

实验

Nettack

攻击数量 (n_perturbations) =节点度数

数据集：citeseer

nhid=256

dropout=0.5

模型准确率：0.7518

target_node = 2

degree = 3

probs						
原图	1.7326763e-04	3.6682227e-06	3.2556129e-06	1.9733849e-04	9.9956024e-01	6.2294312e-05
Di攻击 (n_p=3, ac=0.7553)	1.4218735e-04	2.0526582e-05	4.2054210e-02	9.7954168e-04	9.5652556e-01	2.7797490e-04
Di攻击 (n_p=5, ac=0.7559)	5.31222846e-04	1.13729155e-04	2.67369449e-01	1.94640784e-03	7.28962719e-01	1.07648724e-03
Di攻击 (n_p=10,ac=0.7541)	1.1138700e-04	1.6566119e-05	8.4839410e-01	2.4468792e-04	1.5109171e-01	1.4152337e-04

target_node = 835

degree=3

probs						
原图	9.0885547e-04	2.7260825e-04	1.6283998e-03	2.4812532e-04	1.1325887e-03	9.9580950e-01
Di攻击 (n_p=3, ac=0.7577)	9.2156470e-04	2.0588623e-04	4.4301958e-03	1.1053098e-03	9.2521888e-01	6.8118252e-02
GNNGuard	0.00317302	0.00101452	0.07646983	0.00427487	0.08355595	0.8315118
In攻击 (n_p=3, ac=0.7405)	2.58953753e-03	1.08276625e-04	1.40421512e-03	9.15708602e-04	7.12281838e-02	9.23754036e-01
In攻击 (n_p=5, ac=0.7405)	4.3731881e-03	2.7371987e-04	2.4297575e-03	1.4615151e-03	1.5104952e-01	8.4041232e-01
In攻击 (n_p=8, ac=0.7399)	6.6988729e-04	4.6672038e-05	4.3032473e-04	7.3149381e-04	9.9786931e-01	2.5229124e-04

target_node = 673

degree=1

probs						
原图	0.02265007	0.03263679	0.79987675	0.07627997	0.05615364	0.01240286
Di攻击 (n_p=1, ac=0.7565)	0.00565171	0.00527534	0.05544702	0.01821648	0.90212035	0.01328904
GNNGuard	0.01883293	0.02634256	0.7645346	0.10336491	0.06031256	0.02661247

target_node = 1104

degree=1

probs						
原图	5.91320358e-03	5.71389496e-01	1.70132320e-04	5.91473505e-02	1.52842915e-02	3.48095536e-01
Di攻击 (n_p=1, ac=0.7571)	0.00754101	0.00863327	0.00498412	0.04477421	0.88995546	0.0441118
GNNGuard	8.7293942e-04	5.3738928e-01	1.3083368e-04	3.9997451e-02	9.8550478e-03	4.1175440e-01

Mettack

网络模型	数据集	参数	准确率	错误率
GCN	CORA	no_attack	0.8280	0.172
		ptb_rate: 0.05	0.7827	0.2173
		ptb_rate: 0.1	0.7138	0.2862