ALL YOU NEED IS LOW (RANK): DEFENDING AGAINST ADVERSARIAL ATTACKS ON GRAPHS

A NOTE

Zepeng Zhang

June 21, 2022

This paper [1] explored the properties of NETTACK perturbations and found that only high-rank (low-valued) singular components of the graph are affected. They show that a low-rank approximation of the graph (can be constructed using truncated SVD) can greatly reduce the effect of NETTACK and boost the performance of GCN when facing adversarial attacks. They also investigate the influence of a low-rank attack LowBlow, which is designed based on NETTACK. However, LowBlow perturbations are noticeable and the attacked graph does not have the same degree distribution as the input graph. Besides, by modifying LowBlow to preserve the degree distribution makes it a high-rank attack. This implies that an unnoticeable perturbation affects high frequency spectrum of the graph. Consequently, the low-rank vaccination mechanism can defend against unnoticeable adversarial attacks.

References

[1] Negin Entezari, Saba A Al-Sayouri, Amirali Darvishzadeh, and Evangelos E Papalexakis. All you need is low (rank) defending against adversarial attacks on graphs. In *Proceedings of the 13th International Conference on Web Search and Data Mining*, pages 169–177, 2020.