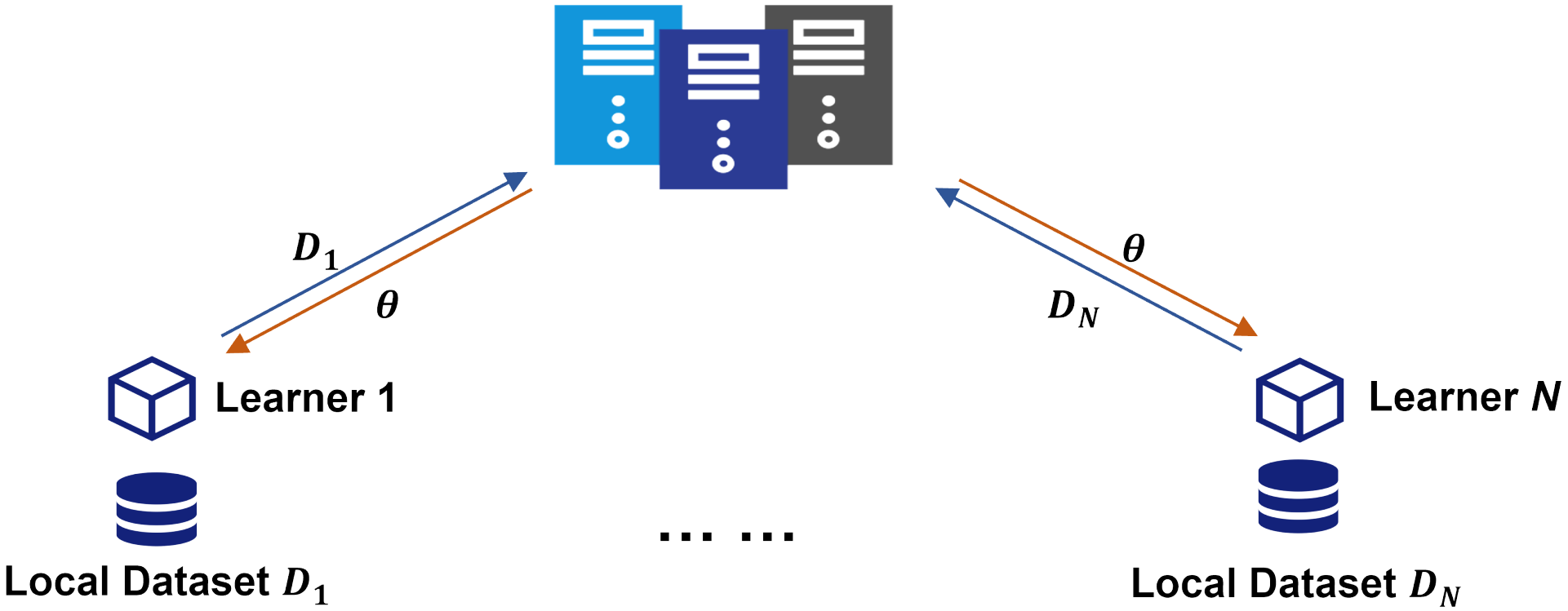
Adaptive and robust federated learning

Yang Lu

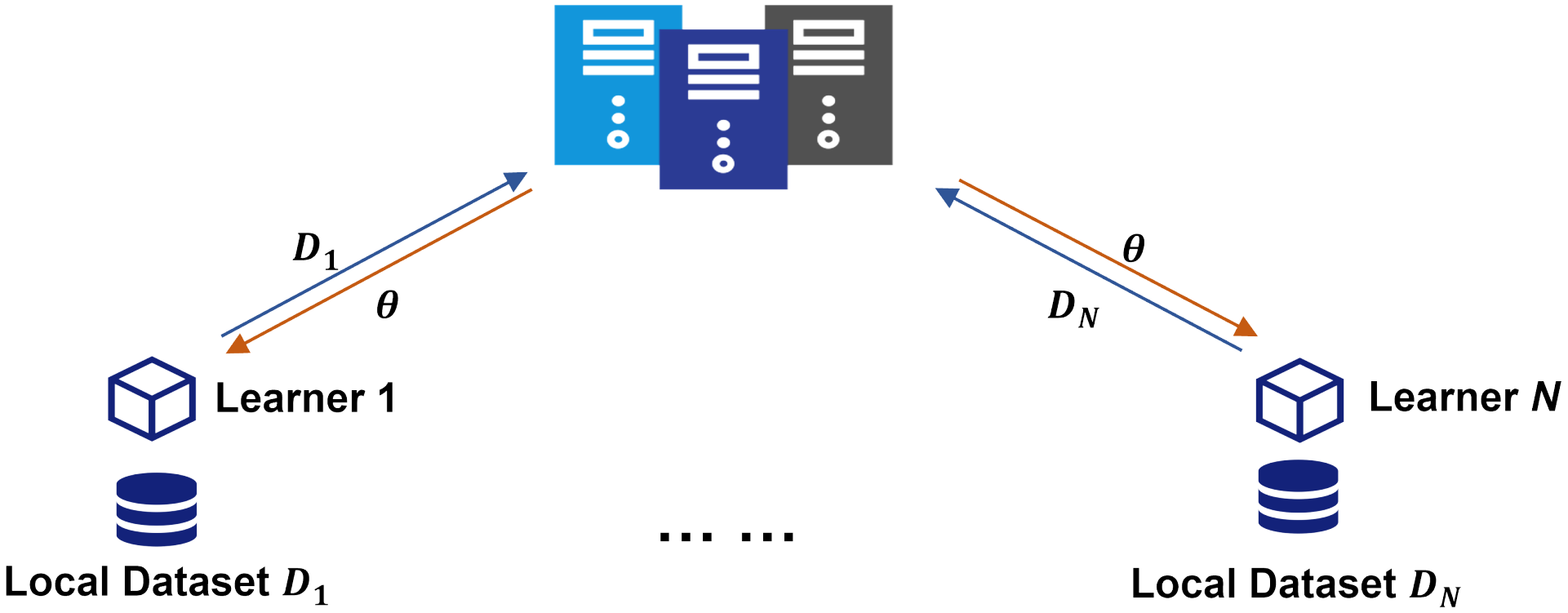
School of Computing and Communications
Lancaster University

11 March, 2024

Traditional multi-agent machine learning

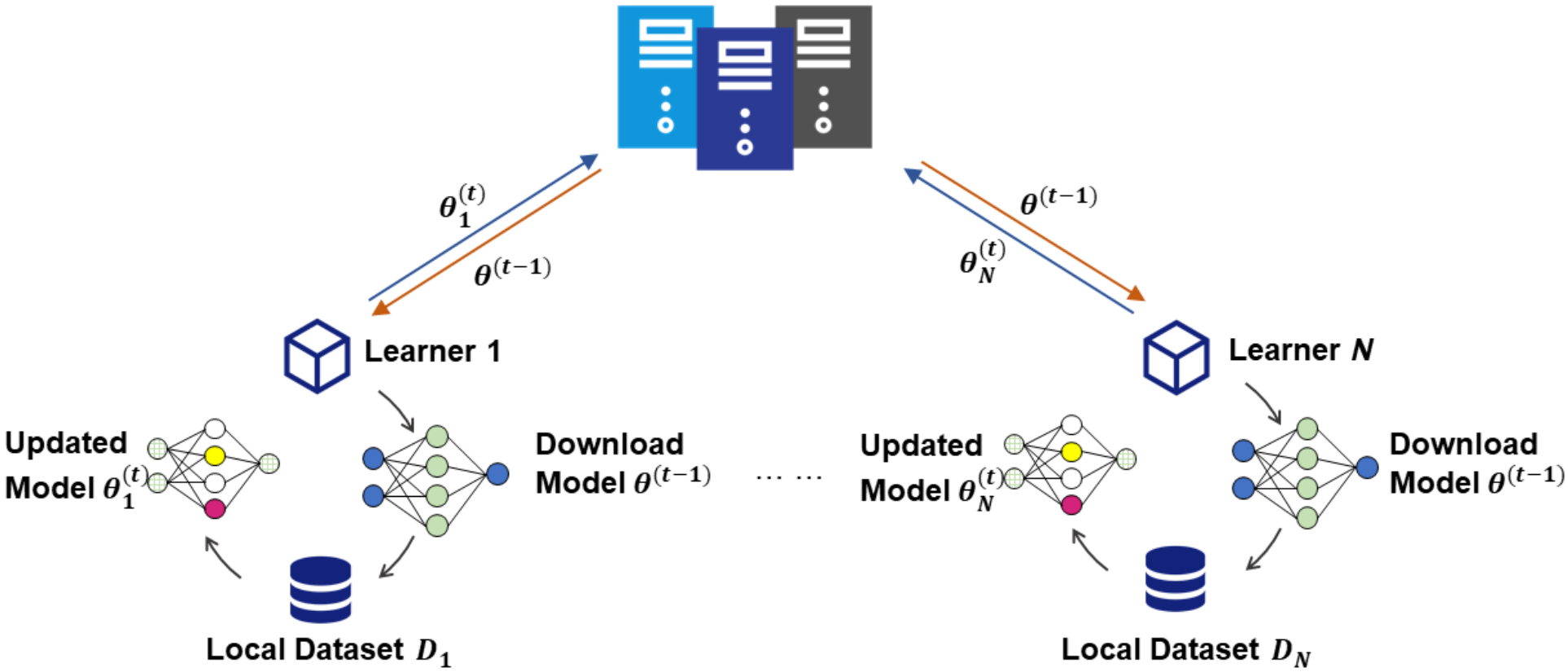


Traditional multi-agent machine learning

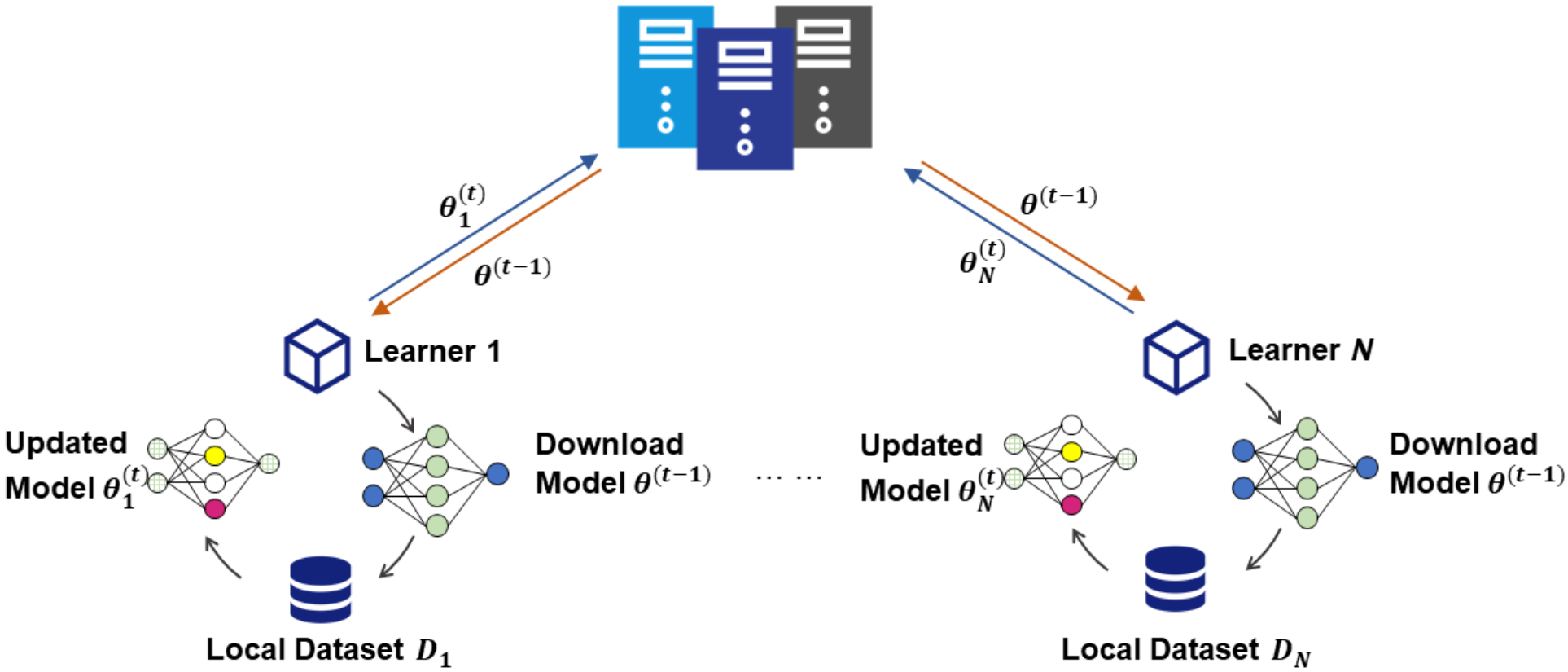


- Leakage of learners' local datasets D_i
- Burdens on the server

Federated learning

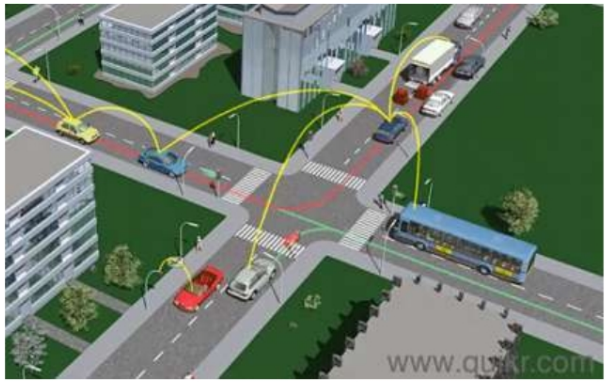


Federated learning



- Local datasets D_i never leave their owners' devices
- Training is distributed at learners' side

Ubiquitous applications

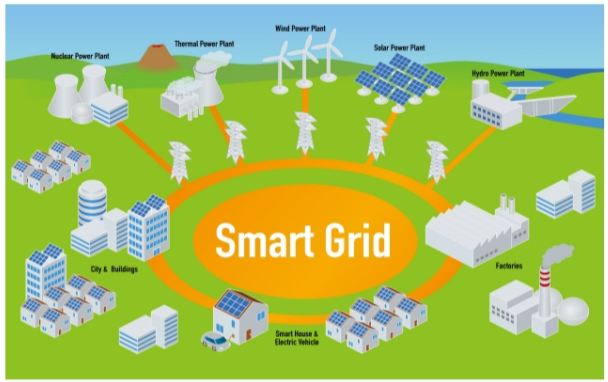


Intelligent Transportation Systems

Information Technologies

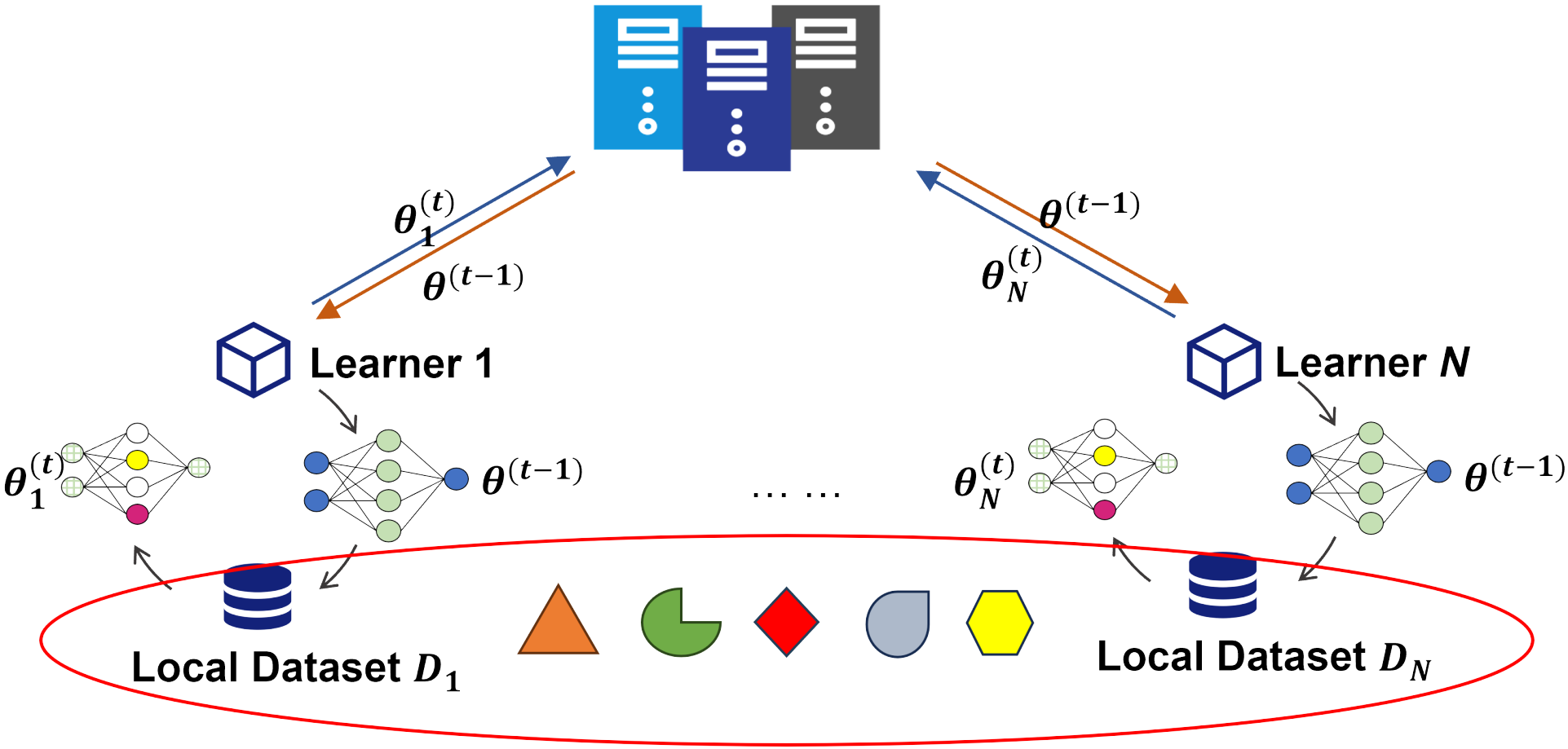
Smart Buildings

Multi-Robot Systems

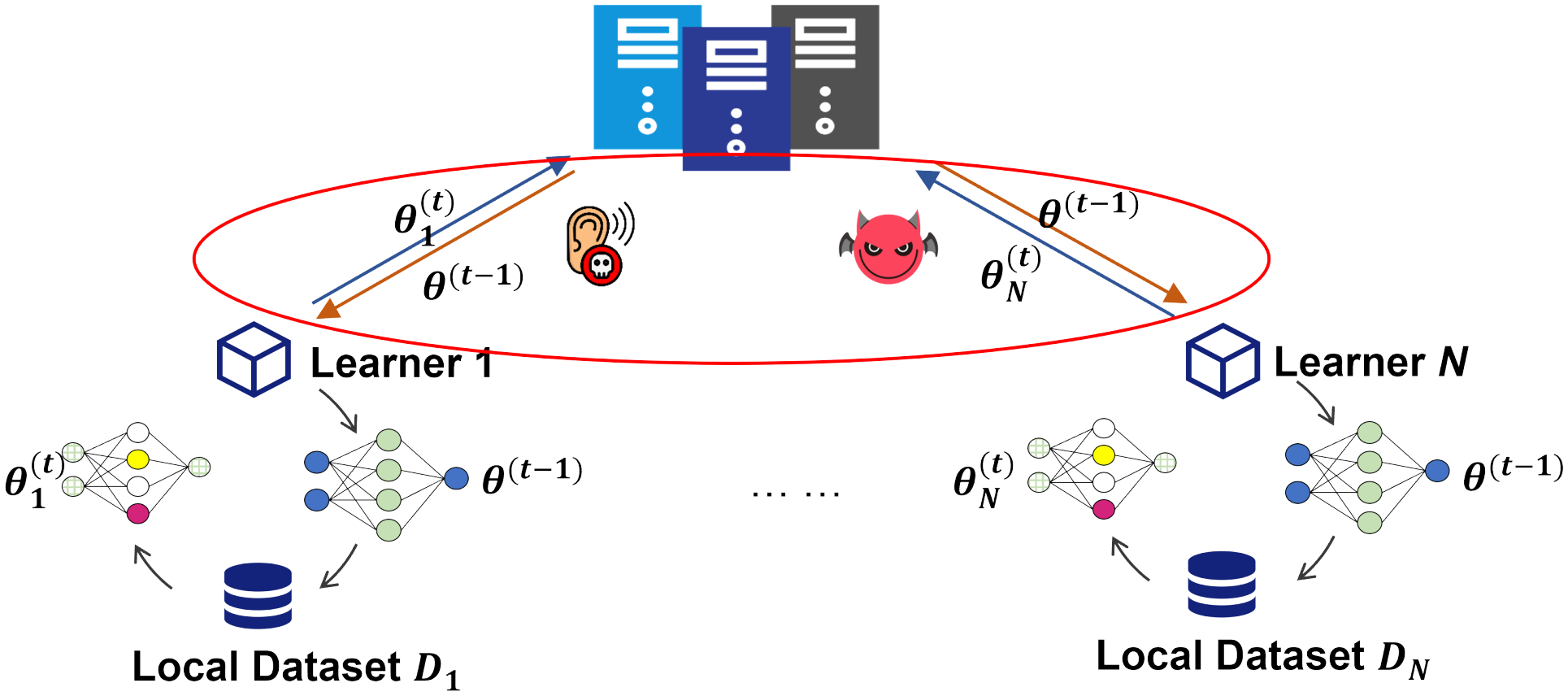


Smart Grid

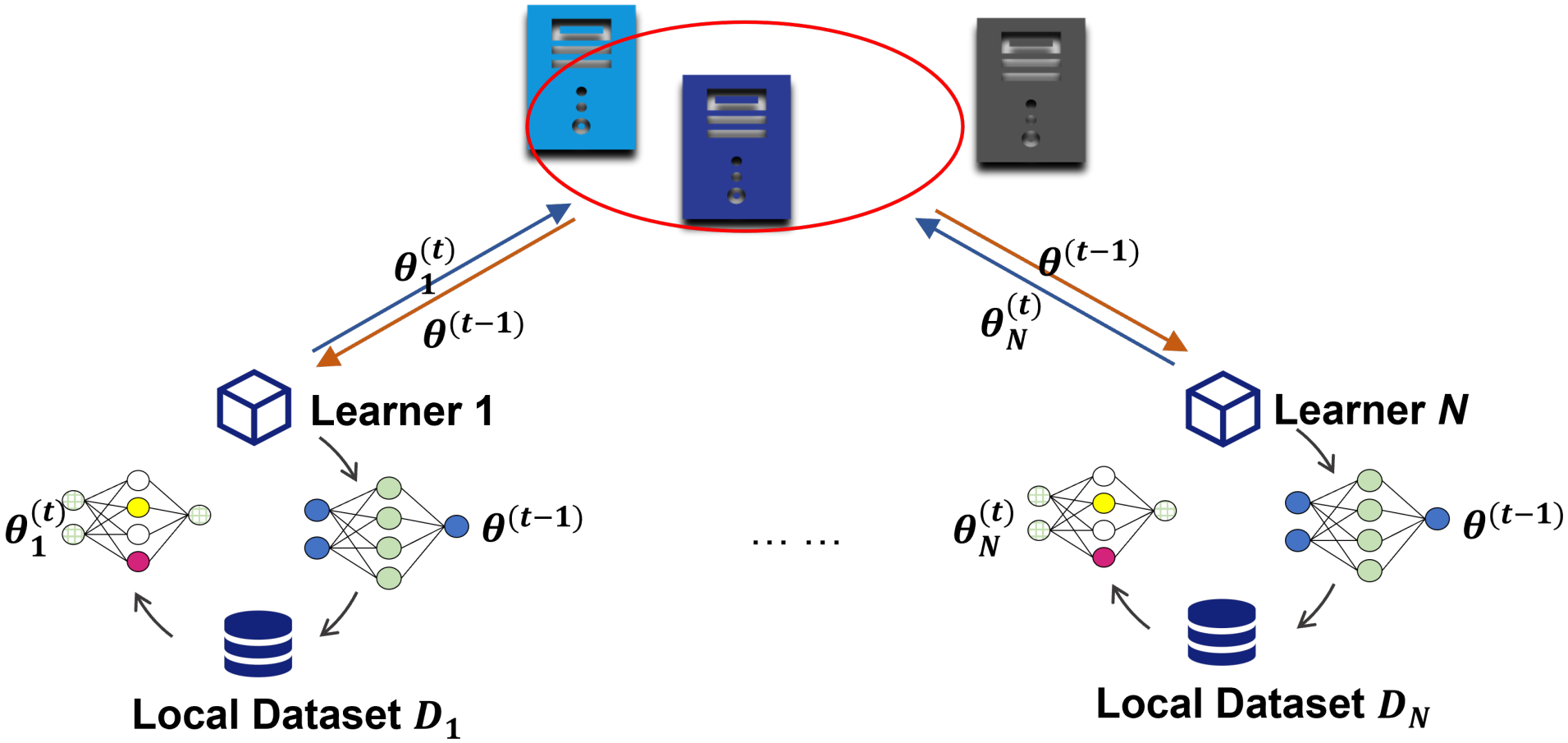
Limitations



Limitations

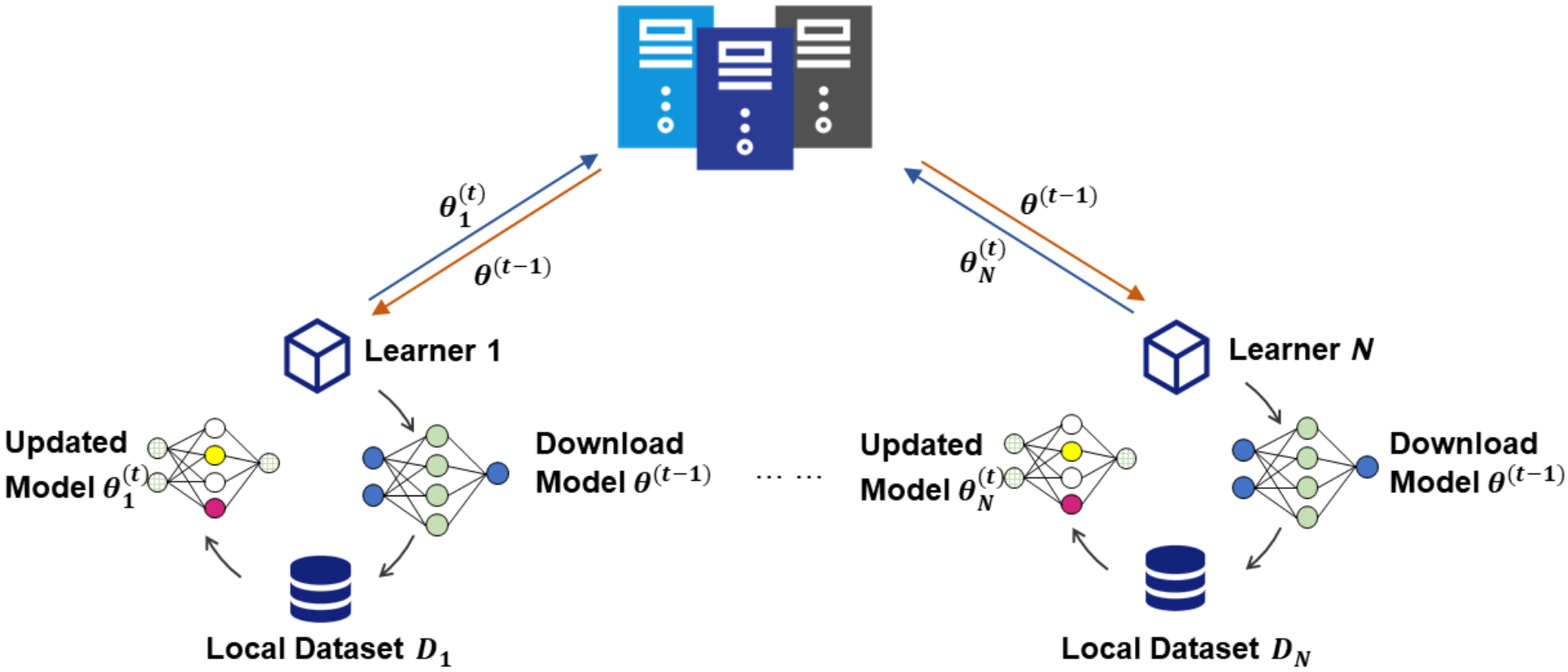


Limitations



Outline

Challenges with federated learning



- Data in edge nodes
  - Highly heterogeneous
  - Dynamic
  - Limited data size
- Learning scheme
  - Only train a single common global model
  - Rely on a fixed central server

Objectives

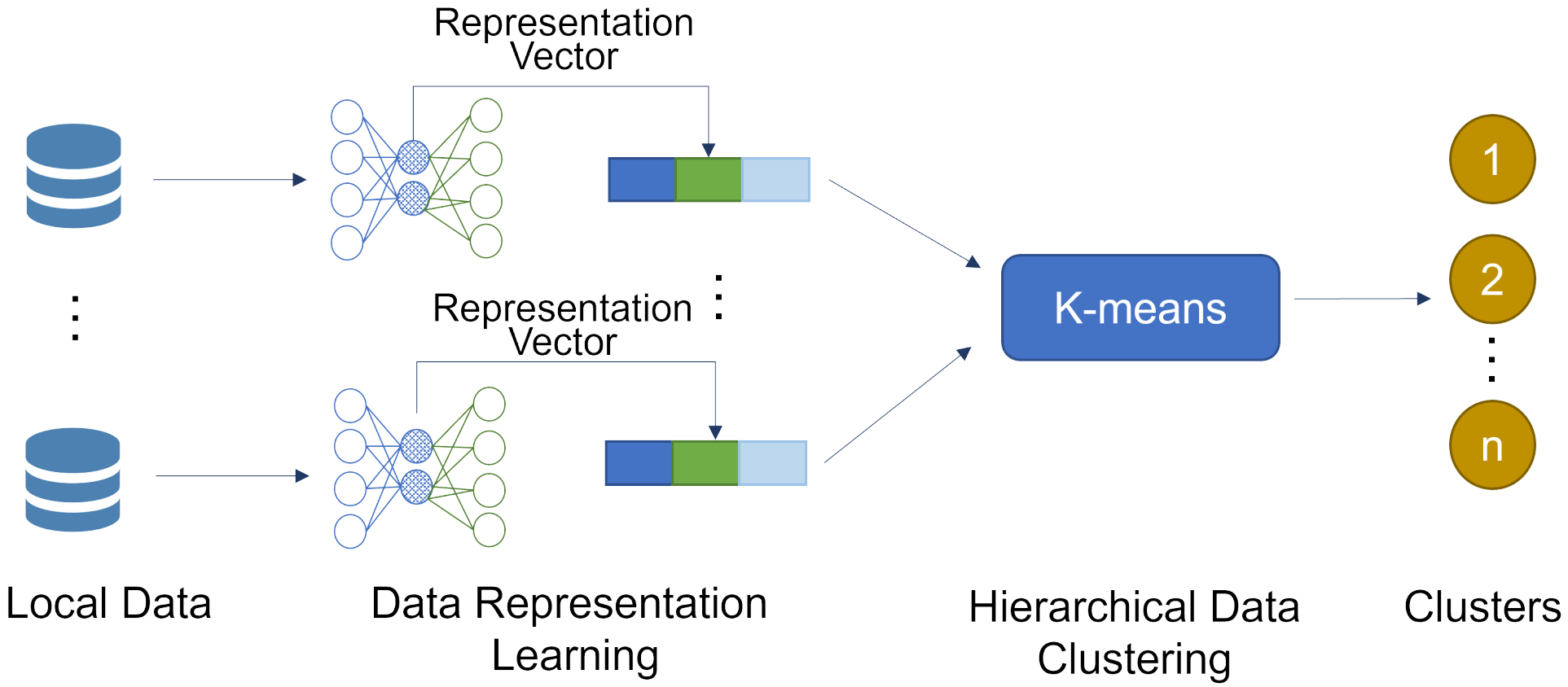
An adaptive and hierarchical federated Meta-learning framework

- Adaptively match characteristics of heterogeneous and dynamic data
  - Dynamically generate data clusters
- Train personalized models for edge nodes
  - Generate multiple hierarchical learning loops
- Remove reliance on a fixed central server
  - Dynamically pick edge nodes to serve as central server

Z. Yu, Y. Lu, P. Angelov, and N. Suri. PPFM: An Adaptive and Hierarchical Peer-to-Peer Federated Meta-Learning Framework. *The 18th International Conference on Mobility, Sensing and Networking (MSN)*, pages: 502–509, December, 2022. Best Paper Award.

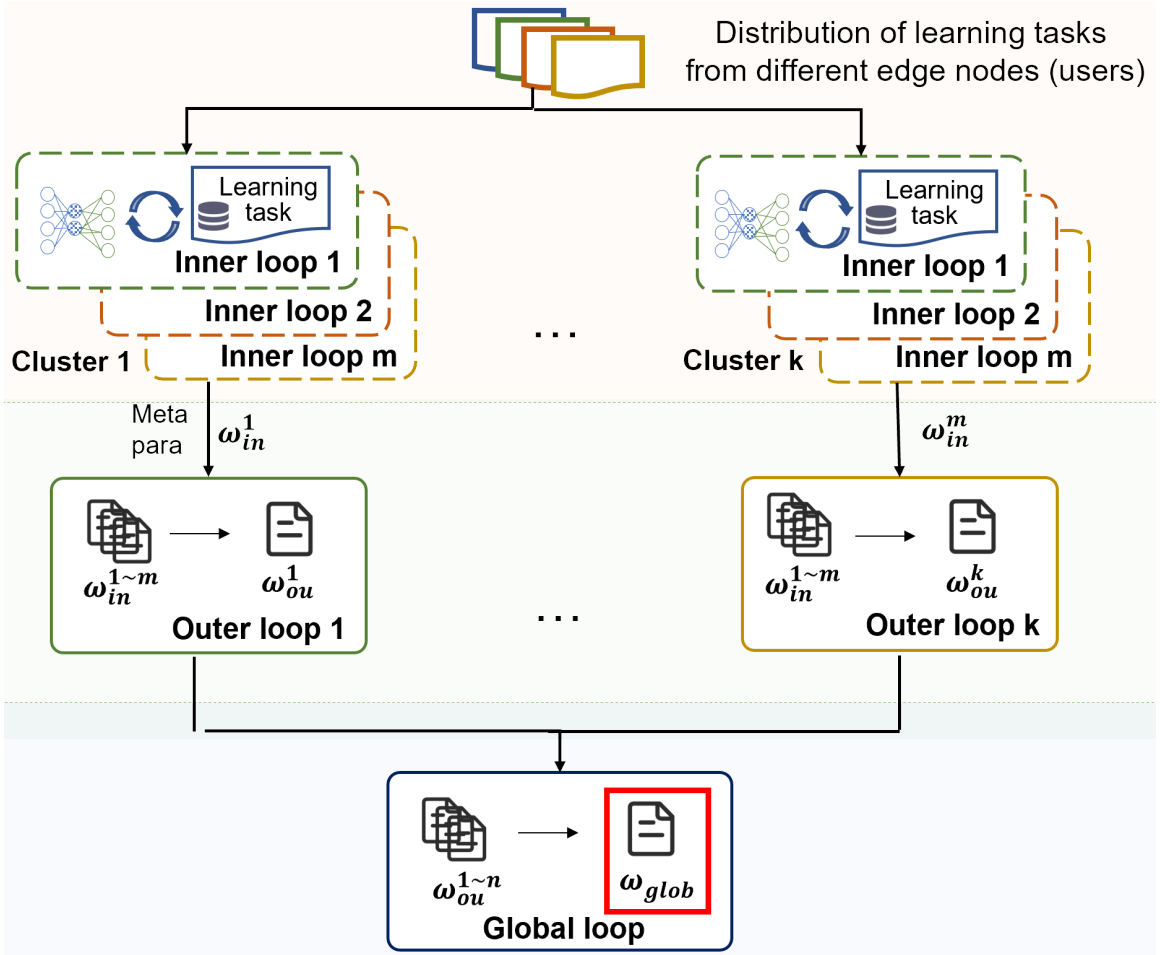
Data clustering

- Kullback-Leibler divergence based K-means clustering
- Representation vectors are obtained from variational autoencoders

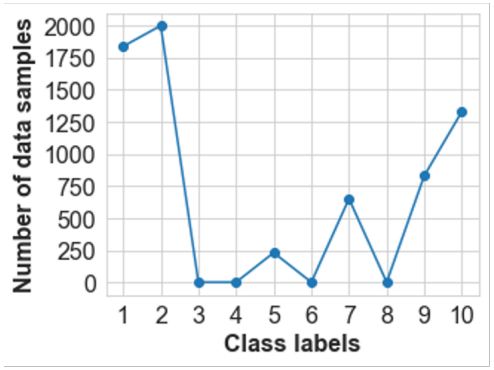


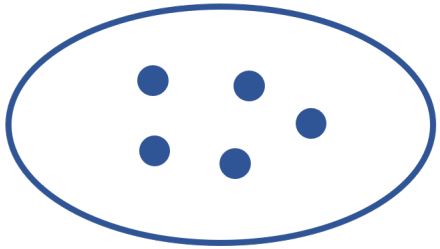
Hierarchical Meta-learning architecture

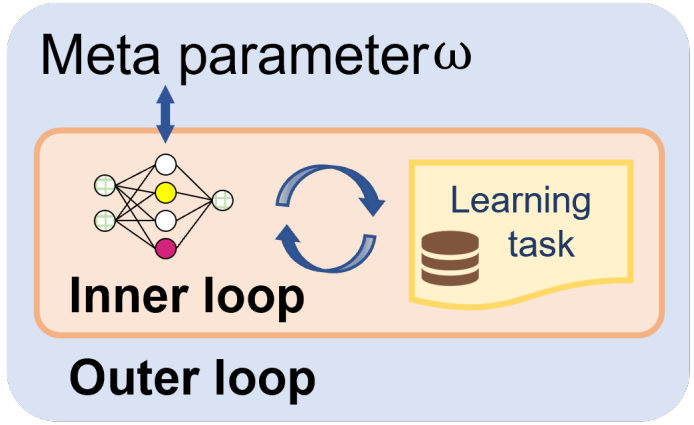
- Inner loop
  - Train task-specific models with local data
- Outer loop
  - Extract common features from similar tasks
  - Optimize adaptability of similar tasks
- Global loop
  - Extract global knowledge across clusters
  - Optimize generalizability across heterogeneous tasks



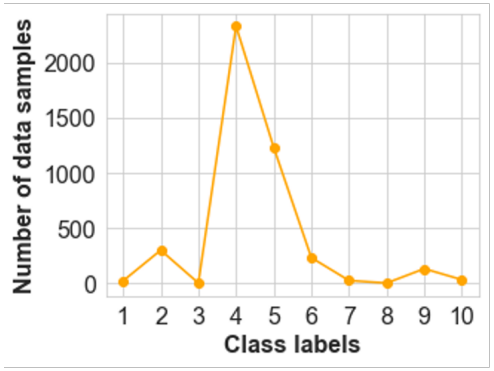
Dynamic clustering and learning loops

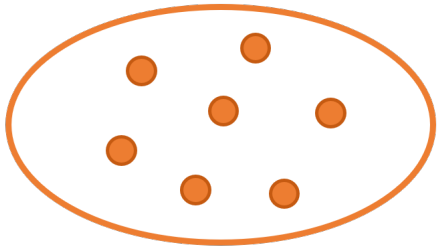


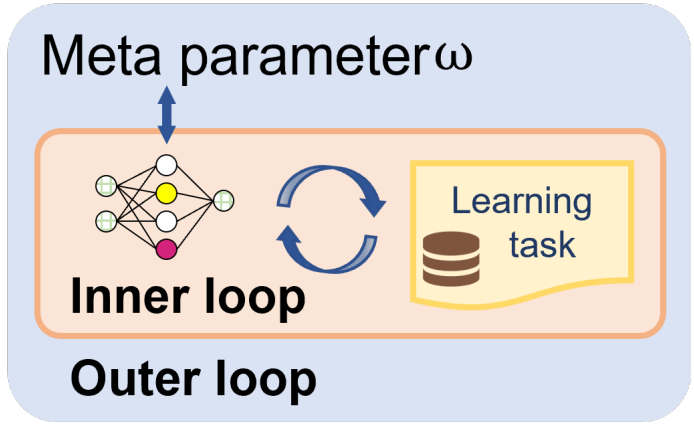




... ...

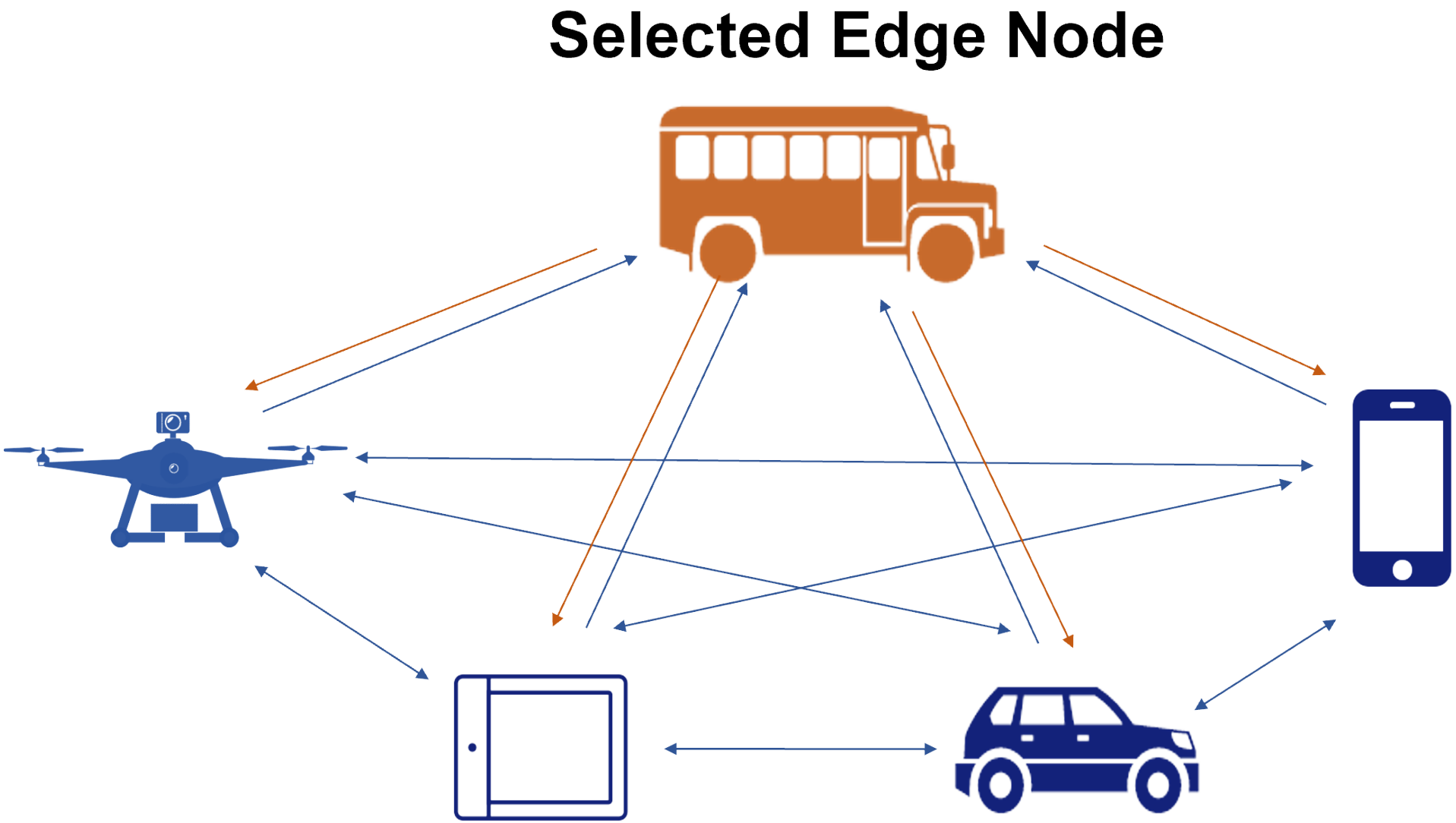






... ...

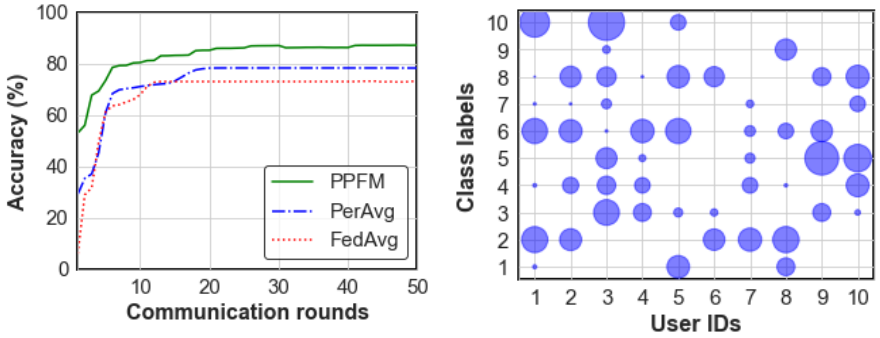
Dynamic central server for federated learning



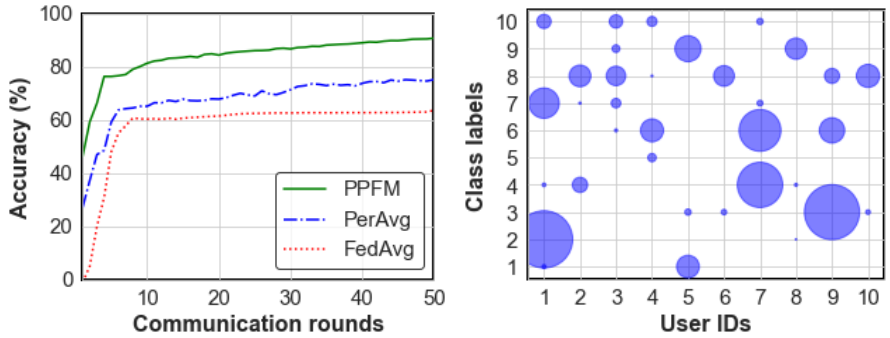
Experimental settings

- Environment
  - Multi-access computing environment: 5-100 edge nodes
  - 3 $\times$ HP Z440 workstations with 64G memory
- Datasets
  - MNIST
  - CIFAR-10
  - Synthetic datasets
- Learning models
  - Feedforward neural network (FNN)
  - Convolutional neural network (CNN)
  - Conditional multinomial logistic regression (CMLR)

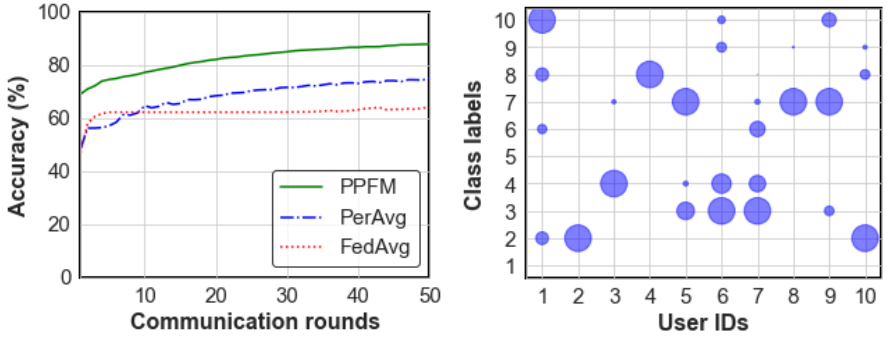
Experimental results: Classification



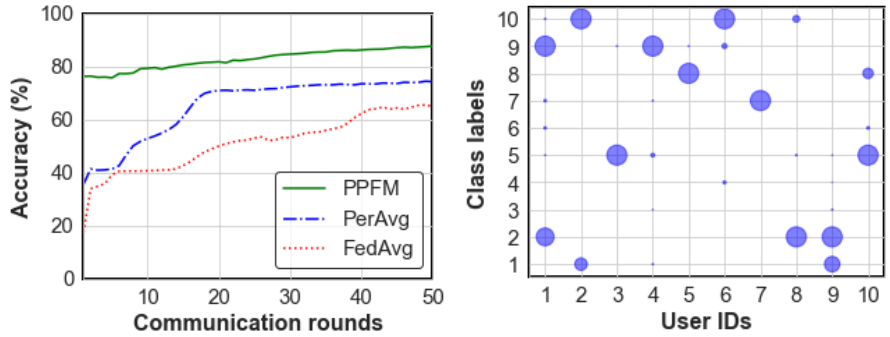
(a) Synthetic Dataset 1 ($\gamma = 0.1$)



(b) Synthetic Dataset 2 ($\gamma = 0.3$)



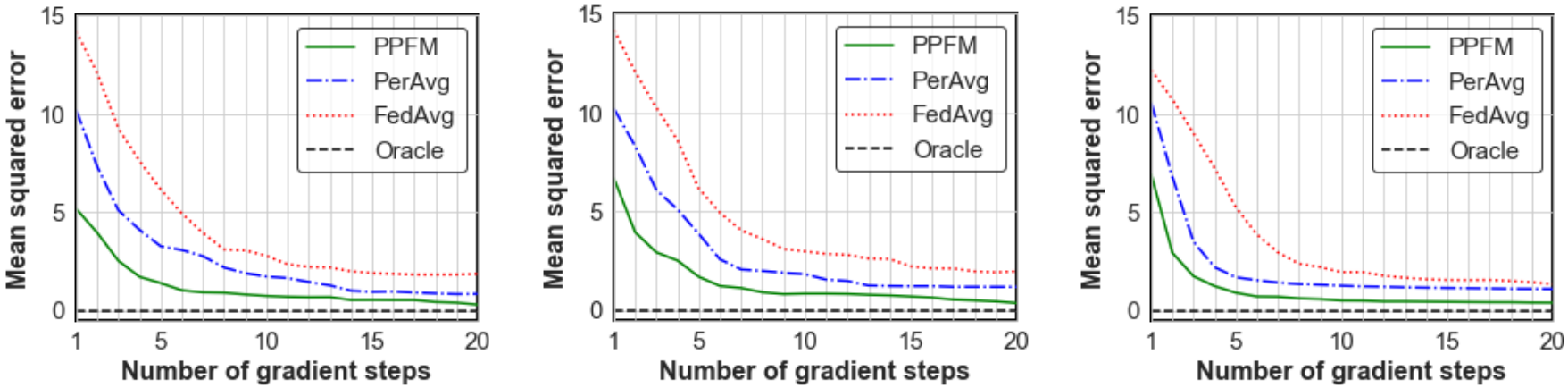
(c) Synthetic Dataset 3 ($\gamma = 0.6$)



(d) Synthetic Dataset 4 ($\gamma = 1$)

PPFM vs. Comparative algorithms (Synthetic Datasets)

Experimental results: Regression



(a) Amplitude = 4.5, phase = 0.44

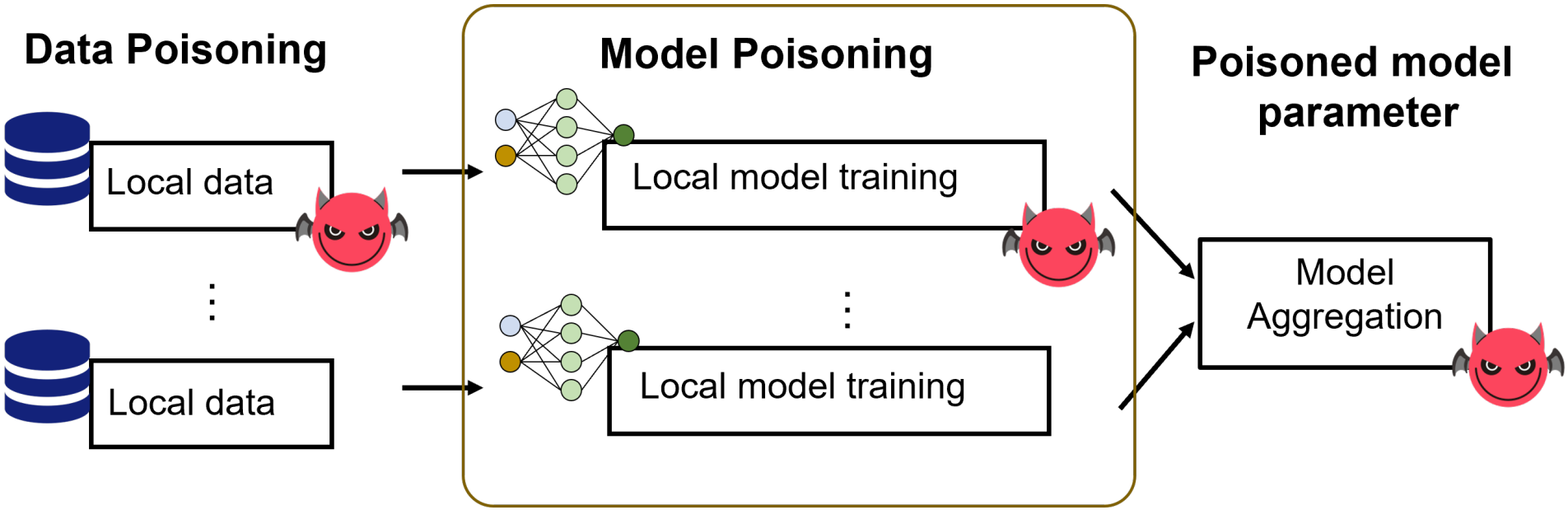
(b) Amplitude = 1.88, phase = 1.65

(c) Amplitude = 0.15, Phase = 1.36

Sinusoid regression results (Synthetic Dataset)

Outline

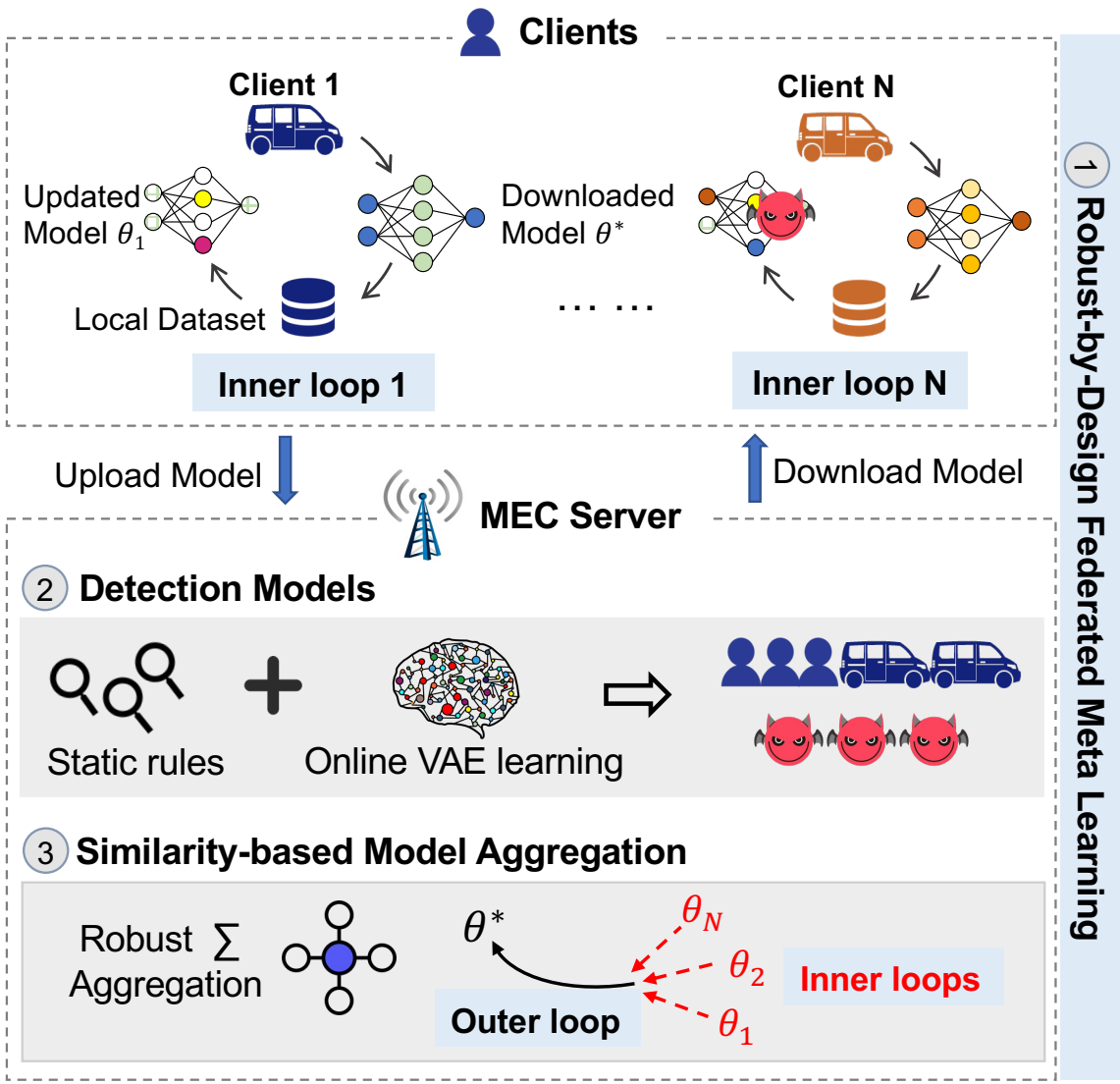
Security for federated learning



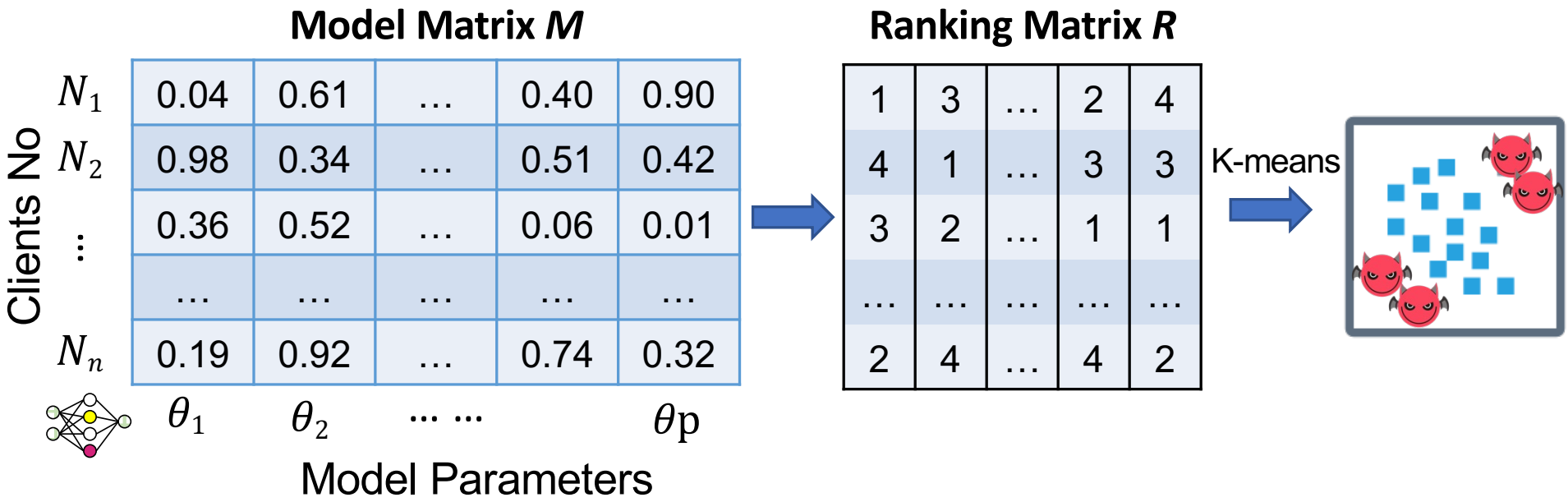
Z. Yu, Y. Lu, and N. Suri. RAFL: A Robust and Adaptive Federated Meta-Learning Framework Against Adversaries. *IEEE 20th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, pages: 496–504, September, 2023.

Robust federated Meta-learning framework

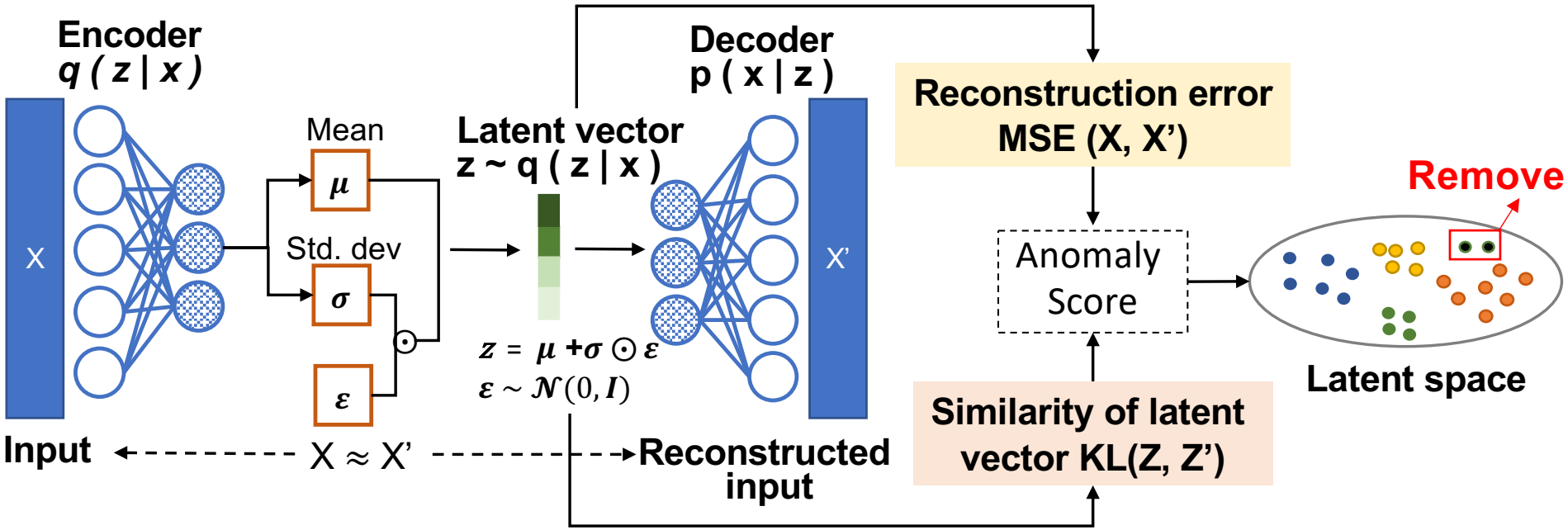
- Robust-by-design federated Meta-learning
- Residual rule-based detector
- VAE-based detector
- Similarity-based aggregation



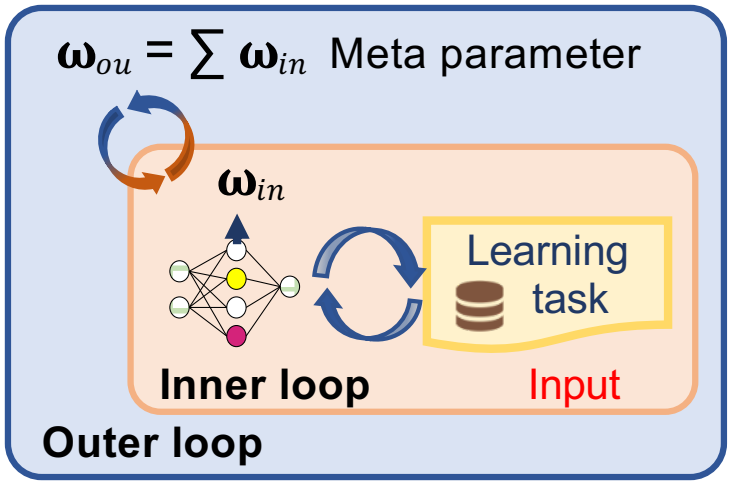
Residual rule-based detector

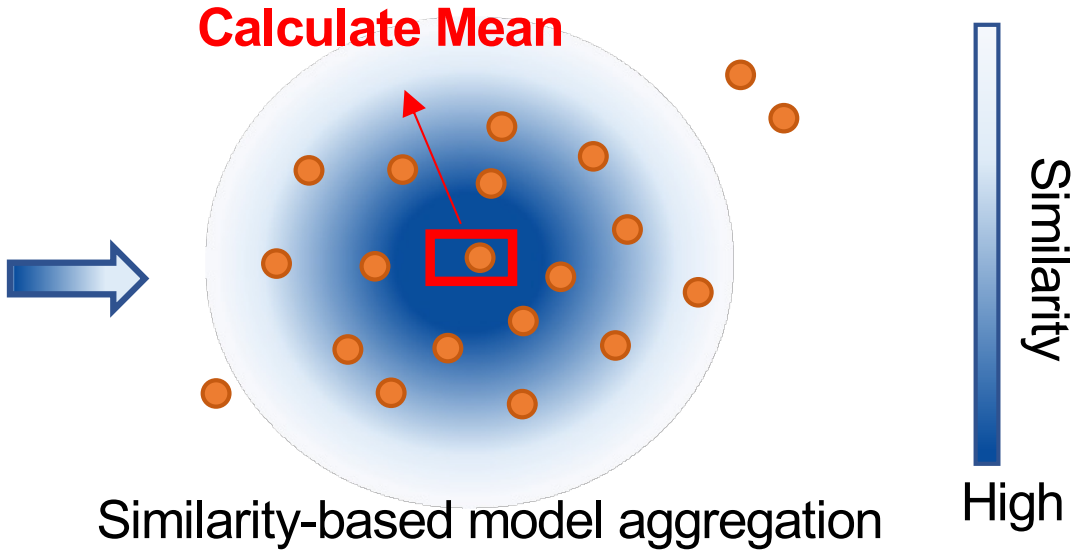


VAE-based detector



Similarity-based aggregation





Experimental settings

- Environment
  - Multi-access computing environment: 100 edge nodes
  - 3 $\times$ HP Z440 workstations with 64G memory
- Datasets
  - MNIST
  - CIFAR-10
- Learning models
  - Feedforward neural network (FNN)
  - Convolutional neural network (CNN)
  - Conditional multinomial logistic regression (CMLR)

Experimental results