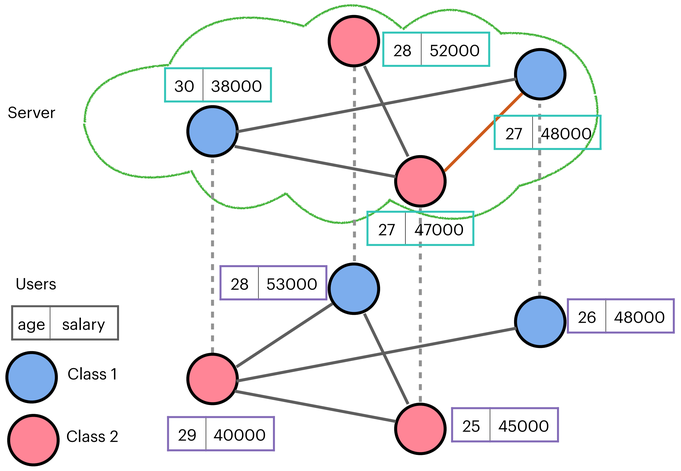
Edge-Level Privacy in Graph Neural Networks

Rucha Bhalchandra Joshi and Subhankar Mishra
NISER Bhubaneswar and HBNI Mumbai, India

Overview

TL; DR: Make the structure of the graph private in addition to the privacy of node features and labels



Local Differential Privacy:

$$\forall y \in Range(\mathscr{A}) : Pr[\mathscr{A}(x) = y] \leq e^{\epsilon} Pr[\mathscr{A}(x') = y]$$

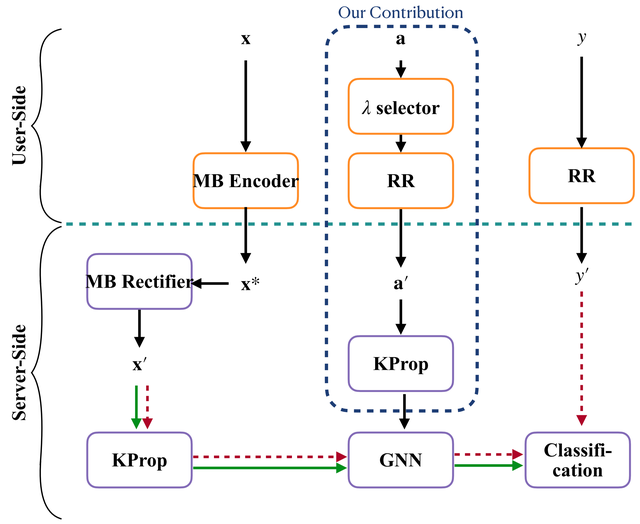
where ϵ is the privacy budget.
The noise is added at the users' side before passing on the information to the server where it is given to a Graph Neural Network.

λ-selector

To select the amount of noise to add to neighborhood data of each node, we propose λ-selector algorithm, where λ is the percentage of noise to be added
For each node:

1. Calculate λ percentage of degree
2. Sample λ percent nodes from a set of nodes except the actual neighborhood
3. Return the nodes sampled in step 2 along with the actual neighborhood

Method: EP-GNN



Randomization

To add noise, take the set of nodes and apply **randomized response (RR)** as follows:

$$p(a'|a) = \begin{cases} \frac{e^{\epsilon}}{1+e^{\epsilon}} & \text{if } a' = a \\ \frac{1}{1+e^{\epsilon}} & \text{otherwise} \end{cases}$$

k-Prop

Added noise is removed to some extent by using aggregation of the node features over the neighborhood of a node. This aggregation is performed in k-Prop.

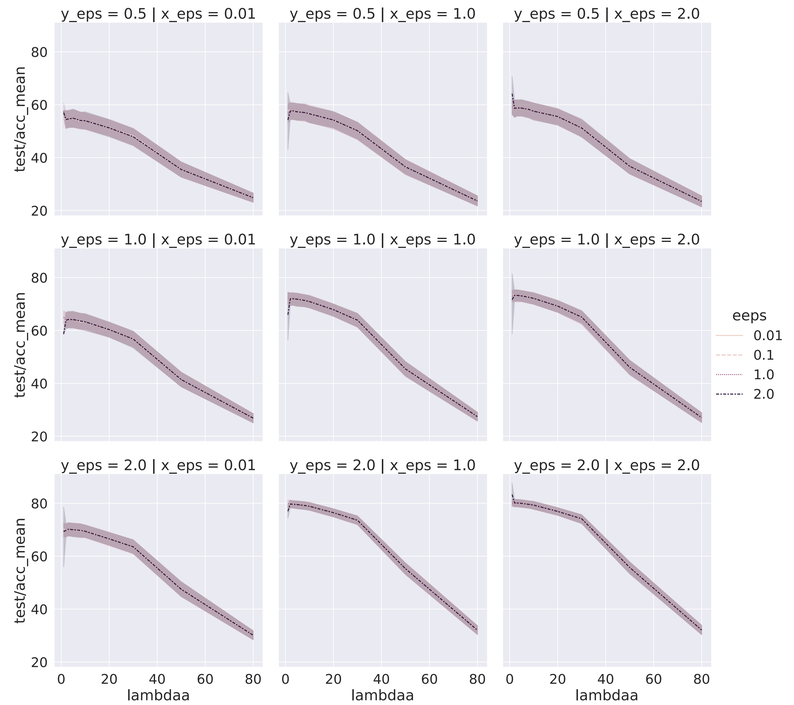
$$h^{k}_{\mathcal{N}(v)} = \text{Aggregate}\left(\{h^{k-1}_{\mathcal{N}(u)}, \forall u \in \mathcal{N}(v) - \{v\}\}\right)$$

Privacy in node features and labels: Earlier methods [1] provide ways to privatize the node features by using multi-bit mechanism and node labels by applying RR.

Dataset Statistics

Dataset	Classes	Nodes	Edges	Features	Average Degree
Cora	7	2708	5278	1433	3.90
Pubmed	3	19717	44324	500	4.50
Facebook	4	22470	170912	4714	15.21
LastFM	10	7083	7842	7842	7.29

Results



Privacy in our model is controlled by λ and ϵ. Addition of more noise, makes the data more private, but leads to drop in accuracy in the task the GNN addresses.

Reference:
[1] Sajadmanesh, Sina and Daniel Gática-Pérez. "Locally Private Graph Neural Networks." Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (2021): n. pag.