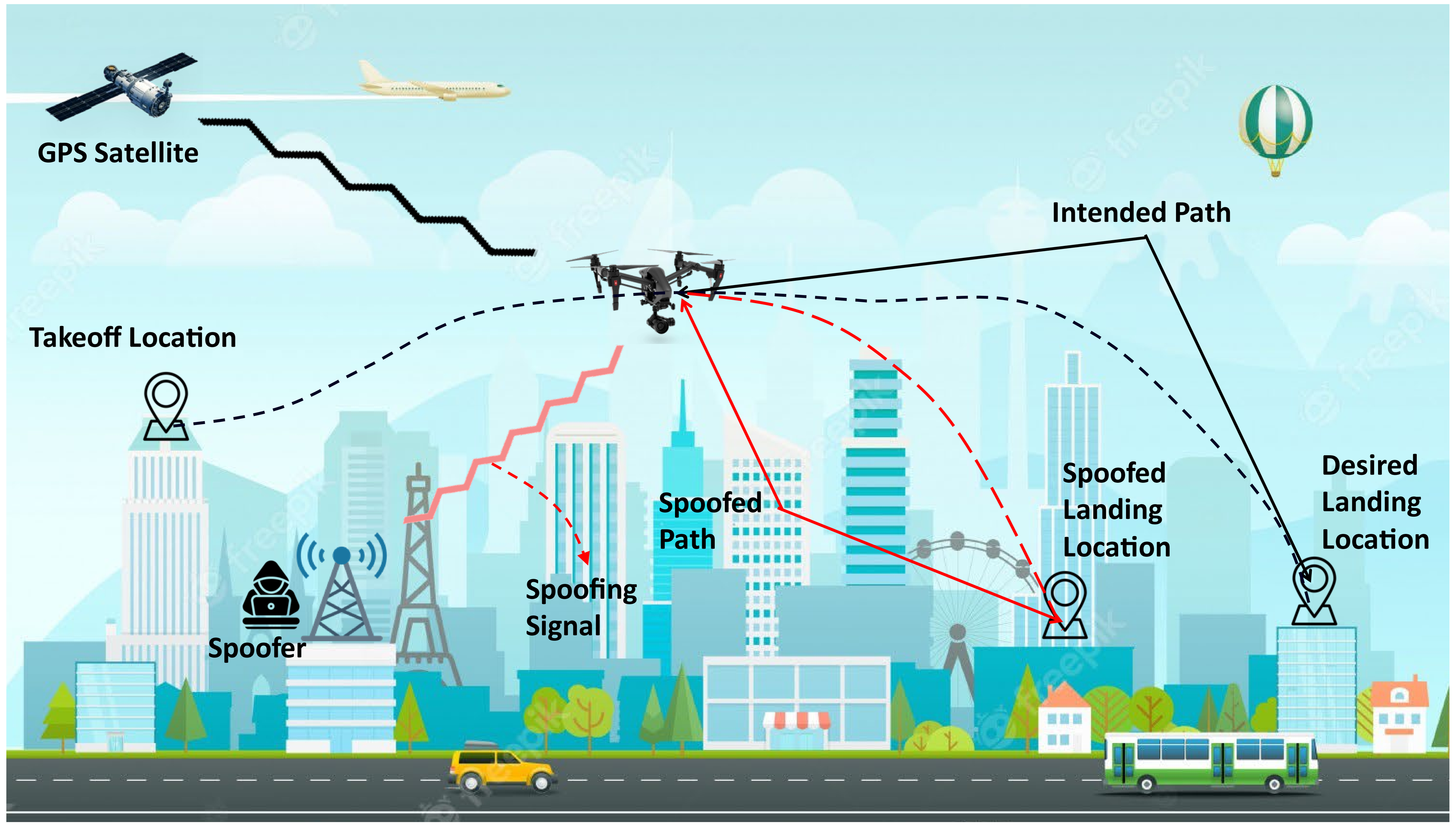
Federated Meta Learning for UAV Visual Navigation in Urban Airspace in the Presence of GPS-Spoofing Attacks

Cranfield University & Lancaster University

Researchers: Dr. Burak Yuksek, Dr. Zhengxin Yu
Investigators: Prof. Gokhan Inalhan, Prof. Neeraj Suri

Visual Navigation for Autonomous Vehicles



Operations in Urban Airspace

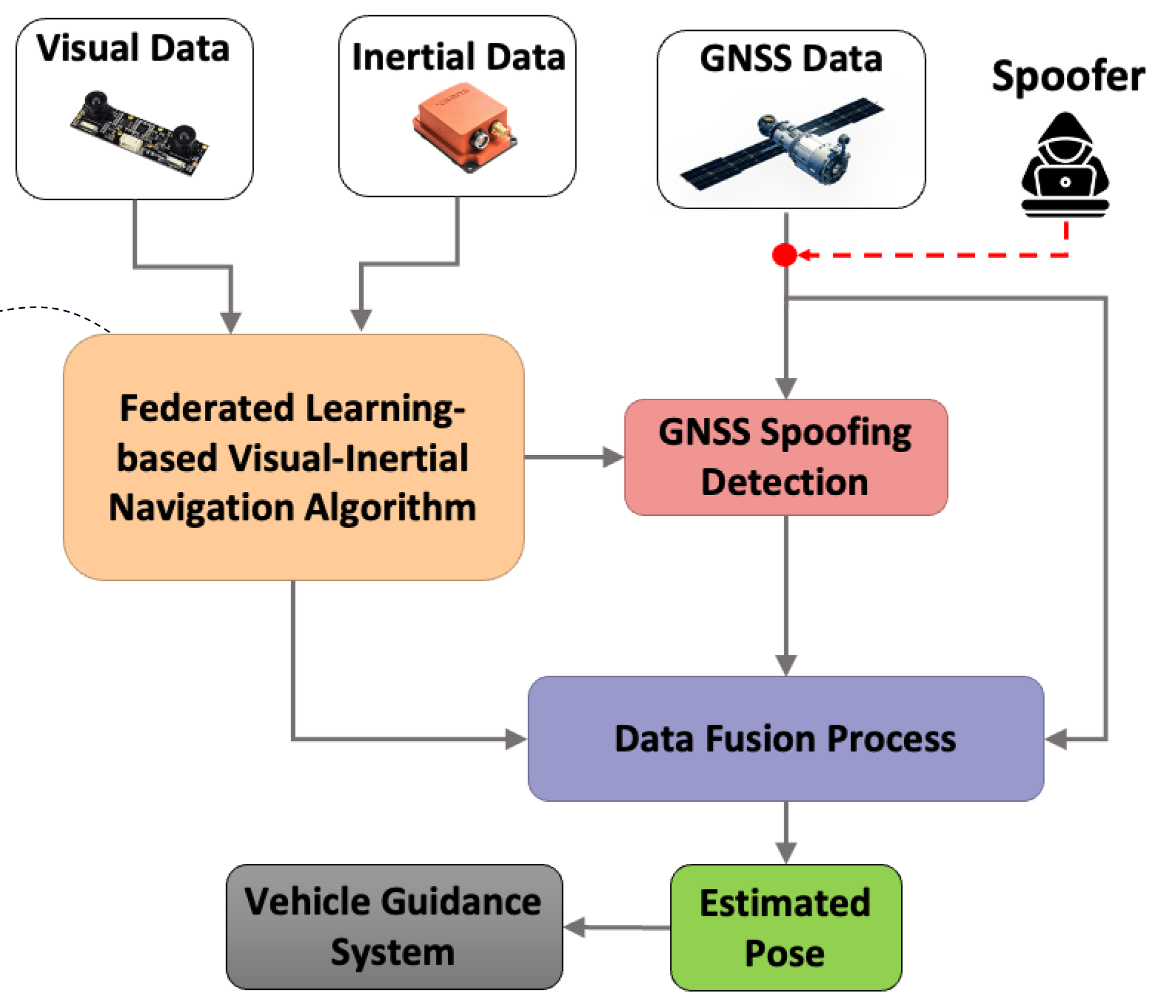
- Require high level of safety
- GNSS is one of the most vulnerable system against cyber-attacks such as jamming and spoofing
- Spoofing attacks are more harmful and difficult to detect
- Measurement errors such as multi-path error should be compensated for high positioning accuracy
- GNSS system should be supported by utilising multi-sensor pose estimation algorithms not only to detect the attacks but also to provide safety for the vehicle.

Design Goals

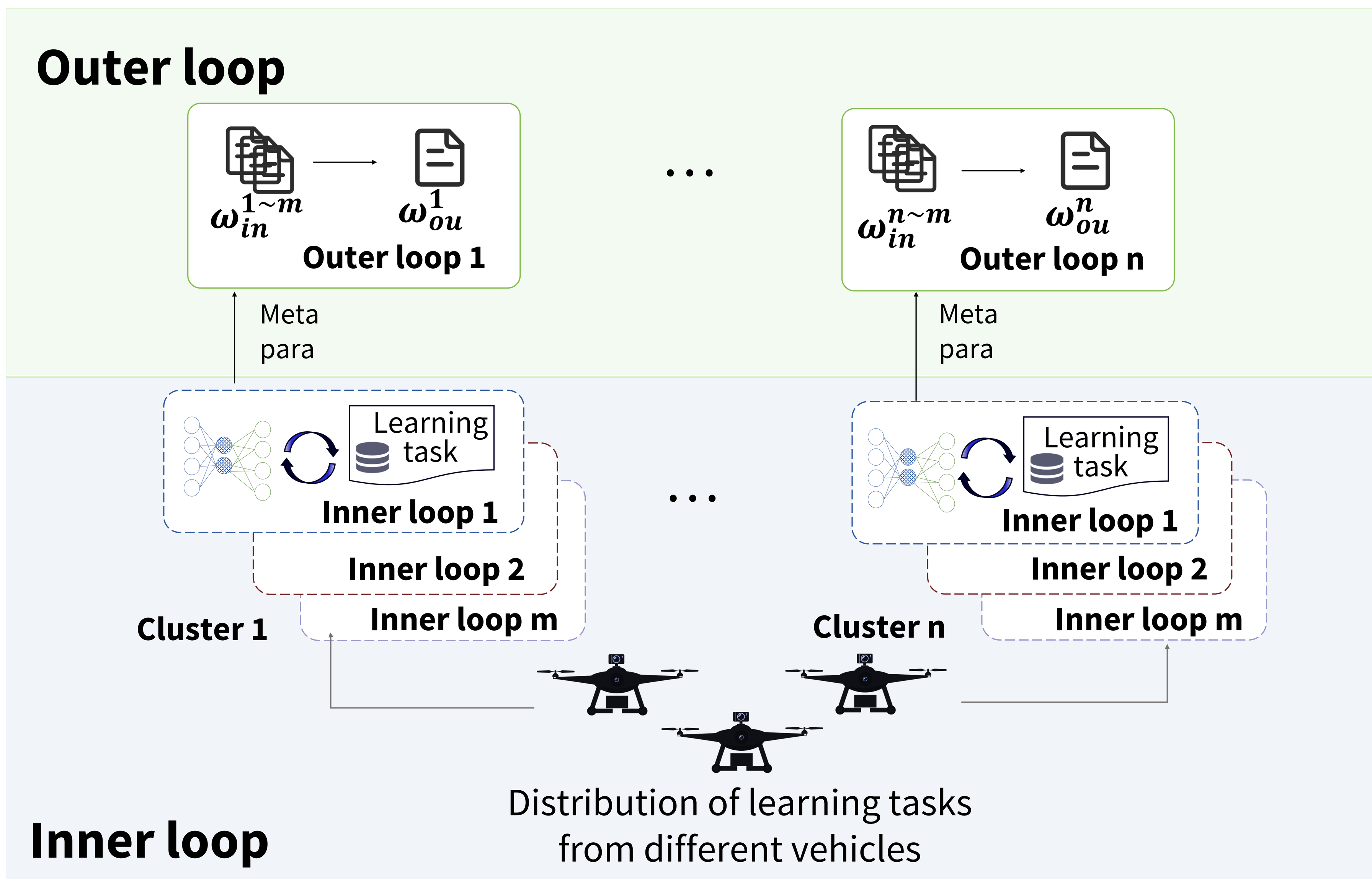
- GNSS-spoofing attack detection
- Increasing pose estimation accuracy
- Generalizability and adaptation for new environments
- Lifelong learning ability

Federated Learning-based Visual Odometry Framework

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

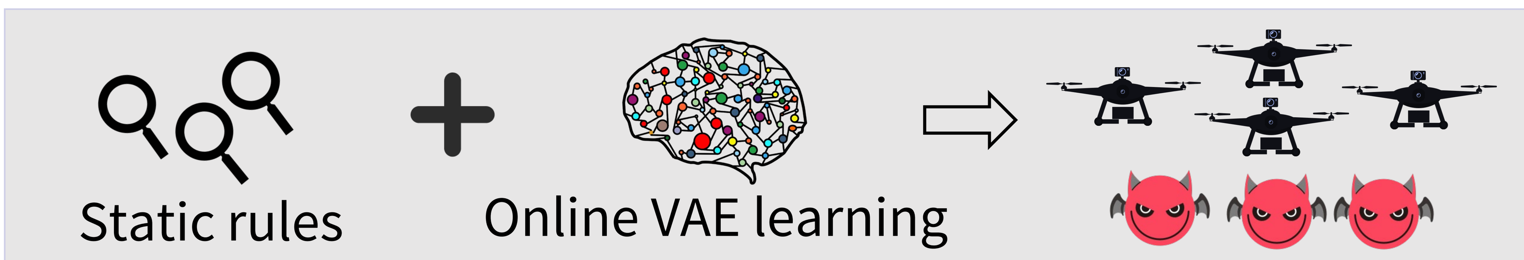


Adaptive and Robust Federated Meta Learning



A P2P federated learning + meta-learning for navigation

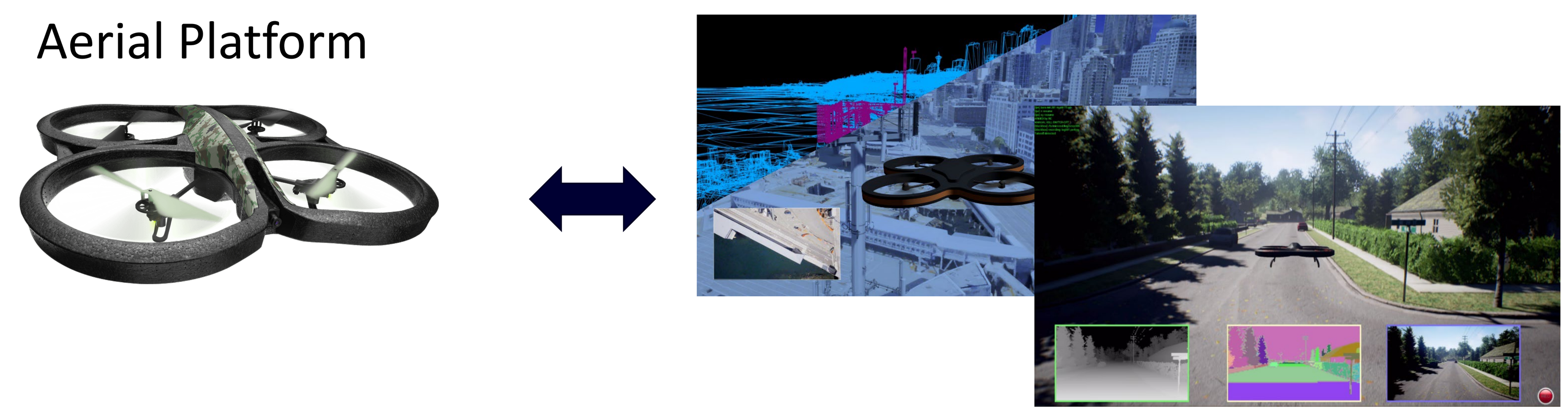
- **An adaptive meta-learning architecture** is proposed to adapt to new environments and enable vehicles to have the lifelong learning capability.
  - Inner loop:
    - Train a task-specific model based on local data
  - Outer loop:
    - Extract common features from similar tasks
    - Optimize meta-model adaptability of similar tasks
- **A robust-by-design federated meta-learning architecture** is developed to adaptively defend against a range of adversarial attacks.
  - A composite rule-based and learning-based detection method to effectively identify adversarial vehicles 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.



Detection Models — Outer loops

Simulation Framework

- Unreal Engine and AirSim
- Nonlinear dynamical model for aerial vehicles
- Realistic sensor models (IMU, GNSS, LIDAR)
- Photorealistic Camera Data Monocular and Stereo
  - Gray scale and RGB



Ongoing and Future Works

- Implementation of the proposed algorithm will be completed.
- Adaptability and transferability will be evaluated in outdoor environments for different weather and light conditions.

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