

Resilient Federated Learning Framework

Supervisor: Mário Antunes (mario.antunes@ua.pt)

Co-Supervisor: Rui Aguiar (ruilaa@ua.pt)

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. This research investigates the design and evaluation of a resilient FL framework capable of adapting to dynamic network conditions and handling fluctuations in the number of participating devices. By systematically examining various communication layer architectures, we aim to identify the most suitable options for ensuring efficient and reliable model aggregation, even in the presence of node failures or network partitions.

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. Ultimately, this research seeks to develop a versatile FL system that can operate effectively across a wide range of network environments, from stable enterprise networks to challenging edge computing scenarios.

Work Plan:

- Comprehensive Literature Review
- Thorough FL and communication layers Familiarization
- Solution Design and Implementation
- Solution Evaluation
- Dissertation Writing