

# GNNGuard

## Mettack

网络模型	数据集	参数	准确率
GCN	CORA	no_attack	0.8280
		ptb_rate: 0.05	0.7827
		ptb_rate: 0.1	0.7138

## 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

n\_perturbations=3

原图分类 概率:						
probs	1.7326763e-04	3.6682227e-06	3.2556129e-06	1.9733849e-04	<b>9.9956024e-01</b>	6.2294312e-05

Di攻击:						
probs	1.4218735e-04	2.0526582e-05	4.2054210e-02	9.7954168e-04	<b>9.5652556e-01</b>	2.7797490e-04

模型准确率: 0.7553

n\_perturbations=5

Di攻击:						
probs	5.31222846e-04	1.13729155e-04	2.67369449e-01	1.94640784e-03	<b>7.28962719e-01</b>	1.07648724e-03

模型准确率: 0.7559

n\_perturbations=10

Di攻击:						
probs	1.1138700e-04	1.6566119e-05	8.4839410e-01	2.4468792e-04	1.5109171e-01	1.4152337e-04

模型准确率: 0.7541

target\_node = 835

n\_perturbations=3

原图分类概率:						
probs	9.0885547e-04	2.7260825e-04	1.6283998e-03	2.4812532e-04	1.1325887e-03	9.9580950e-01

Di攻击:						
probs	9.2156470e-04	2.0588623e-04	4.4301958e-03	1.1053098e-03	9.2521888e-01	6.8118252e-02

模型准确率: 0.7577

In攻击:						
probs	2.58953753e-03	1.08276625e-04	1.40421512e-03	9.15708602e-04	7.12281838e-02	9.23754036e-01

模型准确率: 0.7405

n\_perturbations=5

In攻击:						
probs	4.3731881e-03	2.7371987e-04	2.4297575e-03	1.4615151e-03	1.5104952e-01	8.4041232e-01

模型准确率: 0.7405

n\_perturbations=8

In攻击:						
probs	6.6988729e-04	4.6672038e-05	4.3032473e-04	7.3149381e-04	9.9786931e-01	2.5229124e-04

模型准确率: 0.7399

target\_node = 673

n\_perturbations=1

原图分类 概率:						
probs	0.02631131	0.22100534	<b>0.6239099</b>	0.07506889	0.03079453	0.02291001

Di攻击:						
probs	0.00565171	0.00527534	0.05544702	0.01821648	<b>0.90212035</b>	0.01328904

模型准确率: 0.7565

---

target\_node = 1104

n\_perturbations=1

0.00754101 0.00863327 0.00498412 0.04477421 0.88995546 0.0441118

原图分类 概率:						
probs	0.04508255	0.3628147	0.01089143	<b>0.40291938</b>	0.0286	0.14969192

Di攻击:						
probs	0.00754101	0.00863327	0.00498412	0.04477421	<b>0.88995546</b>	0.0441118

模型准确率: 0.7571

---