.12%, respectively, indicating that the proposed model can still maintain relatively stable performance under moderate PMU data loss. When the missing ratio further increases to 60%, all models suffer significant performance degradation, especially in specificity. Under this condition, the specificity values of CNN, GCN, and GAT decrease to 30.96% ± 7.04%, 35.68% ± 6.22%, and 40.22% ± 5.73%, respectively, whereas EE-GAT still maintains greater specificity of 57.35% ± 5.30%. Meanwhile, the accuracy and F1-score of EE-GAT remain at 72.38% ± 3.22% and 74.17% ± 2.48%, respectively, which are also higher than those of all compared methods. These results indicate that missing PMU measurements have a stronger impact on larger-scale systems, particularly on the identification of insecure operating states. By incorporating PMU masks, branch power flow features, and line operating status, EE-GAT can better exploit edge-side information and topology states

when node measurements are incomplete, thereby improving robustness and reducing the risk of misclassifying insecure states as secure under high missing data ratios.

Table 6. Robustness comparison under different missing PMU data ratios on the NPCC 140-Bus System.

Metric	Model	0%	10%	20%	40%	60%
Acc (%)	XGBoost	91.89 ± 0.20	90.72 ± 0.62	88.41 ± 1.28	77.94 ± 2.82	50.86 ± 6.20
	LSTM	92.59 ± 0.22	91.46 ± 0.53	89.35 ± 1.11	79.53 ± 2.45	53.64 ± 5.46
	CNN	93.14 ± 0.24	92.27 ± 0.47	90.51 ± 0.98	82.66 ± 2.12	56.95 ± 4.78
	GCN	94.31 ± 0.26	93.61 ± 0.39	91.71 ± 0.84	84.89 ± 1.81	60.76 ± 4.20
	GAT	95.13 ± 0.28	94.17 ± 0.35	92.83 ± 0.73	86.54 ± 1.58	64.31 ± 3.74
	EE-GAT	96.47 ± 0.25	95.84 ± 0.29	94.56 ± 0.62	90.19 ± 1.35	72.38 ± 3.22
F1 (%)	XGBoost	91.06 ± 0.20	90.08 ± 0.60	87.95 ± 1.19	79.12 ± 2.36	59.92 ± 4.72
	LSTM	91.79 ± 0.23	90.80 ± 0.53	88.81 ± 1.05	80.35 ± 2.10	62.05 ± 4.16
	CNN	92.37 ± 0.25	91.59 ± 0.48	89.93 ± 0.94	82.87 ± 1.83	64.58 ± 3.67
	GCN	93.63 ± 0.28	93.02 ± 0.40	91.11 ± 0.82	84.78 ± 1.60	67.30 ± 3.26
	GAT	94.52 ± 0.30	93.56 ± 0.36	92.22 ± 0.73	86.24 ± 1.42	69.85 ± 2.89
	EE-GAT	95.99 ± 0.28	95.32 ± 0.31	93.99 ± 0.64	89.61 ± 1.26	74.17 ± 2.48
Sp (%)	XGBoost	88.45 ± 0.57	84.97 ± 0.99	80.69 ± 2.11	63.34 ± 4.72	24.70 ± 9.10
	LSTM	89.44 ± 0.35	86.27 ± 0.86	82.33 ± 1.83	65.99 ± 4.09	27.53 ± 8.01
	CNN	90.24 ± 0.40	87.75 ± 0.73	84.23 ± 1.62	71.32 ± 3.57	30.96 ± 7.04
	GCN	91.70 ± 0.40	89.27 ± 0.65	86.19 ± 1.42	74.95 ± 3.14	35.68 ± 6.22
	GAT	93.02 ± 0.46	90.74 ± 0.59	88.15 ± 1.27	77.70 ± 2.82	40.22 ± 5.73
	EE-GAT	94.93 ± 0.40	93.49 ± 0.53	91.01 ± 1.12	83.80 ± 2.50	57.35 ± 5.30

Note: Values are reported as mean ± standard deviation over five independent runs; bold indicates the best result for each metric.

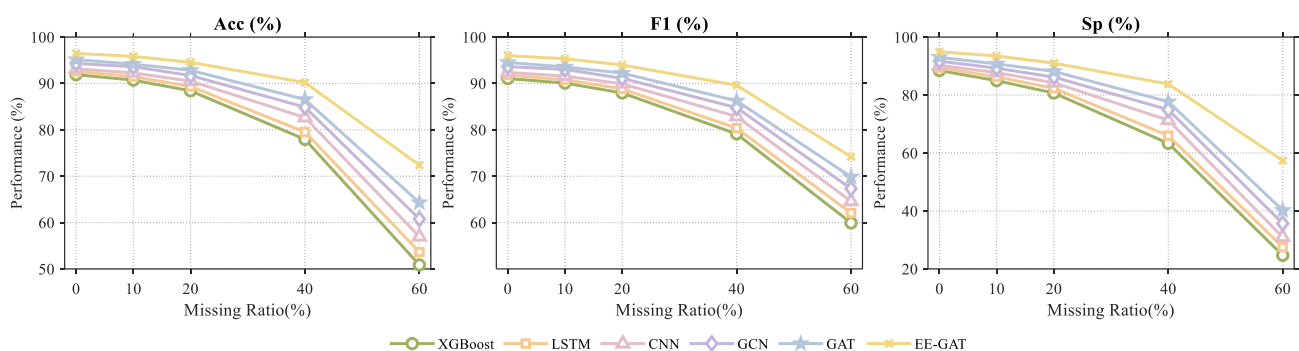


Figure 11. Classification performance variation under different missing PMU data ratios on the NPCC 140-bus system.

4.5. Online Efficiency Analysis

To verify the online efficiency of the proposed EE-GAT model, the average execution times of the conventional $N-1$ small-signal stability analysis method, XGBoost, LSTM, CNN, GCN, GAT, and EE-GAT are compared on the New England 39-bus system and the NPCC 140-bus system. All computational experiments are conducted on the same hardware platform equipped with an Intel Core i9 CPU and an NVIDIA GeForce RTX 3060 GPU. For the conventional method, the execution time includes power flow calculation, system linearization, and eigenvalue analysis for the test samples and their corresponding contingency sets, resulting in a heavy computational burden. For the learning-based methods, the execution time refers to the total model inference time required for the same test batch in the online stage. The execution times of different methods and their speedup ratios relative to the conventional method are listed in Table 7.

Table 7. Online efficiency comparison of different methods on the New England 39-bus and NPCC 140-bus systems.

Test System	Metric	Conventional	XGBoost	LSTM	CNN	GCN	GAT	EE-GAT
New England 39	Execution time	61.72 s	0.100 s	0.022 s	0.015 s	0.0025 s	0.0029 s	0.0034 s
	Speedup ratio	1×	617×	2805×	4115×	24,688×	21,283×	18,153×
NPCC 140	Execution time	594.79 s	0.240 s	0.052 s	0.033 s	0.0038 s	0.0043 s	0.0051 s
	Speedup ratio	1×	2478×	11,438×	18,024×	156,524×	138,323×	116,625×

As shown in Table 7, the conventional $N-1$ small-signal stability analysis method requires significantly longer computation time than the learning-based methods. For a single operating condition, the conventional small-signal stability analysis takes approximately 1.3–1.4 s on the New England 39-bus system and 2.5–2.6 s on the NPCC 140-bus system. When the full $N-1$ contingency set is considered, the total execution time further increases to 61.72 s and 594.79 s, respectively. This indicates that the conventional eigenvalue-based method involves a considerable computational burden and is difficult to apply to real-time online assessment, particularly for large-scale power systems with multiple contingency scenarios. In comparison, the proposed EE-GAT completes the same test batch evaluation in only 0.0034 s and 0.0051 s on the two systems, achieving speedup ratios of approximately 18,153× and 116,625×, respectively. This high inference efficiency is mainly attributed to the sparse message passing mechanism of graph neural networks, which enables information aggregation directly along the physical topology of the power grid. Although EE-GAT further incorporates edge features and line status information into the attention mechanism, the additional computational cost remains limited. These results show that EE-GAT can substantially improve the online assessment efficiency of small-signal stability while preserving the capability to model branch-level features and perceive topology variations under $N-1$ contingency conditions.

5. Discussion

The proposed EE-GAT is intended for real-time pre-contingency small-signal security screening of transmission systems for which the current network topology, bus operating quantities, branch power flows, and at least partial PMU or state estimation measurements are available. For each current operating condition, the model uses pre-contingency graph features to predict whether the system satisfies the prescribed small-signal security criterion under the considered $N-1$ contingencies. It is therefore particularly suitable for rapidly screening a large number of operating conditions before detailed physics-based analysis. The model is intended as a decision support tool rather than a replacement for conventional modal analysis when critical eigenvalues, damping ratios, oscillation frequencies, mode shapes, or participation factors are required.

The applicability of EE-GAT is primarily limited by the operating range and topology space represented in the offline training dataset. Substantial changes in generation composition, control parameters, renewable penetration, or the current network topology may cause data distribution shifts and reduce classification accuracy. Although topology variations represented in the training data can be learned by the graph model, previously unseen or large-scale structural changes may require incremental training, transfer learning, or model retraining. In addition, the present model performs binary security classification and does not directly identify the specific contingency responsible for insecurity or provide detailed modal information. The current validation is also based on simulated benchmark systems, and further evaluation using field measurements is required before large-scale practical deployment.

In the present study, the simulation-generated operating quantities are treated as noise-free reference measurements, and random measurement errors or systematic biases are not explicitly considered. In practical applications, PMU noise, synchronization errors, communication anomalies, and state estimation errors may affect the input features and consequently degrade the reliability of the classification results. These effects should be addressed through online data quality monitoring, bad data detection, measurement filtering, and model recalibration.

Moreover, the statistical distribution of PMU measurements may vary over time because of seasonal and weather-dependent load changes, renewable power fluctuations, topology modifications, and control strategy adjustments. Future work will therefore investigate robustness under different types and levels of measurement uncertainty, validation using long-term field PMU data, and data drift detection mechanisms. Online continual learning and domain adaptation strategies will also be explored to update EE-GAT using newly acquired operating samples while mitigating catastrophic forgetting, thereby improving its long-term adaptability and reliability in practical power system operation.

6. Conclusions

This paper proposed an Edge-Enhanced Graph Attention Network for real-time small-signal security assessment under varying operating conditions and $N-1$ contingencies. The EE-GAT model explicitly incorporates branch active and reactive power flows and line operating status into the attention calculation, enabling the joint representation of nodal operating states, electrical coupling, power flow redistribution, and topology variations. In addition, the PMU availability mask distinguishes missing measurements from actual zero-valued inputs, while the global attention readout mechanism adaptively identifies stability-sensitive buses. These mechanisms make EE-GAT an edge-aware, topology-adaptive, and measurement-robust graph learning framework rather than a straightforward application of a conventional GAT.

Case studies on the New England 39-bus and NPCC 140-bus systems showed that EE-GAT achieved classification accuracies of 97.75% and 96.47%, respectively, outperforming XGBoost, LSTM, CNN, GCN, and standard GAT. The ablation studies, missing-PMU robustness tests, and online efficiency analysis further confirmed the effectiveness of the proposed components. The results demonstrate that EE-GAT can reliably identify insecure operating conditions while substantially reducing the computational burden of conventional $N-1$ small-signal security assessment.

Author Contributions: Conceptualization, W.J., K.L. and J.Z.; methodology, W.J.; software, W.J.; validation, W.J., M.W. and Q.S.; formal analysis, W.J.; investigation, W.J.; resources, K.L. and J.Z.; data curation, W.J.; writing—original draft preparation, W.J.; writing—review and editing, W.J., M.W., Q.S., K.L. and J.Z.; visualization, W.J., M.W. and Q.S.; supervision, K.L. and J.Z.; project administration, K.L. and J.Z.; funding acquisition, K.L. and J.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

SSSA	Small-Signal Security Assessment
EE-GAT	Edge-Enhanced Graph Attention Network
GNN	Graph Neural Network
GAT	Graph Attention Network
GCN	Graph Convolutional Network
CNN	Convolutional Neural Network
LSTM	Long Short-Term Memory
XGBoost	Extreme Gradient Boosting
PMU	Phasor Measurement Unit
PST	Power System Toolbox
DAE	Differential Algebraic Equation
MLP	Multilayer Perceptron
BCE	Binary Cross-Entropy
$N-1$	Single-Contingency Condition
NPCC	Northeast Power Coordinating Council

References

1. Morison, K.; Wang, L.; Kundur, P. Power system security assessment. *IEEE Power Energy Mag.* **2004**, *2*, 30–39. [\[CrossRef\]](#)
2. Kundur, P.; Paserba, J.; Ajarapu, V.; Andersson, G.; Bose, A.; Canizares, C.; Hatziargyriou, N.; Hill, D.; Stankovic, A.; Taylor, C.; et al. Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions. *IEEE Trans. Power Syst.* **2004**, *19*, 1387–1401. [\[CrossRef\]](#)
3. Hatziargyriou, N.; Milanovic, J.V.; Rahmann, C.; Ajarapu, V.; Canizares, C.; Erlich, I.; Hill, D.; Hiskens, I.; Kamwa, I.; Pal, B.; et al. Definition and classification of power system stability revisited and extended. *IEEE Trans. Power Syst.* **2021**, *36*, 3271–3281. [\[CrossRef\]](#)
4. Geeganage, J.; Annakkage, U.D.; Weekes, T.; Archer, B.A. Application of energy-based power system features for dynamic security assessment. *IEEE Trans. Power Syst.* **2015**, *30*, 1957–1965. [\[CrossRef\]](#)
5. Bento, M.E.C.; Ramos, R.A. An approach for monitoring and updating the load margin of power systems in dynamic security assessment. *Electr. Power Syst. Res.* **2021**, *198*, 107363. [\[CrossRef\]](#)
6. Chávez-Lugo, M.; Fuerte-Esquivel, C.R.; Gutiérrez-Martínez, V.J. A direct method for the computation of the oscillatory voltage stability boundary. *Electr. Power Syst. Res.* **2019**, *167*, 163–170. [\[CrossRef\]](#)
7. Vu, T.L.; Chatzivasileiadis, S.; Chiang, H.-D.; Turitsyn, K. Structural emergency control paradigm. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2017**, *7*, 371–382. [\[CrossRef\]](#)
8. Alimi, O.A.; Ouahada, K.; Abu-Mahfouz, A.M. A review of machine learning approaches to power system security and stability. *IEEE Access* **2020**, *8*, 113512–113531. [\[CrossRef\]](#)
9. Kummerow, A.; Monsalve, C.; Brosinsky, C.; Nicolai, S.; Westermann, D. A Novel Framework for Synchrophasor Based Online Recognition and Efficient Post-Mortem Analysis of Disturbances in Power Systems. *Appl. Sci.* **2020**, *10*, 5209. [\[CrossRef\]](#)
10. Wehenkel, L.A. *Automatic Learning Techniques in Power Systems*; Springer Science & Business Media: New York, NY, USA, 2012.
11. Jayasekara, B.; Annakkage, U.D. Derivation of an accurate polynomial representation of the transient stability boundary. *IEEE Trans. Power Syst.* **2006**, *21*, 1856–1863. [\[CrossRef\]](#)
12. Gomez, F.R.; Rajapakse, A.D.; Annakkage, U.D.; Fernando, I.T. Support vector machine-based algorithm for post-fault transient stability status prediction using synchronized measurements. *IEEE Trans. Power Syst.* **2011**, *26*, 1474–1483.
13. Alhamrouni, I.; Abdul Kahar, N.H.; Salem, M.; Swadi, M.; Zahroui, Y.; Kadhim, D.J.; Mohamed, F.A.; Nazari, M.A. A Comprehensive Review on the Role of Artificial Intelligence in Power System Stability, Control, and Protection: Insights and Future Directions. *Appl. Sci.* **2024**, *14*, 6214. [\[CrossRef\]](#)
14. Sun, M.; Konstantelos, I.; Strbac, G. A deep learning-based feature extraction framework for system security assessment. *IEEE Trans. Smart Grid* **2018**, *9*, 5007–5020. [\[CrossRef\]](#)
15. Li, W.; Deka, D.; Chertkov, M.; Wang, M. Real-time faulted line localization and PMU placement in power systems through convolutional neural networks. *IEEE Trans. Power Syst.* **2019**, *34*, 4640–4651. [\[CrossRef\]](#)
16. Mostafanezhad, M.; Mohammadi, M.; Afrasiabi, S.; Afrasiabi, M.; Aghaei, J.; Chung, C.Y. Data-driven small-signal and $N-1$ security assessment considering missing data. *IEEE Trans. Power Syst.* **2024**, *39*, 2587–2597. [\[CrossRef\]](#)

17. Owerko, D.; Gama, F.; Ribeiro, A. Predicting power outages using graph neural networks. In Proceedings of the 2018 IEEE Global Conference on Signal and Information Processing, Anaheim, CA, USA, 26–29 November 2018; pp. 743–747.
18. Dwivedi, A.; Tajer, A. GRNN-based real-time fault chain prediction. *IEEE Trans. Power Syst.* **2024**, *39*, 934–946. [[CrossRef](#)]
19. Zhao, T.; Yue, M.; Wang, J. Structure-informed graph learning of networked dependencies for online prediction of power system transient dynamics. *IEEE Trans. Power Syst.* **2022**, *37*, 4885–4895. [[CrossRef](#)]
20. Zhu, L.; Wen, W.; Li, J.; Hu, Y. Integrated data-driven power system transient stability monitoring and enhancement. *IEEE Trans. Power Syst.* **2024**, *39*, 1797–1809. [[CrossRef](#)]
21. Lu, G.; Bu, S. Adaptive stability contingency screening for operational planning based on domain-adversarial graph neural network. *IEEE Trans. Power Syst.* **2024**, *39*, 1503–1516. [[CrossRef](#)]
22. Su, Y.; Guo, M.; Yao, H.; Guan, L.; Huang, J.; Zhu, S.; Zhong, Z. Power system small-signal stability assessment model based on residual graph convolutional networks. *J. Phys. Conf. Ser.* **2021**, *2095*, 012011. [[CrossRef](#)]
23. Sun, P.; Huo, L.; Chen, X.; Liang, S. Rotor angle stability prediction using temporal and topological embedding deep neural network based on grid-informed adjacency matrix. *J. Mod. Power Syst. Clean Energy* **2024**, *12*, 695–706. [[CrossRef](#)]
24. Justin, G.; Paternain, S. Real-time small-signal security assessment using graph neural networks. *Sustain. Energy Grids Netw.* **2024**, *39*, 101469. [[CrossRef](#)]
25. Veličković, P.; Cucurull, G.; Casanova, A.; Romero, A.; Lio, P.; Bengio, Y. Graph attention networks. In Proceedings of the International Conference on Learning Representations, Vancouver, BC, Canada, 30 April–3 May 2018.
26. Kingma, D.P.; Ba, J. Adam: A method for stochastic optimization. In Proceedings of the 3rd International Conference on Learning Representations (ICLR 2015), San Diego, CA, USA, 7–9 May 2015.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.