Why FL?

Differences from DML
Federated Learning is used when the devices involved has different datasets with diverse samples and feature space

In our case
Useful to keep carrier topology and failures data private and share common key parameters
How works

Global FL Model

Edge Server

Local FL Model

Data

Device 1

Device 2

Device K

$$g = \frac{\sum_{i=1}^{K} \omega_i}{K}$$
Federated Learning common use cases

**IoT**
Little devices just apply the global model and send back the key values.

**Finance**
Needs to keep transactions data private but need to contribute to the global model for fraud detention.

**Mobile Network**
Provide personalized services without sending personal data to a central server.
Main Features of FL

Preserving data Privacy
Local dataset on local devices without sharing crucial information.

Centralized global server
Communicate with edge servers receiving key parameters and updating the model.

Data Diversity
Aggregation of different dataset and for developing a unique model distribution.

Difficulties with different data distributions
Lack of uniformity in the input space makes challenging to train a model that generalizes.
Task 6

Problem
Use FL to maintain quality of services in the network-cloud ecosystem based on cooperation among different entities

Goal
- improve monitoring/telemetry
- ensure privacy
- accommodate new services and minimize future risks
Objective and Mechanism

Local Model Aggregation
Selection of optimal devices to upload the local models and minimize transmission error.

Communication Efficiency and Energy consumption
Optimize transmission rate, avoid congestions, improve communication design.
Optimize communication efficiency and energy consumption of the ecosystem.

Resource Allocation
Spectrum resource allocation and device selection.
Investigate models for task 1 and 2 by adding FL tools. Thus, each entity can apply global model.

Mechanism Design
Understand how to design the business mechanism with a certain outcome expectation.
Find the right model for perfect cooperation and reach optimal solution for all entities.

Asynchronous FL
Each training round of the synchronous training is limited by the slowest device. Understanding the bottleneck in network-cloud ecosystem and make the training asynchronous.

Homomorphic Encryption
Computing sum of values without having any party reveal its values.
Allow the ecosystem to ensure security of their data adding encrypted secret keys.

Game Theory
Design mathematical cooperative model for Service Pricing.
Establish price and values of services and maximizing profits.

How to apply in task 6?
References


Please comment and suggest, thank you

Ignazio Maria Castrignano