Resilient Federated Learning Framework
Sprint 1

Student: Leonardo Almeida

Supervisor: Mario Luis Pinto Antunes

Co-supervisors: Rui Aguiar

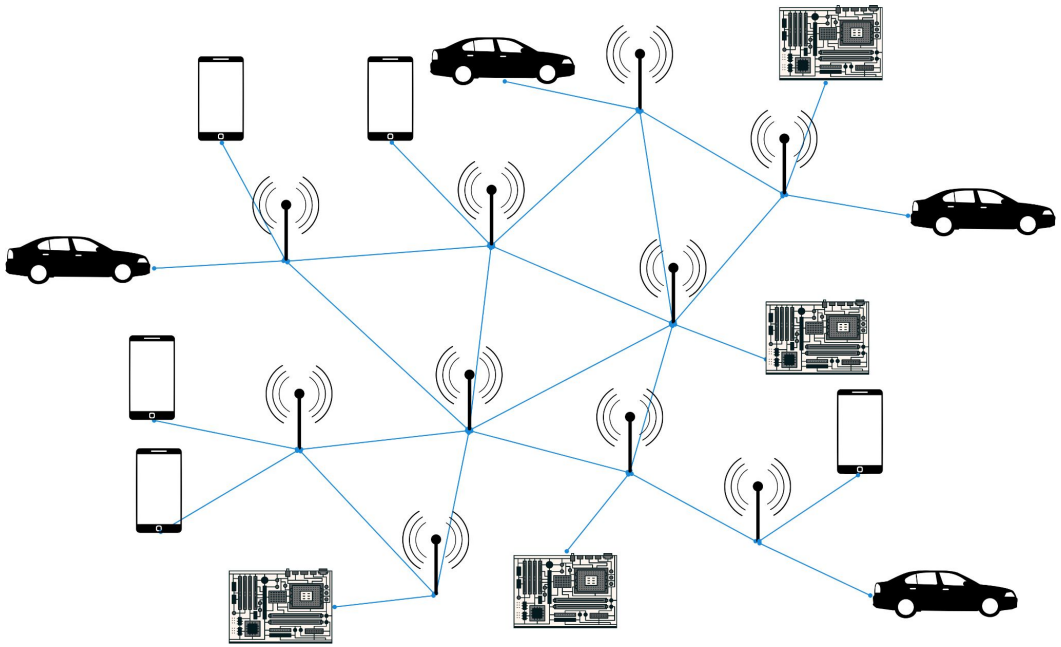
Summary: Federated Learning (FL) offers a promising approach to training machine learning models collaboratively across distributed devices while preserving data privacy. However, the performance and robustness of FL systems are heavily influenced by the underlying communication infrastructure. The proposed framework will incorporate mechanisms to gracefully handle the addition and removal of worker nodes, minimizing disruptions to the training process and maintaining model quality.

Context and Objectives

- How to deal with sensitive data in ML?
- How can multiple entities collaborate to an AI model?
- How to ensure proper functionality when entities fail?

Resilient Federated Learning

- Privacy
- Scalability
- Robustness



Work done / results

Research Initiation Grant at Instituto de Telecomunicações

- Learning about Federated Learning
- When should be used
- Associated costs
- Contribution to published 4 papers

Last weeks

- Portfolio: https://leoalmpt.pages.dev/
- Review FL papers (Background)
- FL code implementation

Future work / challenges

State of the Art

- Resilient Federated Learning
- Communication Frameworks
- Datasets
- Models

Define

- Requirements
- Evaluation
- Advantages / Disadvantages