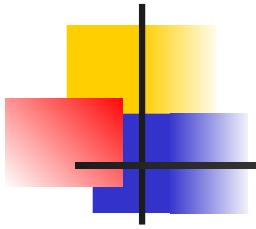


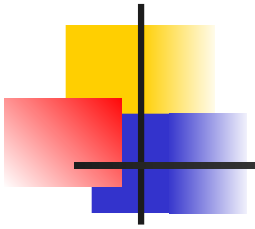
Co-learn - federated learning for IoT

Huawei Network Verification Workshop

Jon Crowcroft,

http://www.cst.cam.ac.uk/~jac22

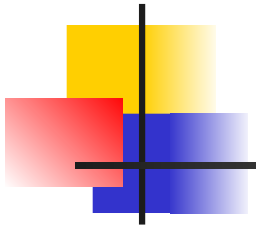
July 29th 2021



Two verification challenges

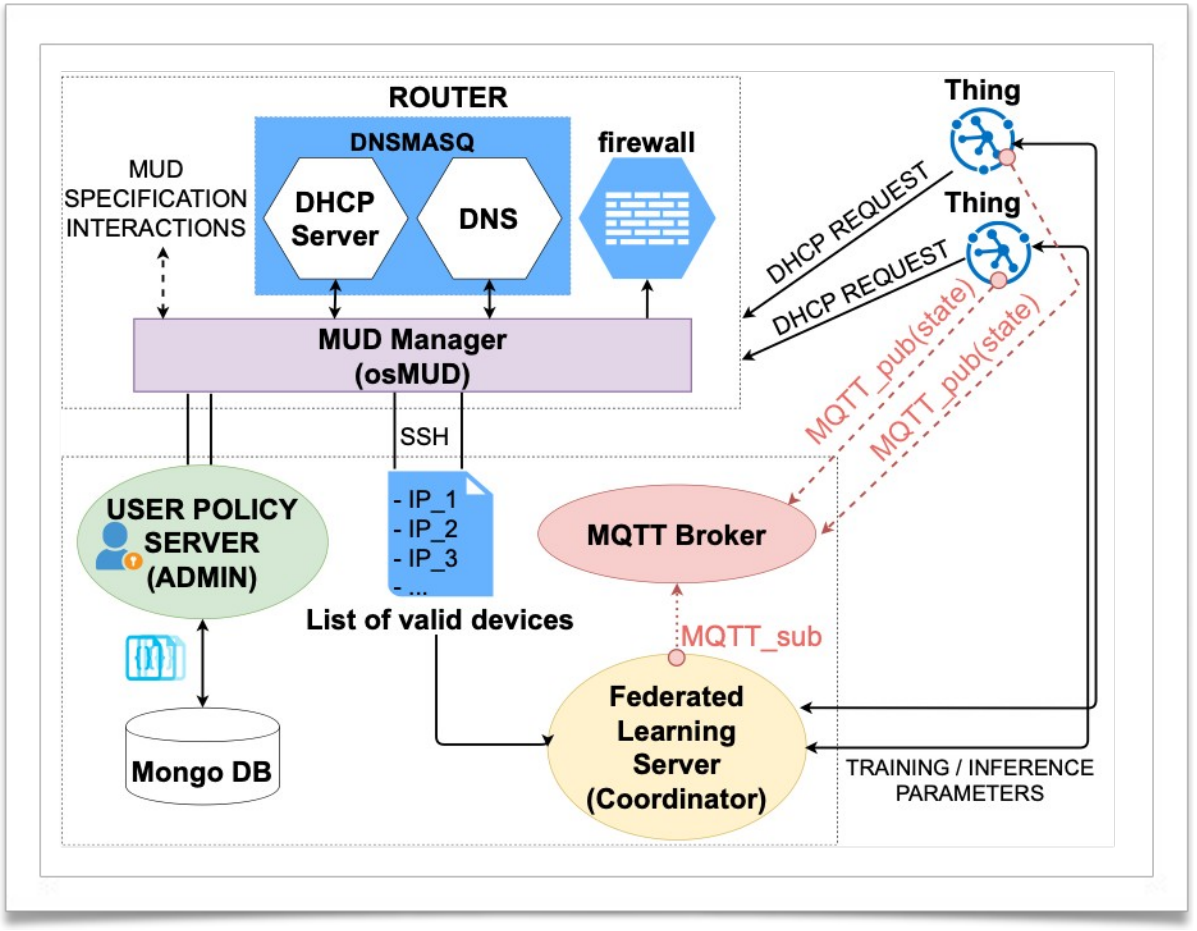
- Verifying network behaviour of dumb "smart" devices" through secure multiparty federated machine learning
- Verifying secure multiparty federated machine learning systems:-)

Systems Context - the problem

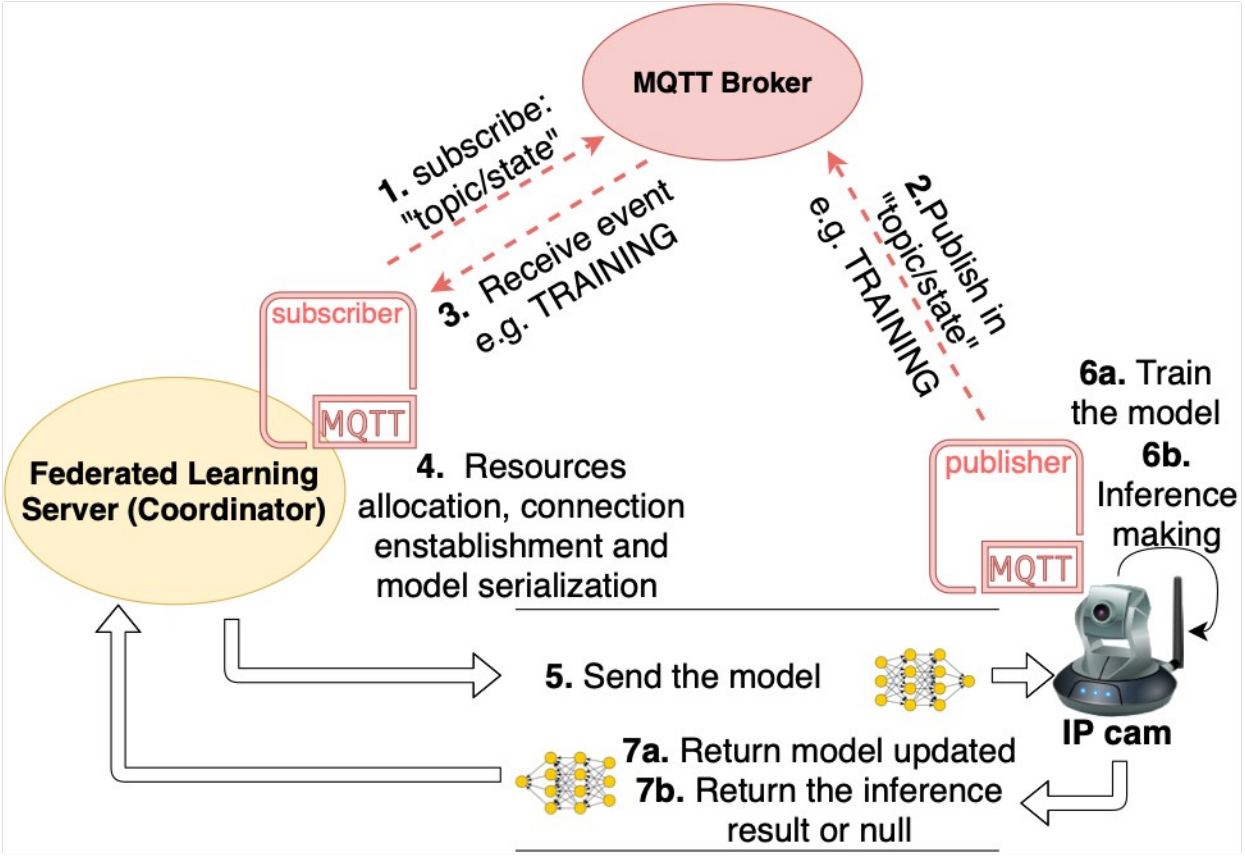


- osMUD - concern over misbehaving devices
- PySft - network worker + coordinator
  - Scale up for future work:-)
- Secure Multiparty Computation via SPDZ & SecureNN
  - Threat model - device owner fear of bad publicity?

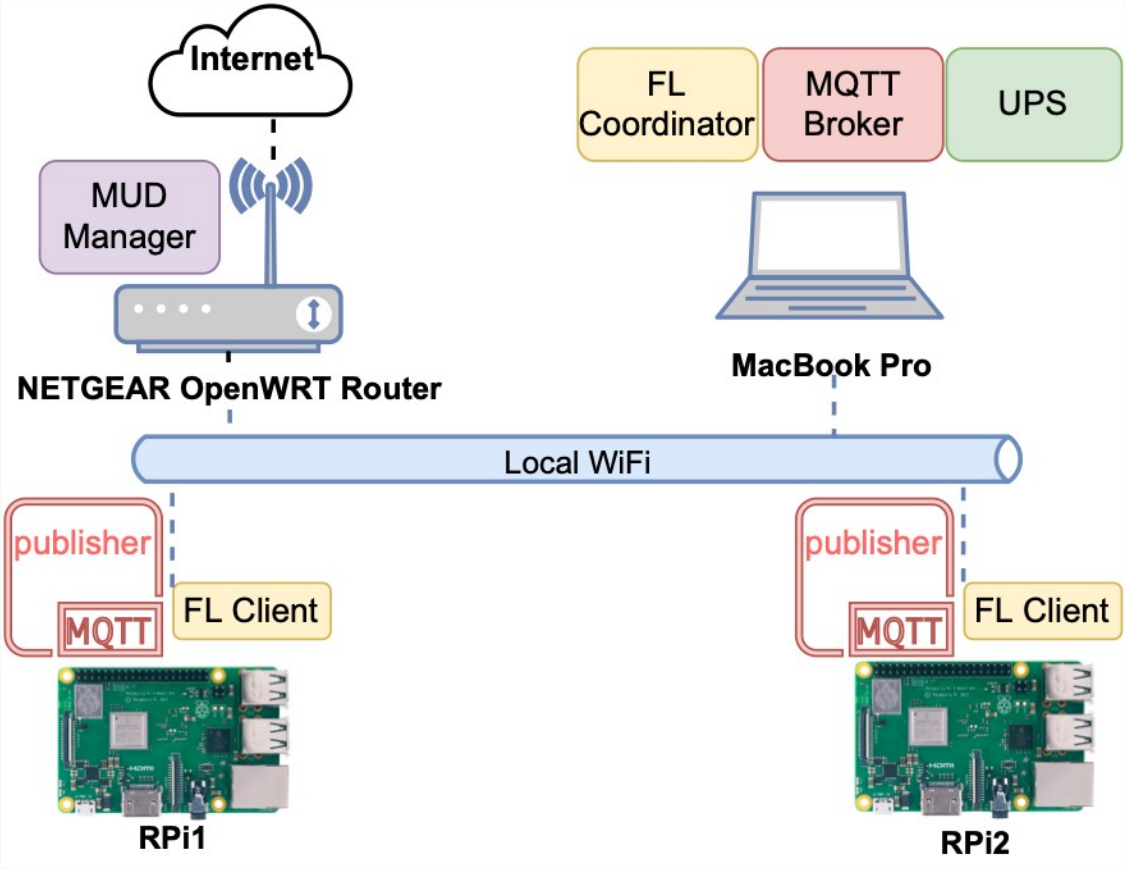
Co-learn context…

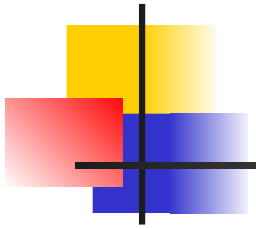


Model acquisition



Experimental Platform

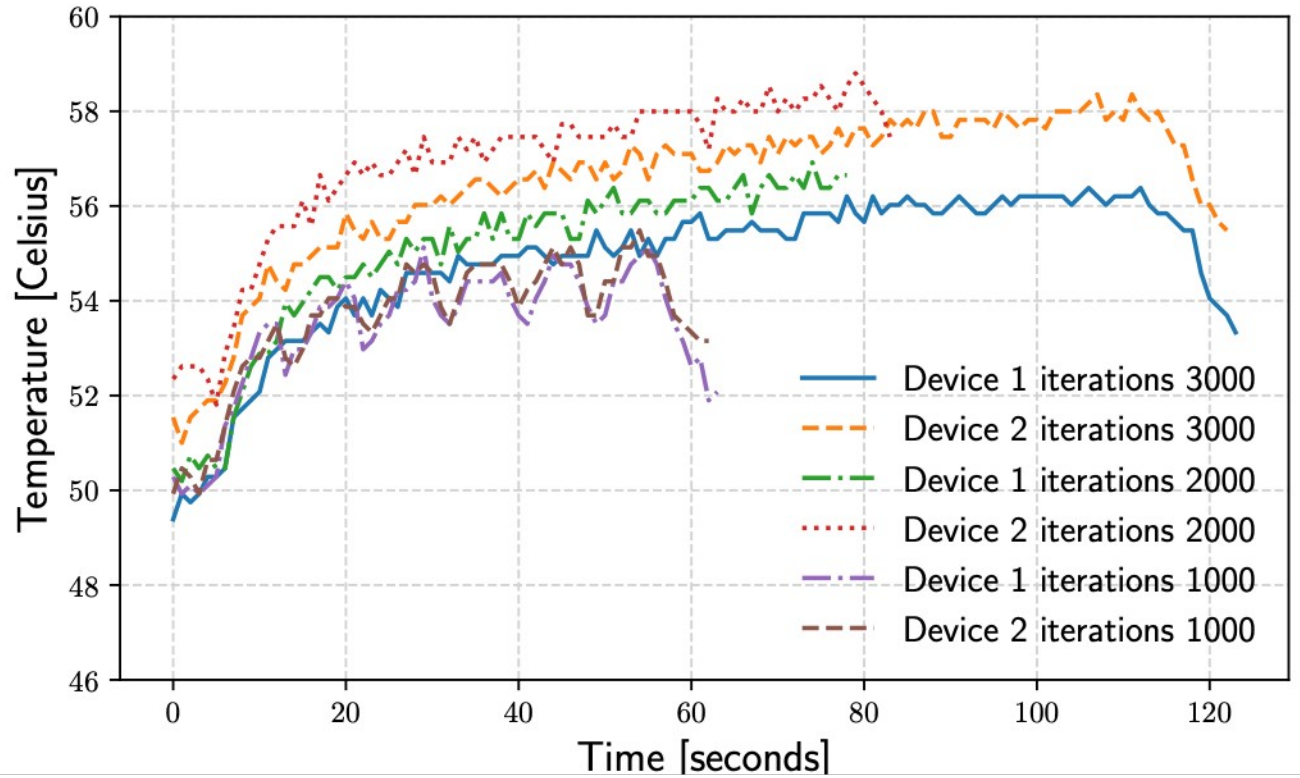




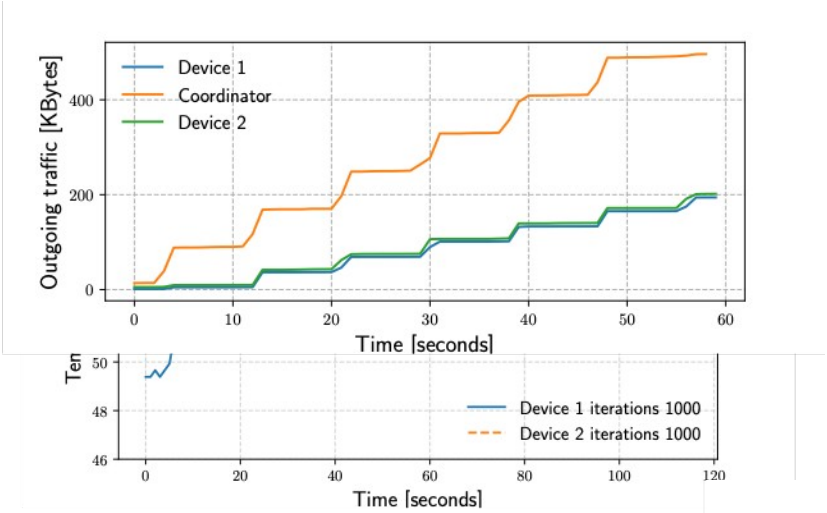
Evaluation

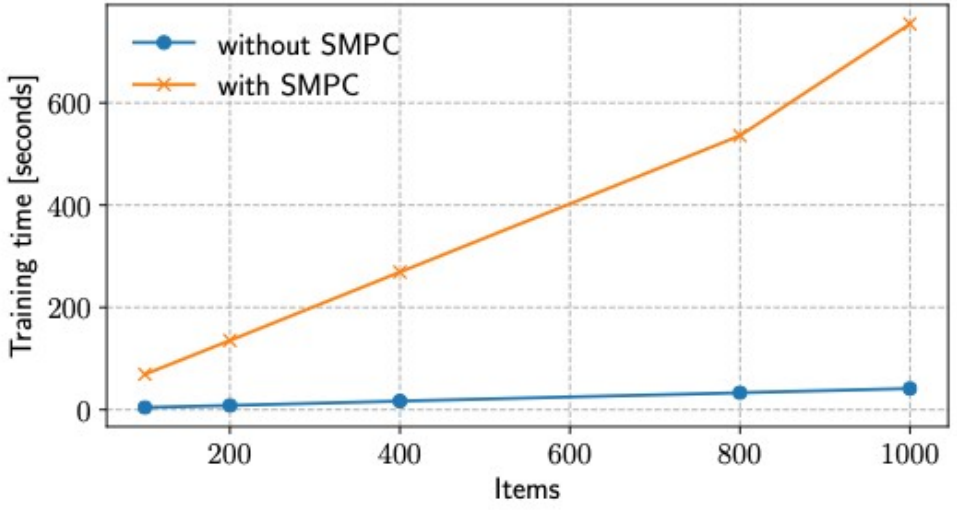
- Open Source botnet id dataset
- feed forward neural net - 2 hidden layers - see paper

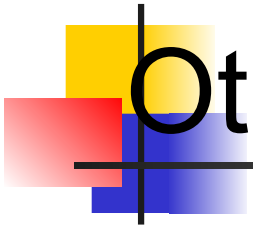
Some results



More details

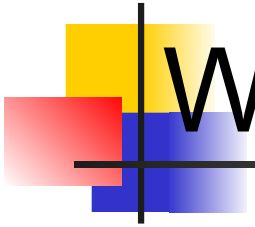






Other things to learn from edge

- MUD targetted IoT
- Could have descriptors for many things
- Including federated learning itself…
- Could run SGD or PCA
- Could even do Bayes model inference



Worries about edge/federated

- Poisoning & Pollution Attacks
  - Catastrophic Forgetting
- Aggregation needs fancy stats not just models
- Model Inversion attacks
- Maybe need DRM for models?

Any Questions?

- ref: colearn
- https://doi.org/10.1145/3378679.3394528
- alt: ppfl
- https://arxiv.org/abs/2104.14380
- Federated PCA https://arxiv.org/abs/1907.08059