Scaling Adversarial Attacks and Defenses for Graph Neural Networks

Anonymous authors
Paper under double-blind review

Abstract

The abstract paragraph should be indented 1/2 inch (3 picas) on both left and right-hand margins. Use 10 point type, with a vertical spacing of 11 points. The word Abstract must be centered, in small caps, and in point size 12. Two line spaces precede the abstract. The abstract must be limited to one paragraph.

1 Introduction

Contributions:

- Scalable defense: Soft Median
- Scalable attacks: Greedy attacks (FSGM, KDD Cup), sampled PGD

2 Related Work

None of the methods really scale or at least it has not been shown (neither for defenses and attacks)

Exception KDD Cup (600k nodes graph)

3 Defense

We build upon the very recent attack Soft Medoid GDC...

3.1 Method

aka Soft Median

$$\arg\min_{x_i \in X} \| x_i - median(X) \|_p$$

$$\arg\min_{x_i \in X} \| x_i - \bar{x} \|_p$$

Somewhat similar to a Gaussian:

$$\exp_{x_i \in X} \| x_i - \bar{x} \|_p / T$$

(Todo: Reference Sirin et al. 2020)

- Derivation: From Soft Medoid via SoftSort to Soft Median
- Using the Soft Median within GNNs: What properties do we need (weighting)
- Alternative motivation: somewhat similar to a Gaussian / Kernel density estimate
- Complexity Analysis
- Robustness properties: i.e. breakdown down

4 Attacks

4.1 Greedy Attacks

4.2 Sampled Projected Gradient Descent

5 Empirical Results

5.1 Experiment Setup

Other defenses: SVD GCN, RGCN, Jaccard GCN Other attacks: Dice, Nettack, PGD, Greedy Attack

5.2 Small Data Sets

5.3 Large Datasets

6 Conclusion

References

A Appendix

You may include other additional sections here.