Edge-level privacy in Graph Neural Networks

Rucha Bhalchandra Joshi[1,2][0000−0003−1214−7985] and Subhankar Mishra[1,2][0000−0002−9910−7291]

[1] National Institute of Science Education and Research, Bhubaneswar India
[2] Homi Bhabha National Institute, Mumbai, India
{rucha.joshi,smishra}@niser.ac.in

Abstract. The problem of privacy in graph neural networks (GNNs) is being studied recently. It is necessary in order to ensure the privacy of the system that is being modeled as graphs. Currently, the existing models primarily consider the node features and the node labels as privacy information corresponding to the graphs. We propose an edge-privacy preserving methodology called EP-GNN to incorporate the privacy of the structural information of the graphs as well in addition to the features and the label information of the graphs. In this preliminary work, we investigate the impact of the noisy neighborhood on the accuracy of the GNNs. This is in addition to the We experiment with the amount of neighborhood that we perturb and the privacy budget for the edge privacy. We propose two methods to consider the neighborhood, namely 1. $\lambda - selector$ from the neighborhood, and 2. complete neighborhood in order to ensure privacy in the edge data of the graph. We continue to use the node and label privacy as they are implemented in the previous methods for privacy in GNNs.

Keywords: Differential Privacy · Graph Neural Networks