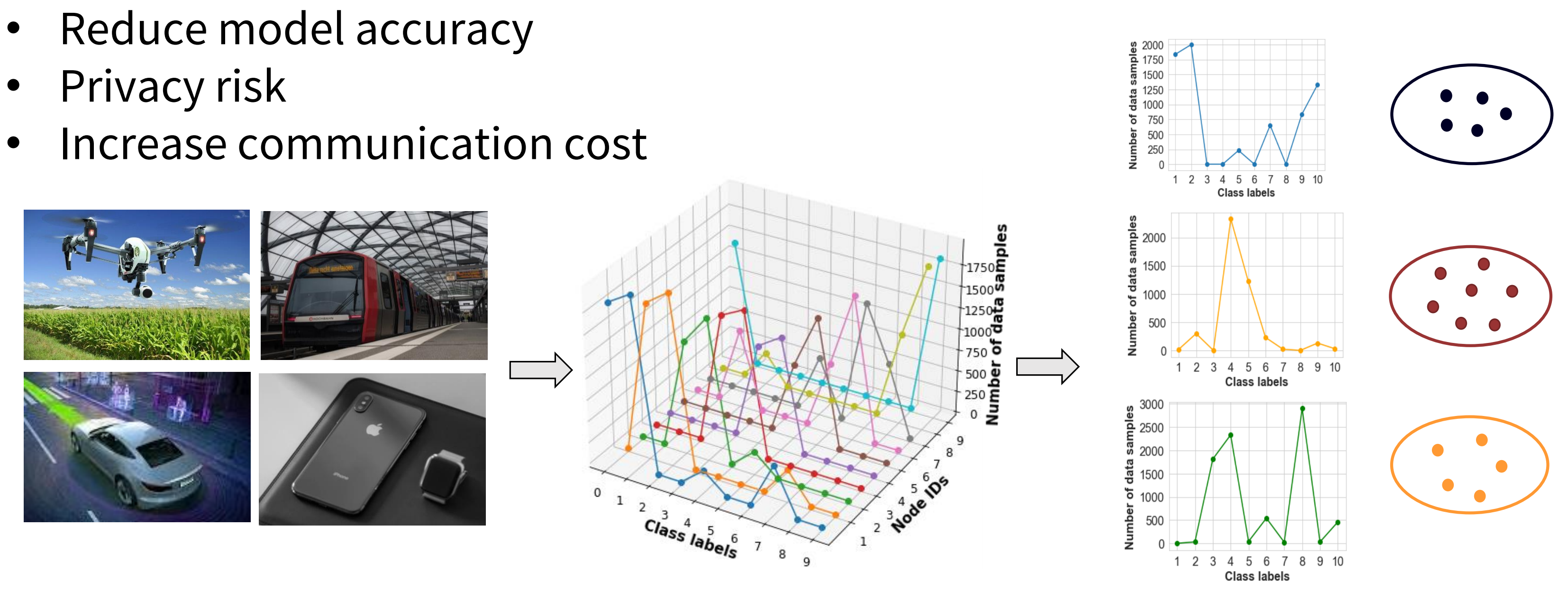
Machine Learning Frameworks for Autonomous System

Lancaster University, UK

Dr. Zhengxin Yu (z.yu8@lancaster.ac.uk)
Prof. Neeraj Suri (neeraj.suri@lancaster.ac.uk)

Heterogenous Data in Autonomous System (AS)

- Distributed nodes in AS contain varied data distribution
- Centralized Machine Learning (ML) frameworks:
  - Reduce model accuracy
  - Privacy risk
  - Increase communication cost

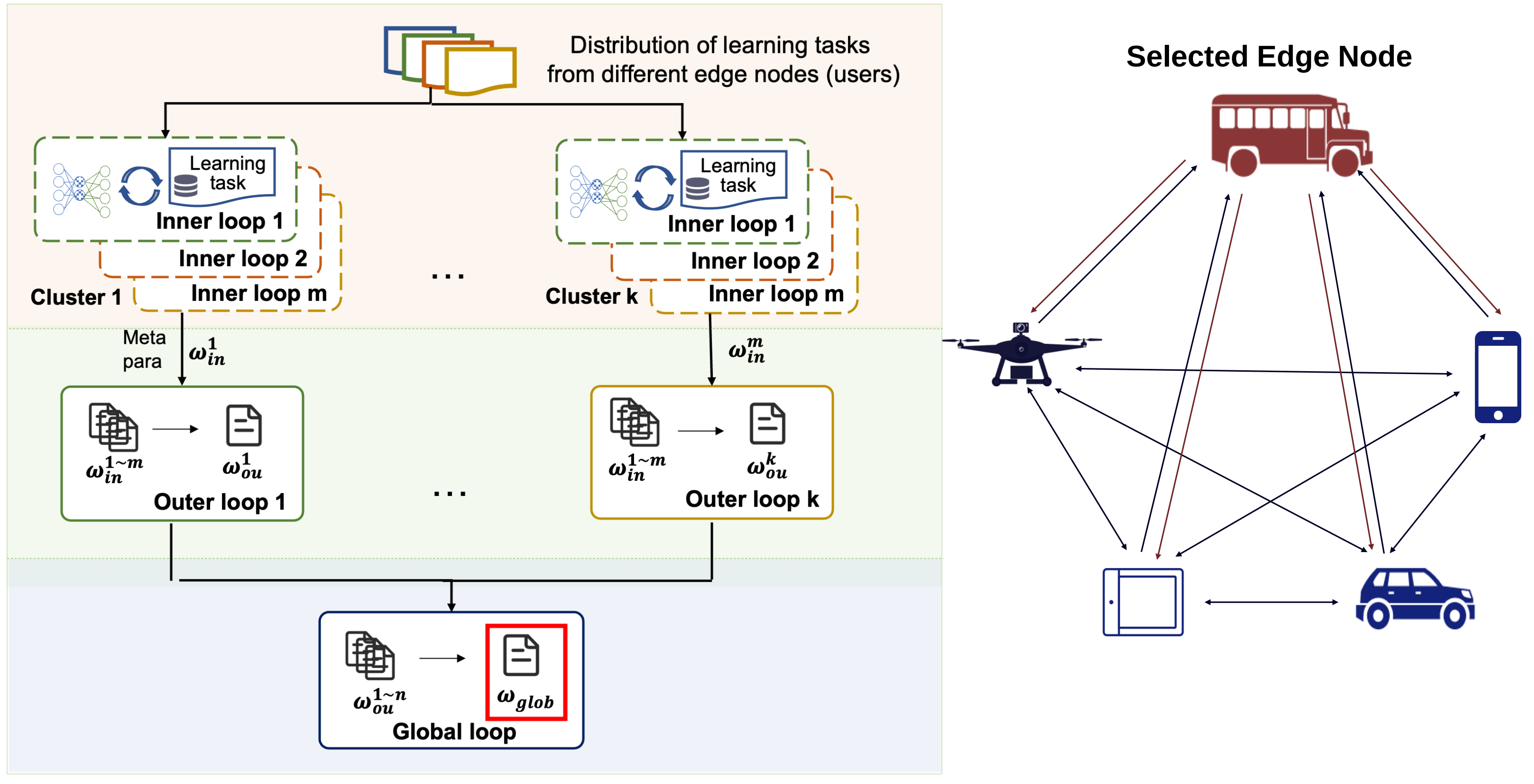


Adaptive and Hierarchical Peer-to-Peer Federated Meta-Learning Framework

Develop a **hierarchal federated meta-learning** framework to adaptively match the characteristics of heterogeneous data (PPFM)

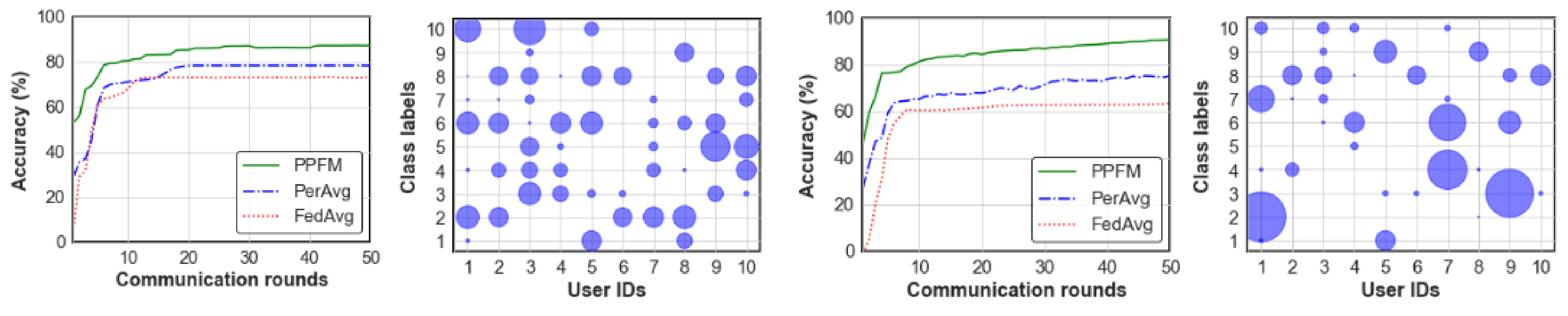
Contributions:

- A novel hierarchal meta-learning architecture
  - Generate multiple learning loops to match different data distribution
- A peer-to-peer federated learning approach
  - Ease reliance on the fixed central server
- A federated learning based data clustering method



Experimental results:

PPFM improves accuracy and efficiency over the state-of-art approaches



(a) Synthetic Dataset 1 (γ = 0.1)

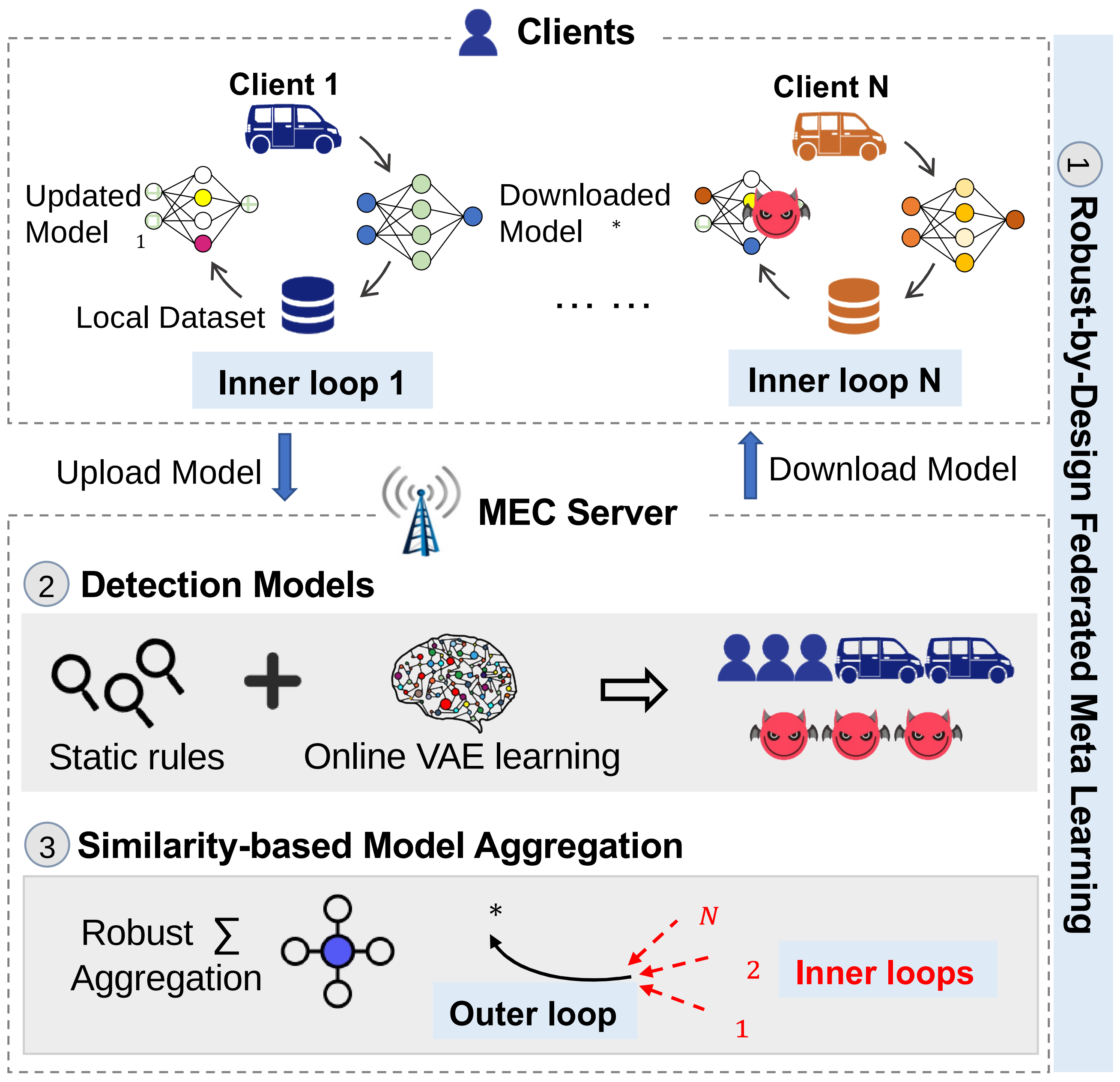
(b) Synthetic Dataset 2 (γ = 0.3)

Robust Federated Meta Learning Framework

Develop a **robust and adaptive** federated meta-learning framework against adversaries (RAFL)

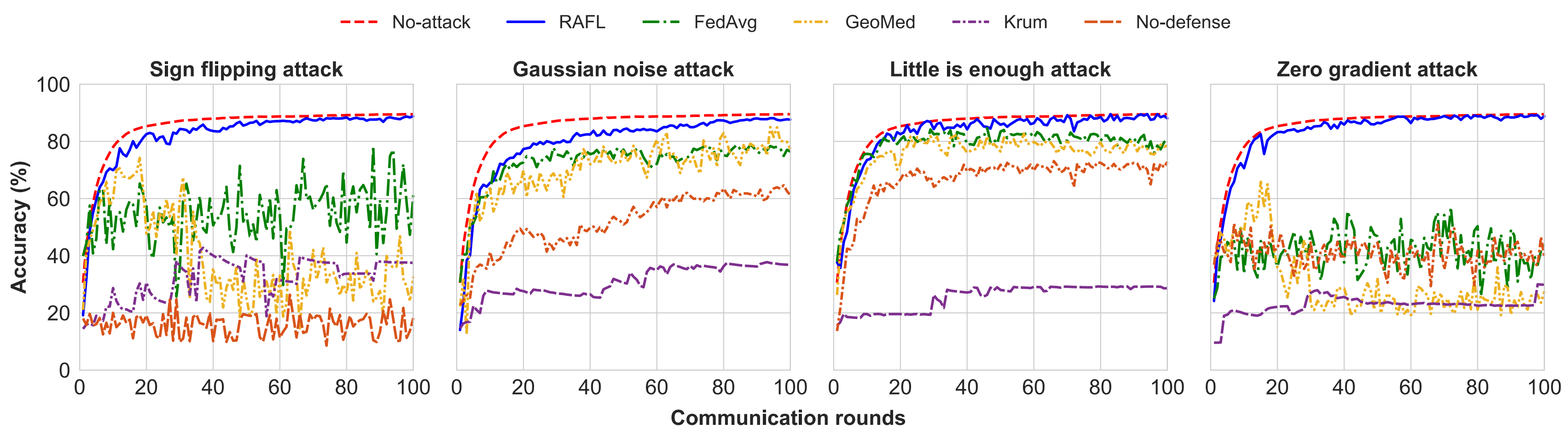
Contributions :

- A robust-by-design federated meta-learning architecture
  - Adaptively defend against a range of adversarial attacks.
- A composite rule-based and learning-based detection method
  - Identify adversaries via ranking domain and low-dimensional embeddings.
- An adaptive model aggregation method
  - Aggregate the global model by considering the degree of similarity between the meta-model and calculated mean model to resilience attacks.



Experimental results:

RAFL is robust by design and outperforms other baseline defensive methods against adversaries in terms of model accuracy and efficiency

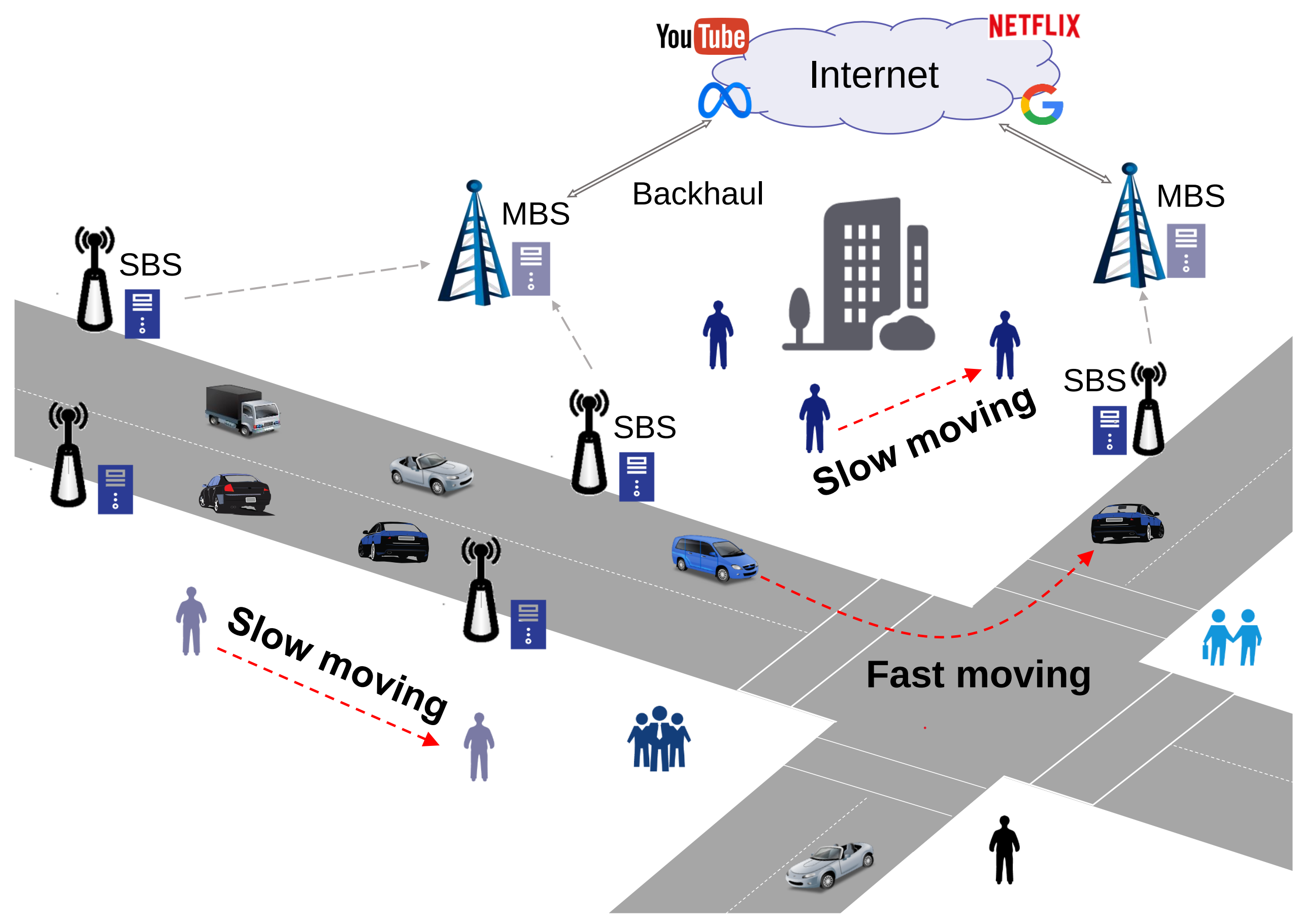


Mobility-aware Federated Learning Framework

Develop a **mobility-aware federated meta-learning** framework to reduce the impact of node mobility

Contributions:

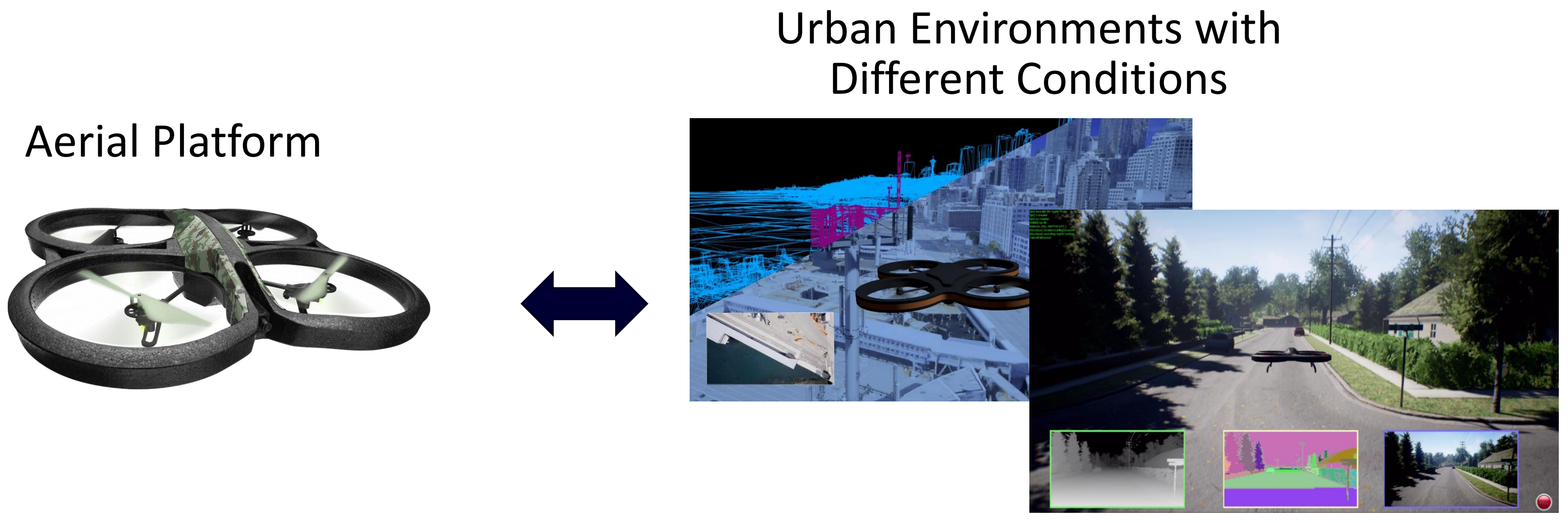
- A novel federated split learning architecture
  - Address the fast changing data distribution
- A semantic-based clustering approach
  - Quick assign edge nodes with non-IID dataset into different distribution



Case Study: Federated Meta Reinforcement Learning for UAV Navigation

Federated Learning-based Visual Odometry Framework

- Combining the AI-based solutions with classical filter-based approach
- Utilising RAFL framework to improve pose estimation accuracy
- Aggregating models trained in different environments and conditions



This work is supported by the Engineering and Physical Sciences Research Council [grant number: EP/V026763/1]