Federated Latent Dirichlet Allocation: A Local Differential Privacy Based Framework

Yansheng Wang, Yongxin Tong, Dingyuan Shi
SKLSDE Lab, BDBC, School of Computer Science and Engineering and IRI, Beihang University, China
{arthur_wang, yxtong, chnsdy}@buaa.edu.cn

Introduction

• Latent Dirichlet Allocation (LDA) is often used for text mining and has been a fundamental building block for many Internet services, but privacy leak in text data is a problem.

• Federated learning (FL) can be a potential solution, but existing techniques can hardly be applied in LDA.

Theoretical Analysis

• Assume frequency of words follow the Zipf’s law (a)

• Use the failure rate $\delta$ to control the remainders with low frequency (b)

• Theorem 1 (Privacy guarantee)
  - By setting $\eta = \frac{1}{\delta \delta_{e} e^{\delta_{e}+1}}$, the proposed mechanism satisfies $(\epsilon, 2\delta)$-LDP, where $\delta_{0} = \delta - (\delta^{-1} + 1)^{-1}$, $\gamma \geq 1$ is a constant.

• Theorem 2 (Utility guarantee)
  - Given a fixed topic, the expected relative error of the model parameter $\phi_{w}$ after perturbation is bounded by $O(\eta k^2)$ where $k$ is the rank of $w$ by sorting $\phi_{w}$ in descending order.

Experimental Evaluation

Results of GS

Results of MH

Varying Privacy budget, number of topics and sampling ratio

The probability that the perturbed word is the one in the rectangle is $0.6 \times 0.6 + 0.2 \times 0.1 = 0.38$