1 abstract

distributed online learning, each learner optimizes its own learning parameter based on local data source and correspond with neighbours timely.

privacy breaches(隐私泄露)

centralized approach

online data collection is inherently decentralized: data source are often widely distributed in different geographical locations.

wide distribution:online learning high velocity: high dimensionality: sparse, spark and parallelize privacy concern:

exchange intermediate parameters with a random part of their own neighboring(spark trees: find a leaf and route to the corresponding subtree)

distributed online learning

similar to the mini-batch online learning. each iteration, the process receives K instances. Then each node processes one of the instances and updates its local model. These nodes communicate with each other to keep the consistency of their local model.

A key factor in designing a distributed algorithm is the communication load between nodes.

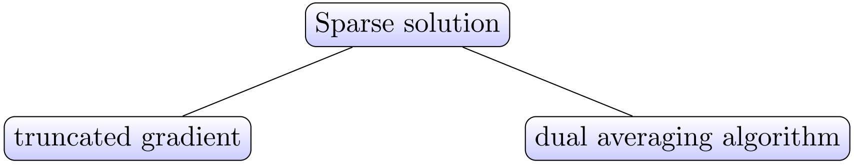
2 INTRODUCTION

All nodes exchange their local parameter with their neighboring nodes.

For the privacy mechanism, differentially private framework is proposed with sensitive data

high-dimensional.

sparse solution.

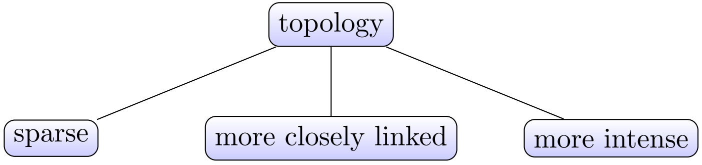


DOLA take online mirror descent and $Lasso - L_1$ norm.

3 EXPERIMENTS

step 1 regard one CPU as one node. and equally distribute the dataset to the m nodes.

There are three different topologies.



step 2, communication matrix A_t. A map for communication.

step 3,

openMPI

4 Related Work

differentially private centralized online learning.

5 problem setting

communication cost is not considered.

any node of the system can measure the regret of the whole system based on its local parameter

use a time-variant matrix A_t to conduct the communications among nodes.

Each node first gets the exchanged parameters and computes the weighted average of them, then updates the parameter w_t^i, finally broadcasts new parameter to its neighbours.

$$\mathcal{G}_i(t) = \{(i, j) : a_{ij}(t) > 0\}.$$

5.1 Differential Privacy Model

Definition 2 Let $\mathcal{A}$ denote differentially private DOLA. Let $\mathcal{X} =< x_1^i, x_2^i, ..., x_T^i >$ be a sequence of questions taken from an arbitrary node's loocal data source. Let $\mathcal{W} =< w_1^i, w_2^i, ..., w_T^i >$ be a sequence of T outputs of the node and $\mathcal{W} = \mathcal{A}(\mathcal{X})$. Then, our algorithm $\mathcal{A}$ is $\epsilon-$differentially private if given any adjacent question sequnces $\mathcal{X}$ and $\mathcal{X}'$ that differ in one question entry, the following holds:

$$Pr[\mathcal{A}(\mathcal{X}) \in W] \leq e^{\epsilon} Pr[\mathcal{A}(\mathcal{X}^{'}) \in W]$$