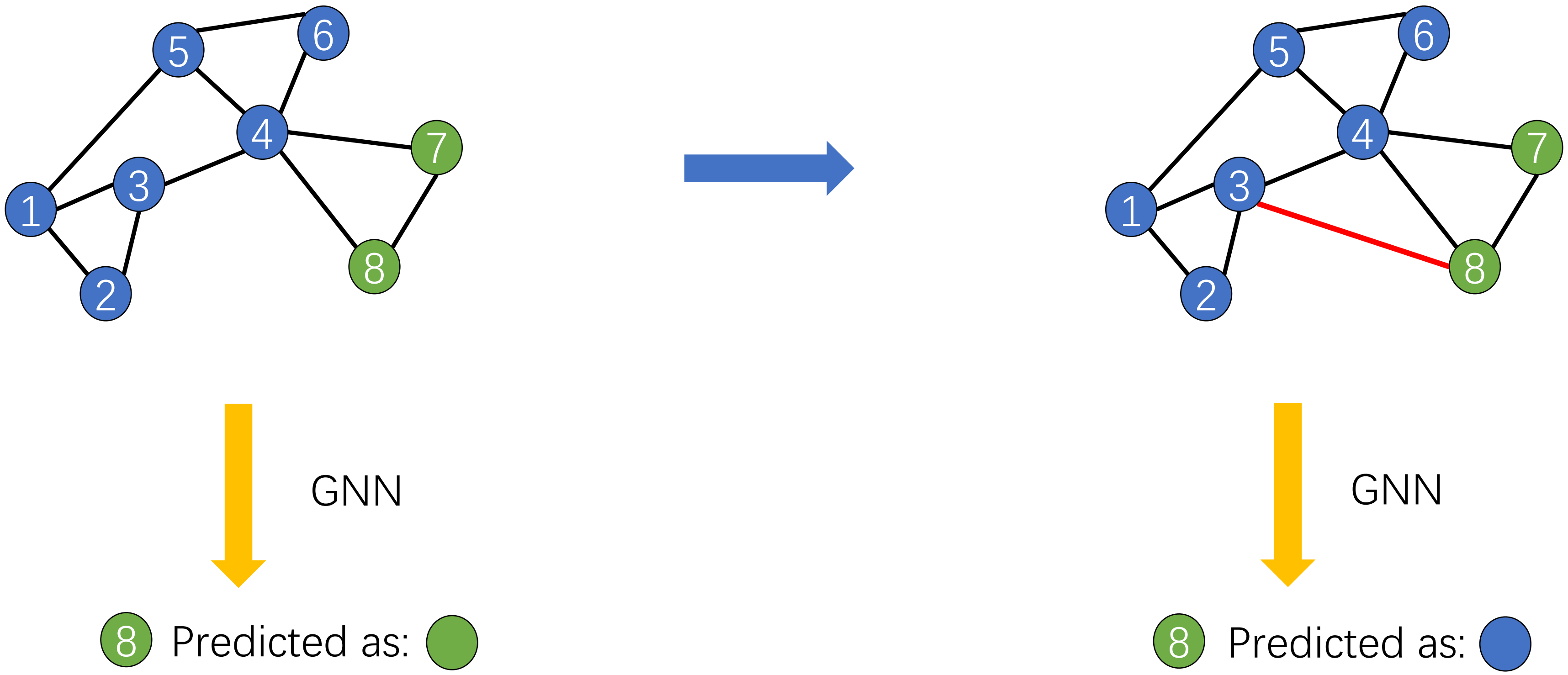
MICHIGAN STATE UNIVERSITY

Graph Structure Learning for Robust Graph Neural Networks

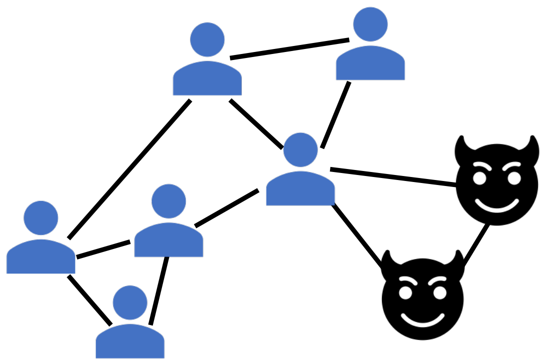
Wei Jin, Yao Ma, Xiaorui Liu, Xianfeng Tang, Suhang Wang, Jiliang Tang

KDD 2020

Adversarial Attacks on GNN



Consequences



- Financial Systems
  - Credit Card Fraud Detection
- Recommender Systems
  - Social Recommendation
  - Product Recommendation
- ….

Pro-GNN: Defend Against Adversarial Attacks

Attack Setting

- Untargeted structure attack
- Poisoning attack
- Node classification
  - Graph dataset $G = (A, X)$
  - Graph neural network f: $f(x_i) \rightarrow \hat{y}_i$

Defense Goal

- Improve the overall performance of GNN on the perturbed graph

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

Pro-GNN: Defend Against Adversarial Attacks

Graph Properties

- Low-rank
- Sparsity
- Feature smoothness

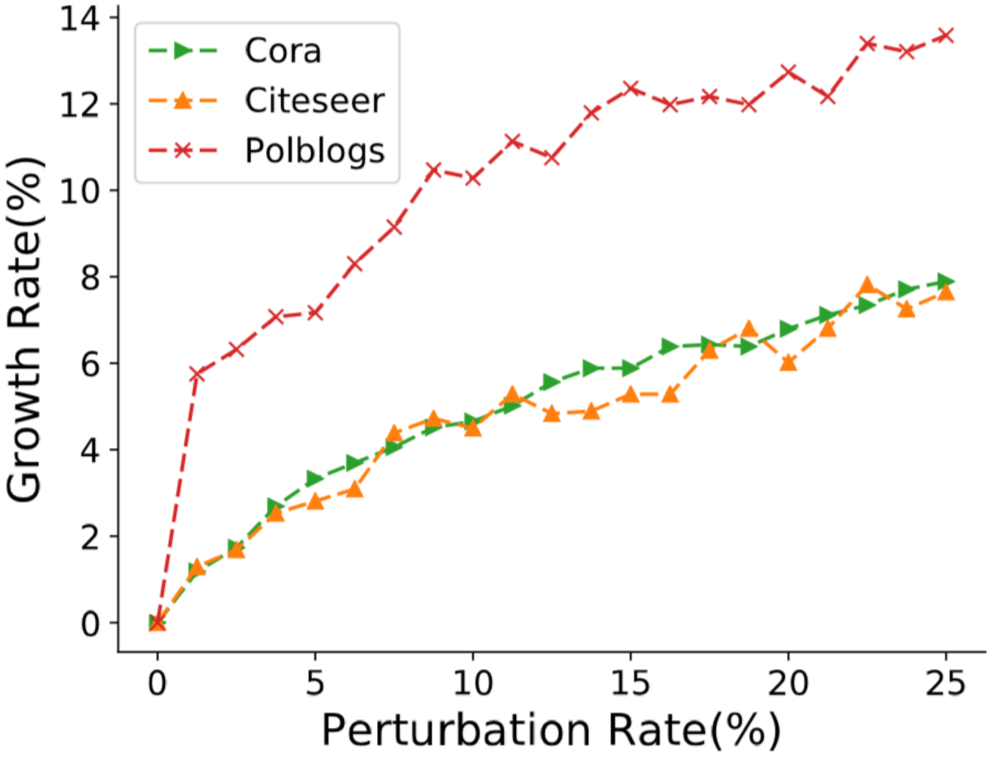
Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

MICHIGAN STATE UNIVERSITY

Pro-GNN: Defend Against Adversarial Attacks

Graph Properties

- Low-rank
- Sparsity
- Feature smoothness



(b) Rank Growth

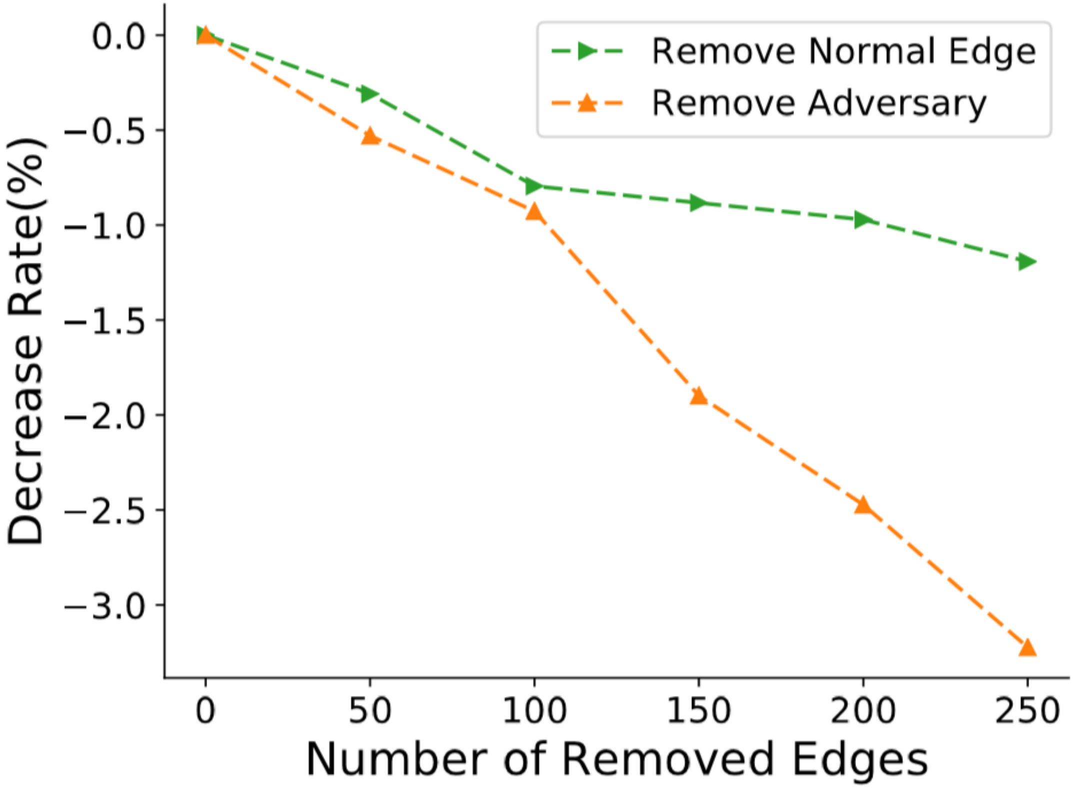
Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

MICHIGAN STATE UNIVERSITY

Pro-GNN: Defend Against Adversarial Attacks

Graph Properties

- Low-rank
- Sparsity
- Feature smoothness



Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

MICHIGAN STATE UNIVERSITY

Pro-GNN: Defend Against Adversarial Attacks

Graph Properties

- Low-rank
- Sparsity
- Feature smoothness

Dataset	$r(\%)$	edge+	edge-	edges	ranks	clustering coefficients
Cora	0	0	0	5069	2192	0.2376
	5	226	27	5268	2263	0.2228
	10	408	98	5380	2278	0.2132
	15	604	156	5518	2300	0.2071
	20	788	245	5633	2305	0.1983
	25	981	287	5763	2321	0.1943
Citeseer	0	0	0	3668	1778	0.1711
	5	181	2	3847	1850	0.1616
	1	341	25	3985	1874	0.1565
	15	485	65	4089	1890	0.1523
	20	614	119	4164	1902	0.1483
	25	743	174	4236	1888	0.1467
Polblogs	0	0	0	16714	1060	0.3203
	5	732	103	17343	1133	0.2719
	10	1347	324	17737	1170	0.2825
	15	1915	592	18038	1193	0.2851
	20	2304	1038	17980	1193	0.2877
	25	2500	1678	17536	1197	0.2723

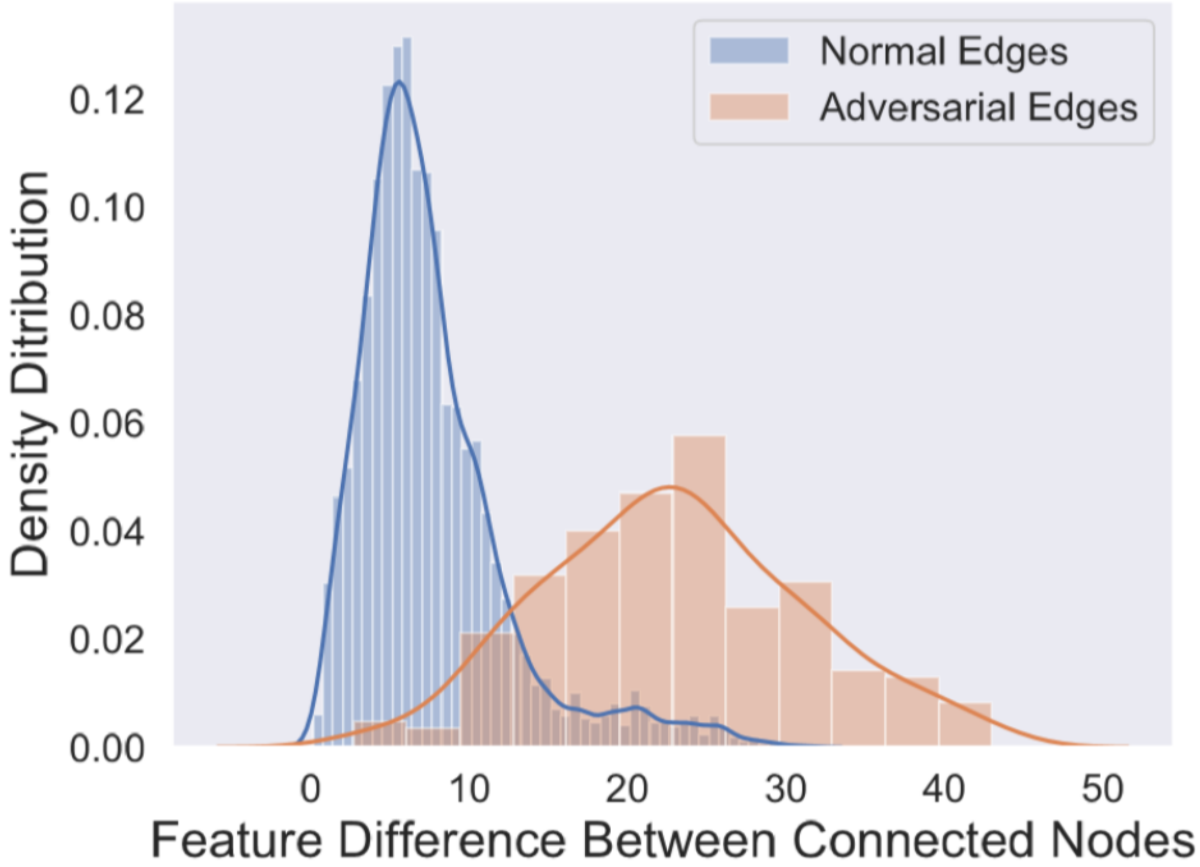
Table Credit: Adversarial Attacks and Defenses on Graphs: A Review and Empirical Study

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

Pro-GNN: Defend Against Adversarial Attacks

Graph Properties

- Low-rank
- Sparsity
- Feature smoothness



(d) Feature Smoothness

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

Pro-GNN: Framework

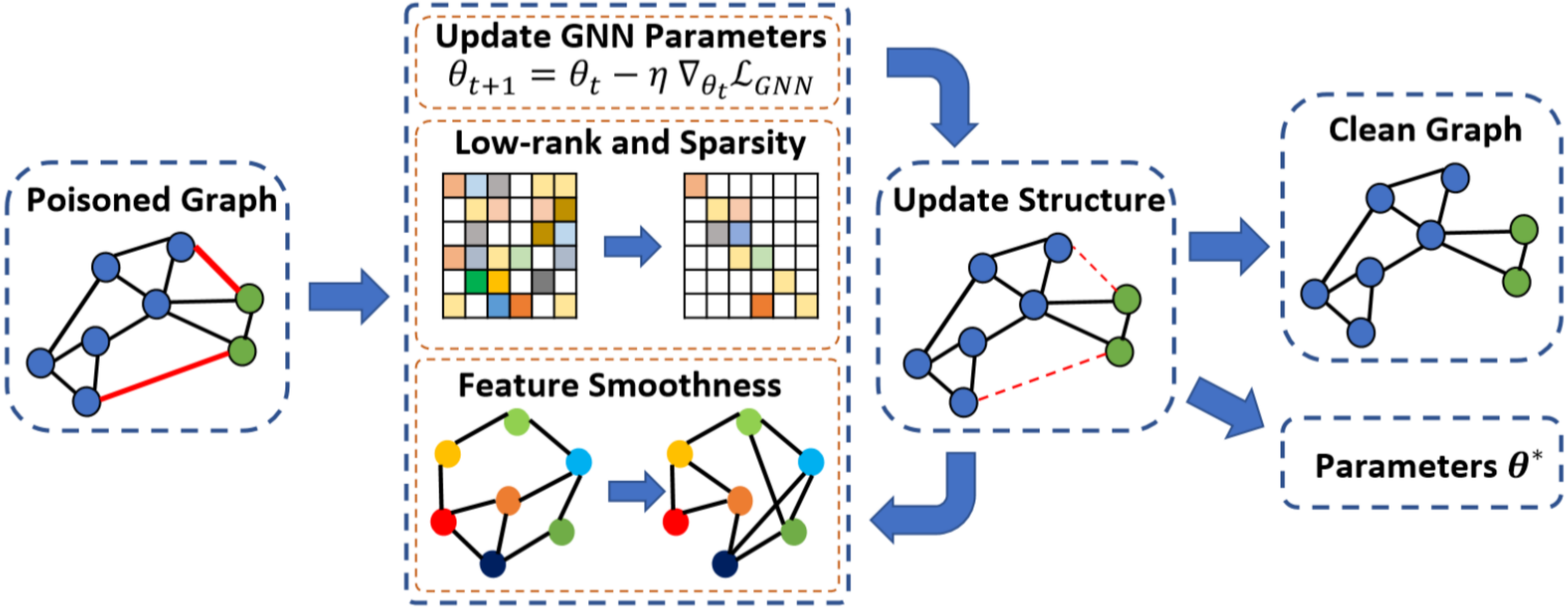


Figure 2: Overall framework of Pro-GNN. Dash lines indicate smaller weights.

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

MICHIGAN STATE UNIVERSITY

Pro-GNN: Modelling

- **Low rank and sparsity**

Perturbed Graph

$$\arg\min_{\mathbf{S}\in\mathcal{S}} \mathcal{L}_0 = \|\mathbf{A}-\mathbf{S}\|_F^2 + \alpha\|\mathbf{S}\|_1 + \beta\|\mathbf{S}\|_*, \ s.t., \mathbf{S} = \mathbf{S}^\top$$

Graph Variable to be Recovered

$$||\mathrm{S}||_1 = \Sigma_{ij}|\mathrm{S}_{ij}| \quad ||\mathrm{S}||_* = \Sigma_{i=1}^{rank(\mathrm{S})}\sigma_i$$

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

Pro-GNN: Modelling

- **Feature smoothness**

$$\mathcal{L}_s = tr(\mathbf{X}^T \hat{\mathbf{L}} \mathbf{X}) = \frac{1}{2} \sum_{i,j=1}^{N} \mathbf{S}_{ij} (\mathbf{x}_i - \mathbf{x}_j)^2$$

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

Pro-GNN: Modelling

- **Overall objective**

$$\arg\min_{\mathbf{S}\in\mathcal{S},\theta} \mathcal{L} = \mathcal{L}_0 + \lambda\mathcal{L}_s + \gamma\mathcal{L}_{GNN}$$

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

Pro-GNN: Optimization

- **Overall objective**

$$\underset{\mathbf{S}\in\mathcal{S},\theta}{\arg\min}\ \mathcal{L} = \mathcal{L}_0 + \lambda\mathcal{L}_s + \gamma\mathcal{L}_{GNN} \tag{9}$$

$$= \|\mathbf{A}-\mathbf{S}\|_F^2 + \alpha\|\mathbf{S}\|_1 + \beta\|\mathbf{S}\|_* + \gamma\mathcal{L}_{GNN}(\theta,\mathbf{S},\mathbf{X},\mathcal{Y}_L) + \lambda tr(\mathbf{X}^T\hat{\mathbf{L}}\mathbf{X})$$

$$s.t. \qquad \mathbf{S} = \mathbf{S}^\top,$$

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

Pro-GNN: Optimization

- **Overall objective**

$$\arg\min_{\mathbf{S}\in\mathcal{S},\theta} \mathcal{L} = \mathcal{L}_0 + \lambda\mathcal{L}_s + \gamma\mathcal{L}_{GNN} \tag{9}$$

$$= \underline{||\mathbf{A}-\mathbf{S}||_F^2} + \alpha||\mathbf{S}||_1 + \beta||\mathbf{S}||_* + \underline{\gamma\mathcal{L}_{GNN}(\theta,\mathbf{S},\mathbf{X},\mathcal{Y}_L) + \lambda tr(\mathbf{X}^T\hat{\mathbf{L}}\mathbf{X})}$$

$$s.t. \qquad \mathbf{S} = \mathbf{S}^\top,$$

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

Pro-GNN: Optimization

- **Alternating Optimization**

Update $\boldsymbol{\theta}$:

$$\min_{\theta} \mathcal{L}_{GNN}(\theta, \mathrm{S}, \mathrm{X}, \mathcal{Y}_L) = \sum_{u \in \mathcal{V}_L} \ell\left(f_\theta(\mathrm{X}, \mathrm{S})_u, y_u\right)$$

Update $\boldsymbol{S}$:

$$\min_{\mathrm{S}} \mathcal{L}(\mathrm{S}, \mathrm{A}) + \alpha\|\mathrm{S}\|_1 + \beta\|\mathrm{S}\|_* \quad s.t., \quad \mathrm{S} = \mathrm{S}^\top, \mathrm{S} \in \mathcal{S},$$

where $\mathcal{L}(\mathrm{S}, \mathrm{A}) = \|\mathrm{A} - \mathrm{S}\|_F^2 + \mathcal{L}_{GNN}(\theta, \mathrm{S}, \mathrm{X}, Y) + \lambda tr(\mathrm{X}^T \hat{\mathrm{L}} \mathrm{X}).$

Pro-GNN: Optimization

- **Incremental Proximal Descent method**

$$\min_{\mathbf{S}} \mathcal{L}(\mathbf{S}, \mathbf{A}) + \alpha \|\mathbf{S}\|_1 + \beta \|\mathbf{S}\|_*$$

For each iteration, do

$$\begin{cases} \mathbf{S}^{(k)} = \mathbf{S}^{(k-1)} - \eta \cdot \nabla_{\mathbf{S}} \left(\mathcal{L}(\mathbf{S}, \mathbf{A}) \right), \\ \mathbf{S}^{(k)} = \operatorname{prox}_{\eta\beta\|\cdot\|_*} \left(\mathbf{S}^{(k)} \right), \\ \mathbf{S}^{(k)} = \operatorname{prox}_{\eta\alpha\|\cdot\|_1} \left(\mathbf{S}^{(k)} \right). \end{cases}$$

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

Pro-GNN: Algorithm

Algorithm 1: Pro-GNN

Data: Adjacency matrix $\mathbf{A}$, Attribute matrix $\mathbf{X}$, Labels $\mathcal{Y}_L$,
Hyper-parameters $\alpha, \beta, \gamma, \lambda, \tau$, Learning rate η, η'

Result: Learned adjacency $\mathbf{S}$, GNN parameters θ

Initialize $\mathbf{S} \leftarrow \mathbf{A}$

Randomly initialize θ

while *Stopping condition is not met* **do**

- $\mathbf{S} \leftarrow \mathbf{S} - \eta \nabla_{\mathbf{S}}(\|\mathbf{S} - \mathbf{A}\|_F^2 + \gamma \mathcal{L}_{GNN} + \lambda \mathcal{L}_s)$
- $\mathbf{S} \leftarrow \mathrm{prox}_{\eta\beta||.||_*}(\mathbf{S})$
- $\mathbf{S} \leftarrow \mathrm{prox}_{\eta\alpha||.||_1}(\mathbf{S})$
- $\mathbf{S} \leftarrow P_{\mathcal{S}}(\mathbf{S})$
- **for** *i=1 to* τ **do**
  - $g \leftarrow \frac{\partial \mathcal{L}_{GNN}(\theta, \mathbf{S}, \mathbf{X}, \mathcal{Y}_L)}{\partial \theta}$
  - $\theta \leftarrow \theta - \eta' g$

Return $\mathbf{S}, \theta$

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

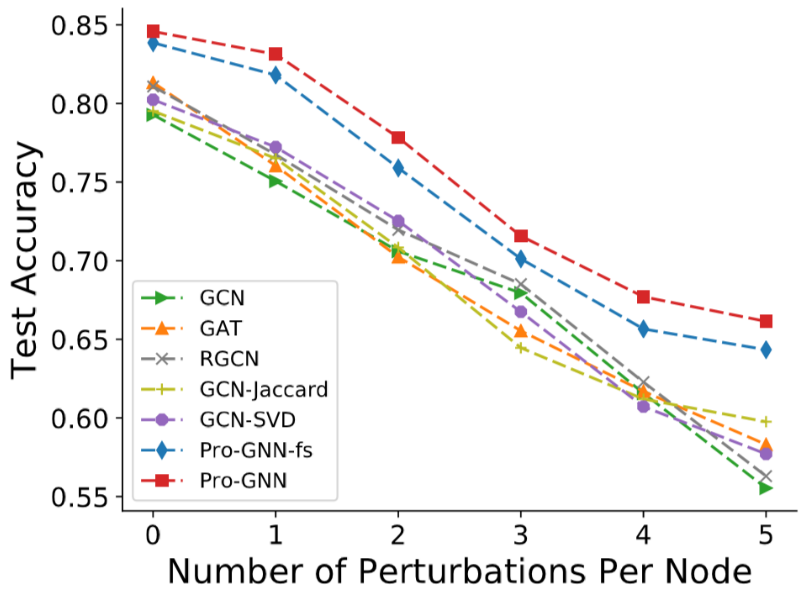
Pro-GNN: Experiments

Table 2: Node classification performance (Accuracy±Std) under non-targeted attack (*metattack*).

Dataset	Ptb Rate (%)	GCN	GAT	RGCN	GCN-Jaccard[2]	GCN-SVD	Pro-GNN-fs	Pro-GNN[3]
Cora	0	83.50±0.44	**83.97±0.65**	83.09±0.44	82.05±0.51	80.63±0.45	83.42±0.52	82.98±0.23
	5	76.55±0.79	80.44±0.74	77.42±0.39	79.13±0.59	78.39±0.54	**82.78±0.39**	82.27±0.45
	10	70.39±1.28	75.61±0.59	72.22±0.38	75.16±0.76	71.47±0.83	77.91±0.86	**79.03±0.59**
	15	65.10±0.71	69.78±1.28	66.82±0.39	71.03±0.64	66.69±1.18	76.01±1.12	**76.40±1.27**
	20	59.56±2.72	59.94±0.92	59.27±0.37	65.71±0.89	58.94±1.13	68.78±5.84	**73.32±1.56**
	25	47.53±1.96	54.78±0.74	50.51±0.78	60.82±1.08	52.06±1.19	56.54±2.58	**69.72±1.69**

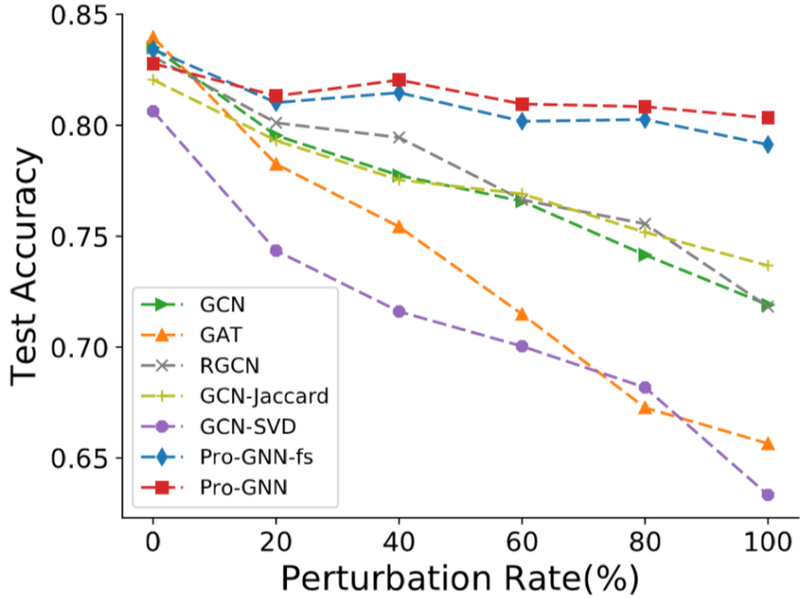
Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

Pro-GNN: Experiments



(a) Cora

Under Nettack



(a) Cora

Under Random Noise

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

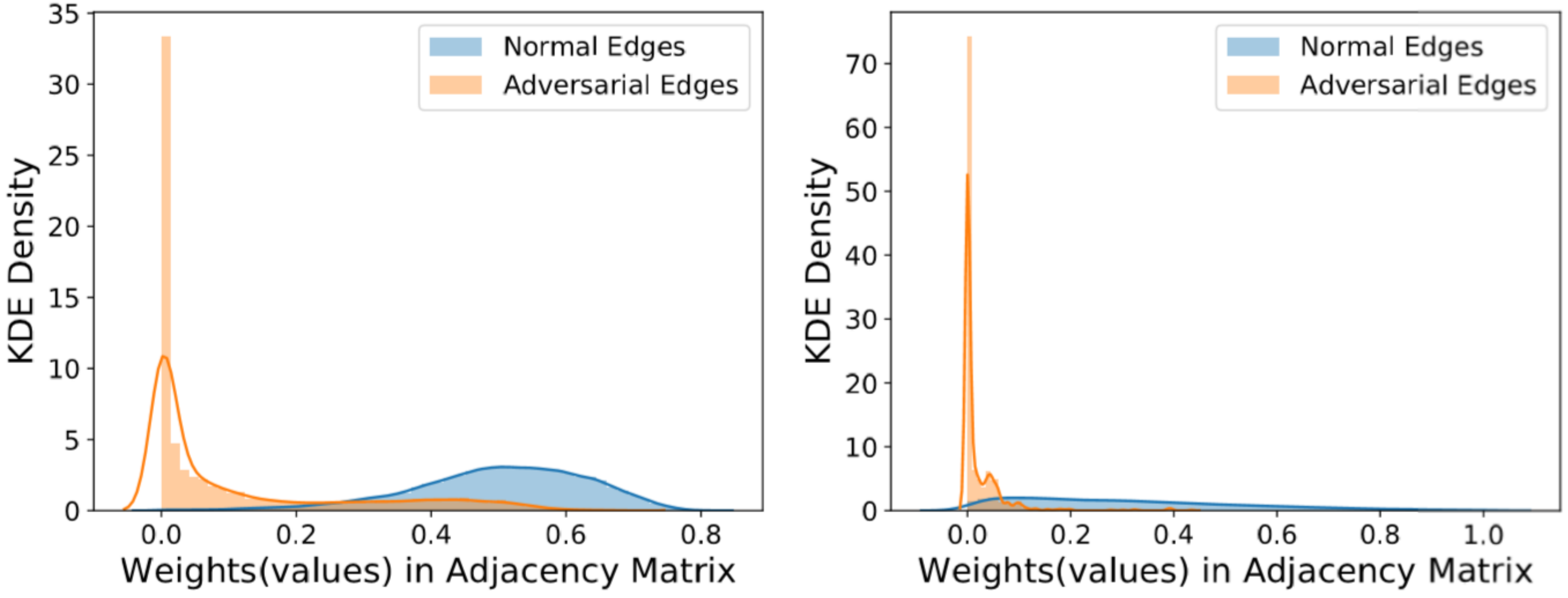
Pro-GNN: Importance of Graph Structure Learning

Table 3: Node classification accuracy given the graph under 25% perturbation by *metattack*.

	GCN	GCN-NoGraph	Pro-GNN
Cora	47.53±1.96	62.12±1.55	**69.72±1.69**
Citeseer	56.94±2.09	63.75±3.23	**68.95±2.78**
Polblogs	49.23±1.36	51.79±0.62	**63.18±4.40**
Pubmed	75.50±0.17	84.14±0.11	**86.86±0.19**

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

Pro-GNN: Importance of Graph Structure Learning

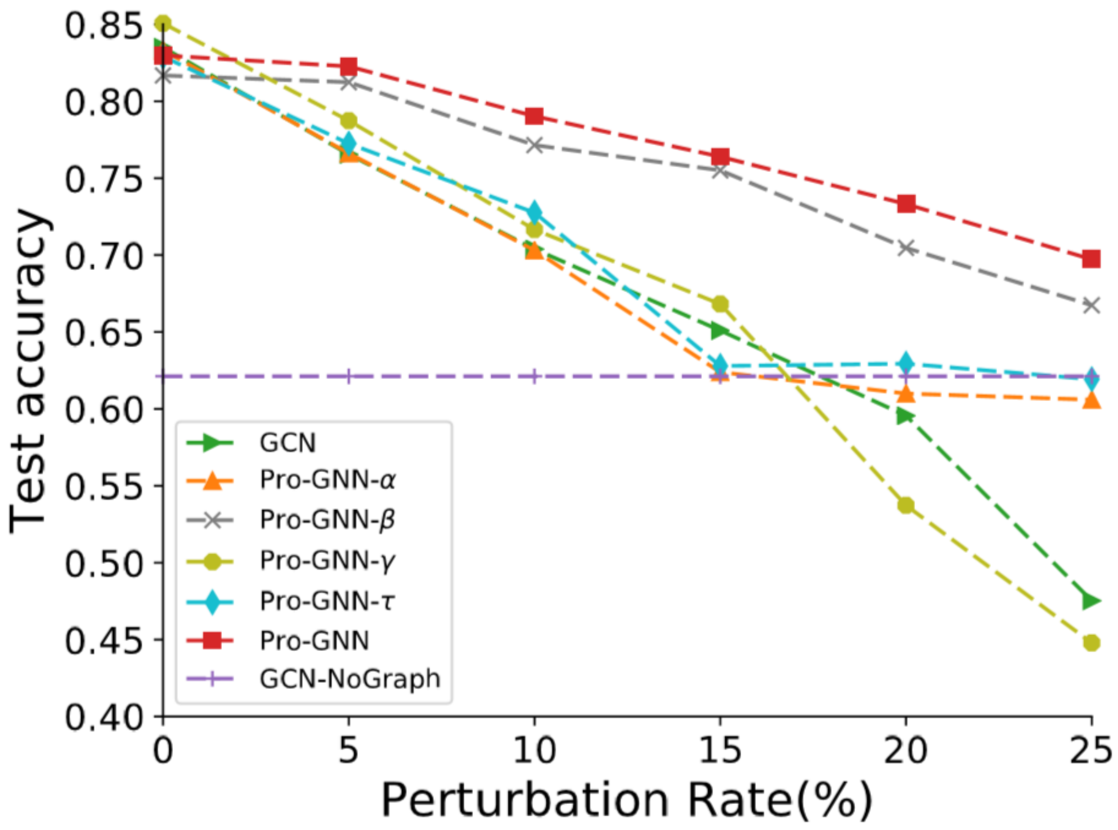


(a) Pubmed (b) Polblogs

Figure 5: Weight density distributions of normal and adversarial edges on the learned graph.

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

Pro-GNN: Ablation Study



(a) Cora

Graph Structure Learning for Robust Graph Neural Networks. KDD 2020.

Conclusion

- We found that graph adversarial attack can break important graph properties
- We introduced a novel defense approach Pro-GNN that learns the graph structure and GNN parameters simultaneously
- Our experiments show that our model consistently improves the overall robustness under various adversarial attacks.

Paper Link:

https://arxiv.org/abs/2005.10203

Code:

https://github.com/ChandlerBang/Pro-GNN

THANK YOU