SA²GFM

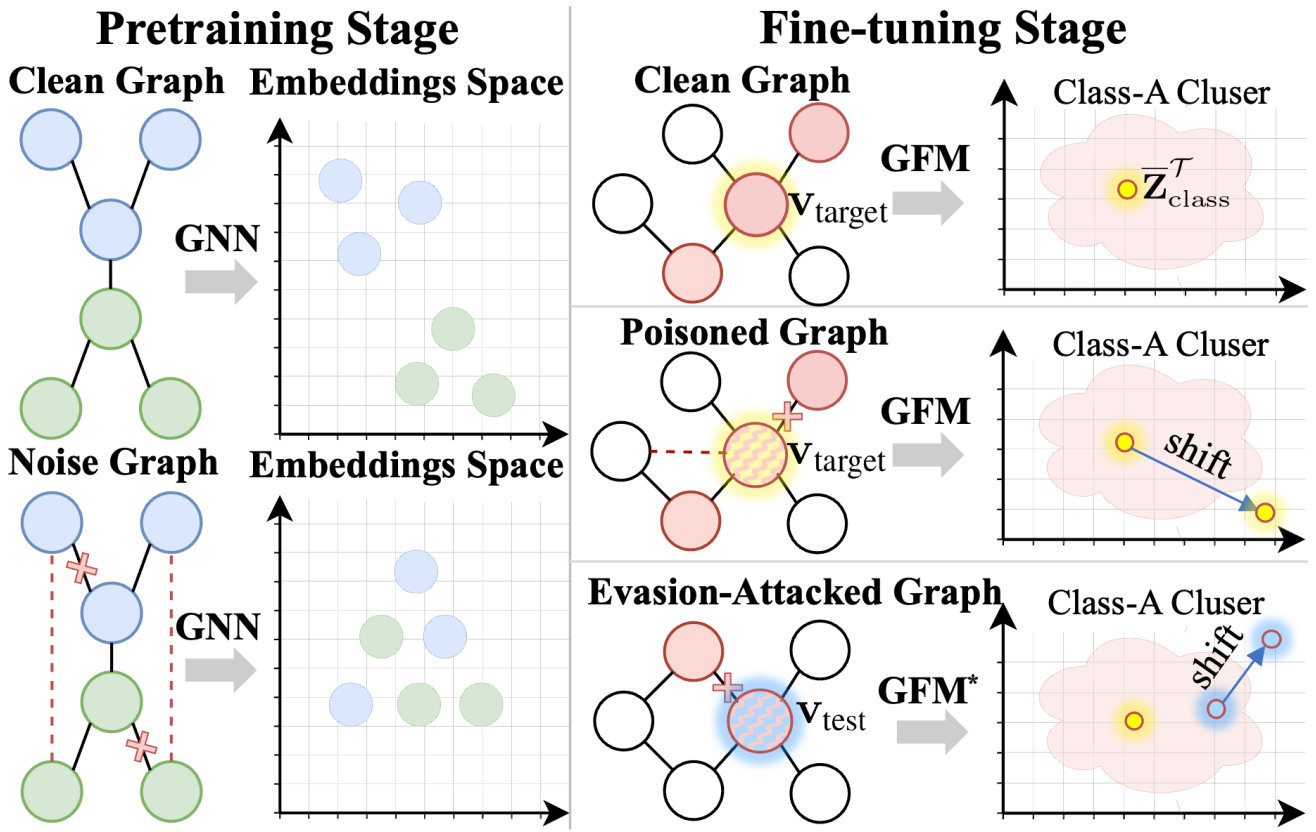
Challenges in Ensuring Robustness of Graph Foundation Models

Architectural bottleneck：

- Insufficient modeling of hierarchical structural semantics.
  - Shallow message-passing GNN backbones.
  - Fail to capture long-range dependencies and higher-level structural semantics.

Deployment Challenges ：

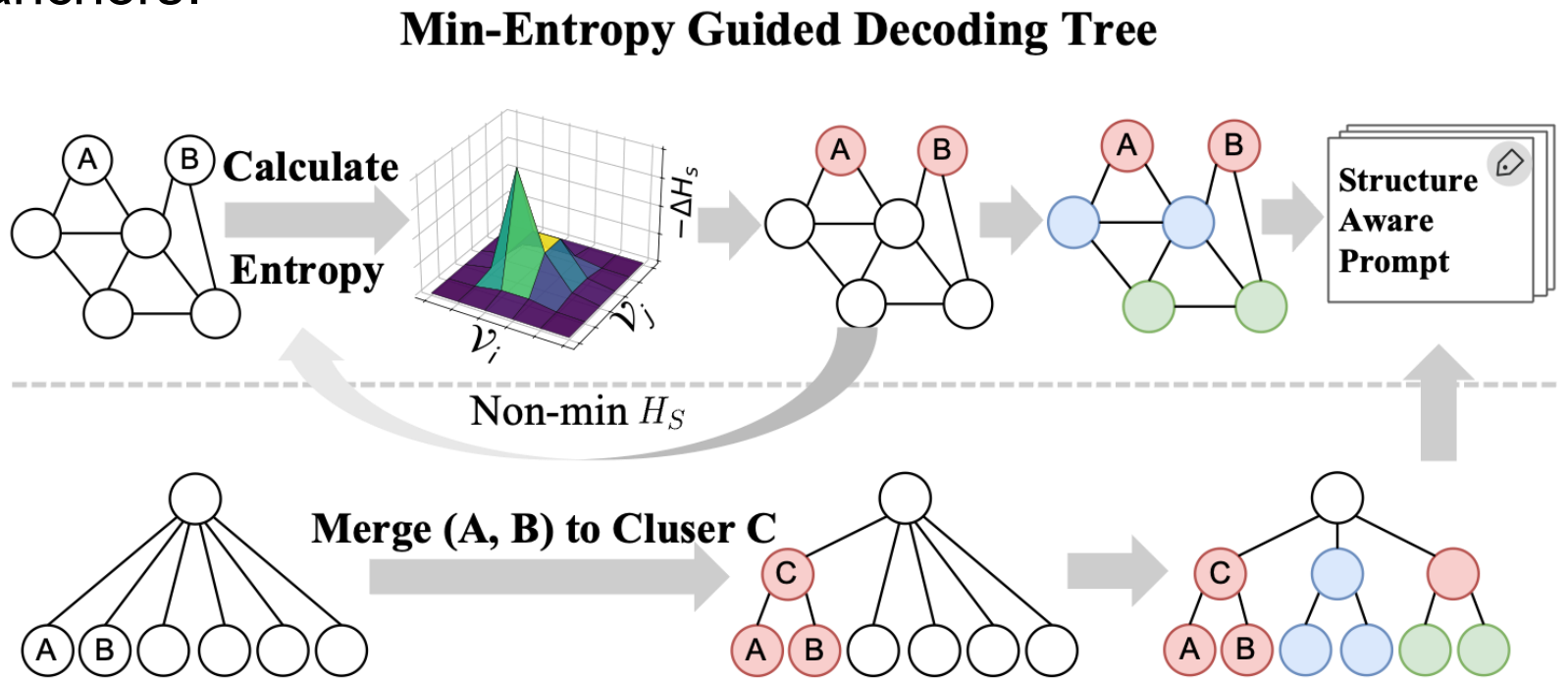
- Rely on idealized assumptions.
  - On attacked graphs, these assumptions are more likely to break down.
- Existing robust methods are costly and weak against localized structural attacks.



Junhua Shi, Qingyun Sun, et al. SA²GFM: Enhancing Robust Graph Foundation Models with Structure-Aware Semantic Augmentation, AAAI 2025.

SA²GFM

- **Motivation: Structural-Entropy Encoding Tree as a Hierarchical Semantic Anchor.**
  - Node attributes are noisy/incomplete; we need stable semantics.
  - Structural-entropy encoding trees provide multi-scale hierarchies and clusters as cross-domain anchors.

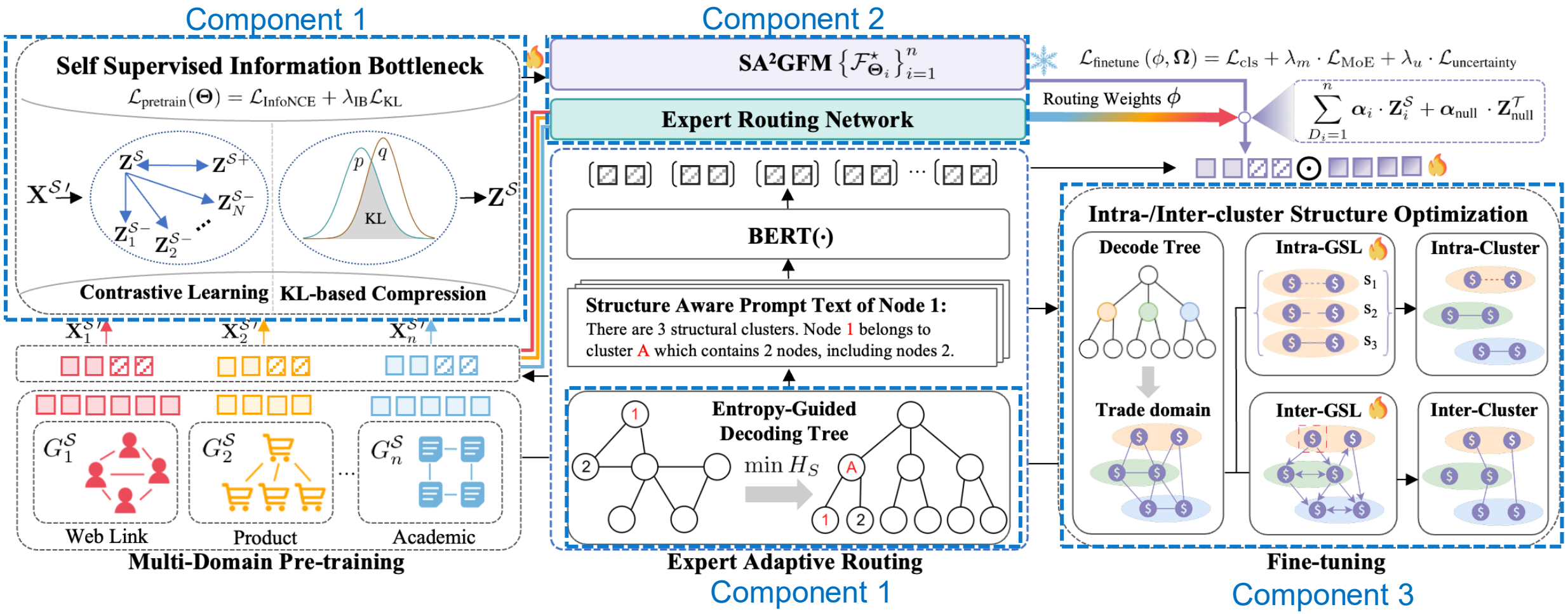


Junhua Shi, Qingyun Sun, et al. SA²GFM: Enhancing Robust Graph Foundation Models with Structure-Aware Semantic Augmentation, AAAI 2025.

SA²GFM

SA²GFM Framework Diagram

A MoE-based Robust GFM Framework.



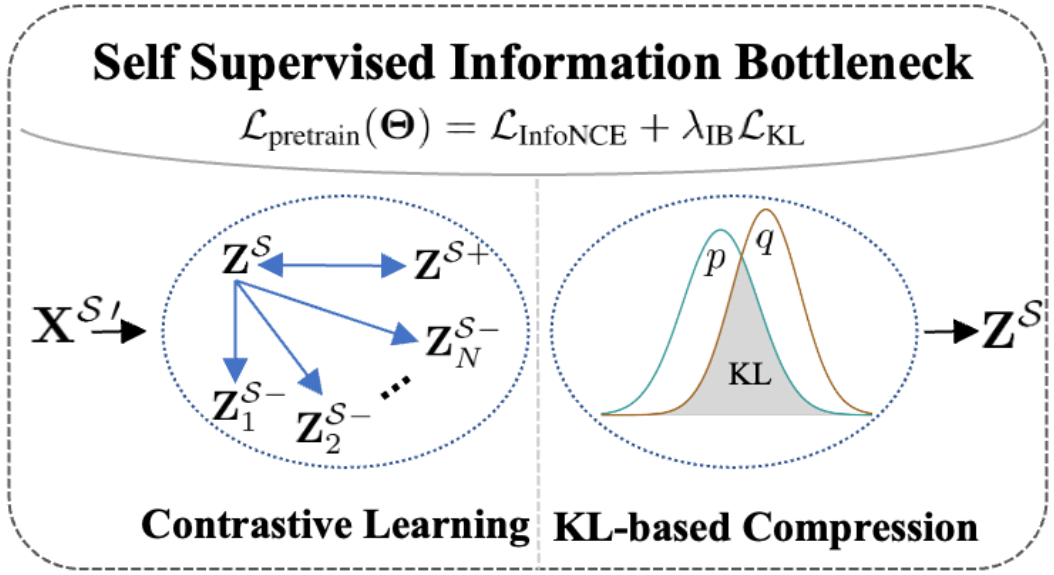
Junhua Shi, Qingyun Sun, et al. SA²GFM: Enhancing Robust Graph Foundation Models with Structure-Aware Semantic Augmentation, AAAI 2025.

SA²GFM

Structure-Aware Semantic Pre-training (SA² + SS-IB).

Inject structural semantics.

- Construct encoding trees to capture hierarchical community structures.
- Convert structural roles (cluster ID, scale) into prompts, encoded into vectors to enrich node features.



Compress noisy information

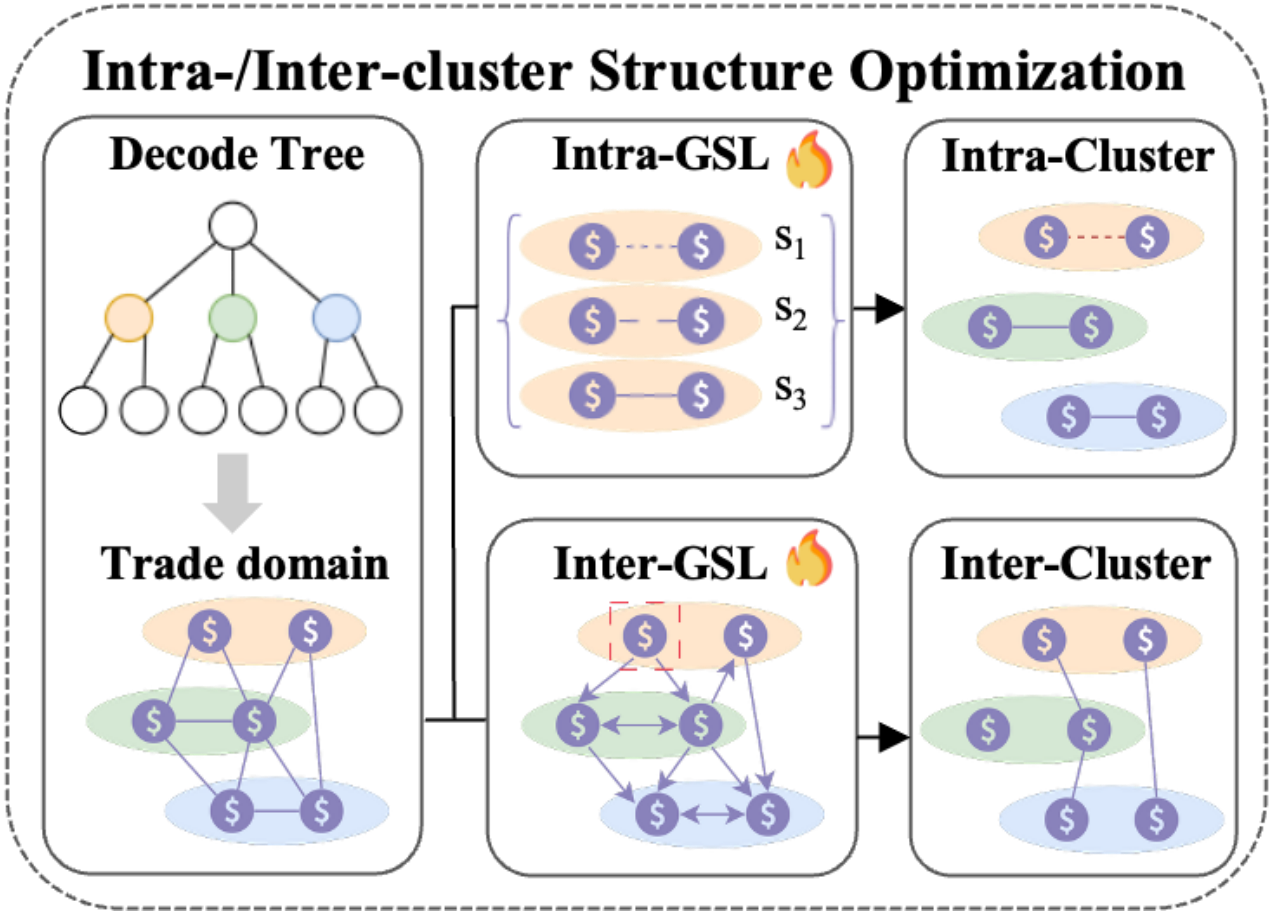
- Maximize consistency with structural neighbors via InfoNCE.
- Suppress irrelevant noise via KL-divergence regularization.

Junhua Shi, Qingyun Sun, et al. SA²GFM: Enhancing Robust Graph Foundation Models with Structure-Aware Semantic Augmentation, AAAI 2025.

SA²GFM

Hierarchical Graph Structure Optimization for Fine-tuning.

- Reuse the structural-entropy encoding tree to partition the graph into structural clusters.
- Intra-cluster GSL: Refining node relationships within each cluster for robust internal structure.
- Inter-cluster GSL: Pruning noisy inter-cluster edges using personalized propagation and soft masking.



Junhua Shi, Qingyun Sun, et al. SA²GFM: Enhancing Robust Graph Foundation Models with Structure-Aware Semantic Augmentation, AAAI 2025.

SA²GFM

Experiment I: Node classification under attacks.

Source	Cross-Dataset								Cross-Domain							
	Cora CiteSeer ogbn-Home Wiki-CS				Cora CiteSeer PubMed Wiki-CS				Cora CiteSeer PubMed ogbn-Home				ogbn-Home ogbn-Tech Wiki-CS			
Target	PubMed				ogbn-Home				Wiki-CS				ogbn-arxiv			
Noise & Attacks	feat.	struct.	evas.	pois.	feat.	struct.	evas.	pois.	feat.	struct.	evas.	pois.	feat.	struct.	evas.	pois.
GCN (backbone)	44.6±8.7	40.9±9.8	36.7±11.0	32.4±9.9	42.9±11.9	51.0±12.9	47.8±13.6	46.4±13.4	38.4±6.9	42.5±9.9	33.8±7.6	38.5±8.8	39.3±5.2	38.8±4.7	36.5±5.3	38.3±6.1
GAT	43.9±7.8	44.2±9.1	37.5±8.6	38.3±8.3	43.9±9.3	53.5±6.7	46.5±6.3	56.0±7.7	37.1±6.2	46.6±4.9	34.4±5.6	37.6±6.7	40.9±5.7	41.4±5.6	34.5±6.7	38.5±5.4
DGI	46.7±7.9	41.2±7.5	42.1±7.6	35.9±8.9	48.7±7.0	61.0±6.2	54.0±4.9	51.0±10.6	45.6±5.6	44.1±7.7	41.1±6.5	45.9±5.1	39.3±4.2	46.6±4.9	36.7±5.4	44.8±4.5
GraphCL	54.9±9.5	48.9±8.8	42.7±7.8	37.5±7.6	47.7±9.1	48.9±7.8	55.9±6.6	53.0±9.1	42.8±6.2	49.3±5.6	42.4±6.1	41.3±4.7	38.8±4.6	43.0±4.9	37.8±4.5	30.0±5.5
GraphPrompt	47.8±8.8	45.2±8.1	45.3±7.5	39.6±6.1	56.0±7.3	58.0±8.4	55.3±8.3	53.5±6.6	51.9±5.9	41.5±7.1	39.4±8.1	32.5±3.7	41.4±4.6	43.4±5.2	39.0±4.7	42.0±4.0
MDGPT	48.6±4.2	56.5±5.5	52.0±6.4	42.1±5.8	59.3±25.1	54.8±25.1	54.0±24.1	57.4±16.4	42.1±7.0	50.4±5.0	49.5±8.9	40.4±7.2	42.5±7.2	46.3±6.7	45.6±5.3	48.3±4.7
GCOPE	53.2±13.3	55.6±11.4	48.7±10.9	44.7±9.4	57.0±23.5	56.0±24.4	55.6±24.3	50.0±23.9	46.6±9.3	46.8±11.8	42.0±10.6	43.6±11.4	48.7±5.9	50.0±7.2	39.1±5.9	49.8±7.6
GraphBridge	51.1±6.8	52.4±4.3	44.0±10.1	46.9±7.4	63.0±4.5	62.2±5.2	57.1±3.7	51.3±6.6	50.1±6.6	47.3±5.7	43.2±10.1	42.4±8.3	46.5±5.7	47.3±6.6	47.5±6.2	44.5±6.0
MDGFM	57.3±6.7	58.4±7.3	53.4±7.3	50.8±5.2	65.0±15.9	65.3±17.0	62.9±15.3	62.1±16.2	53.2±6.9	52.0±5.2	50.1±6.2	46.4±5.7	55.9±4.1	55.7±4.9	50.8±5.0	50.4±4.7
SA²GFM (ours)	**60.0**±5.2	**60.1**±1.4	**56.9**±9.8	**54.5**±1.2	**68.9**±6.2	**69.0**±5.2	**65.9**±2.7	**64.0**±1.3	**55.9**±5.3	**55.9**±1.4	**53.3**±4.9	**50.6**±1.2	**57.9**±7.3	**57.8**±1.4	**55.0**±5.8	**53.0**±1.2

Table 1: Accuracy (% ± std. for 20 runs) of **5-shot node classification**. Best scores are in **bold**, runner-ups are underlined. "feat." and "struct." denote non-targeted attacks ($\lambda = 0.4$), while "evas." and "pois." denote targeted attacks ($p = 3$).

- Models with robustness measures show more stable and higher performance under various attacks.
- Compared to the baseline MDGFM, SA²GFM outperforms in accuracy, especially under "structural perturbations," providing stronger protection.

Junhua Shi, Qingyun Sun, et al. SA²GFM: Enhancing Robust Graph Foundation Models with Structure-Aware Semantic Augmentation, AAAI 2025.