Co-learn - federated learning for IoT

Resource- and Data-Constrained AI Discussion Group<

Jon Crowcroft,

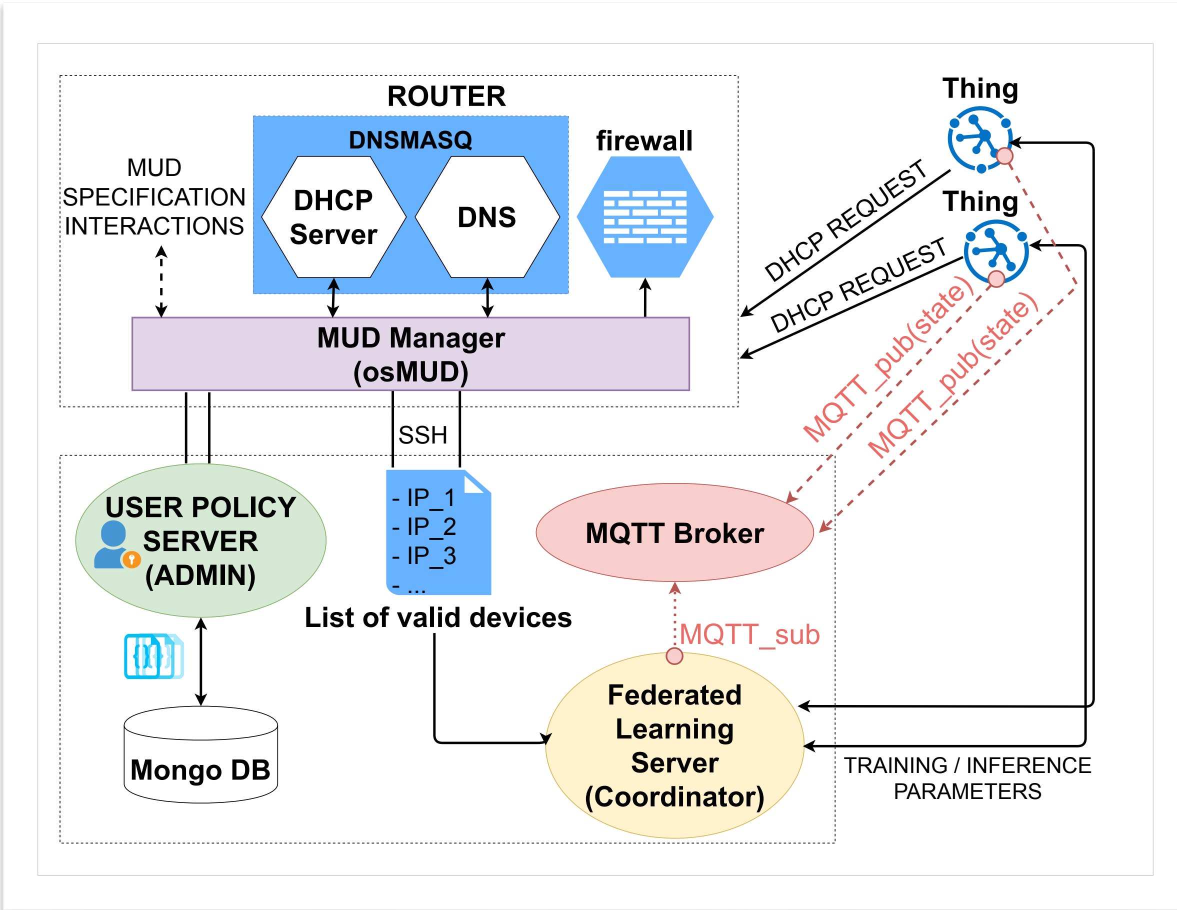
http://www.cl.cam.ac.uk/~jac22

Apr/May 2021

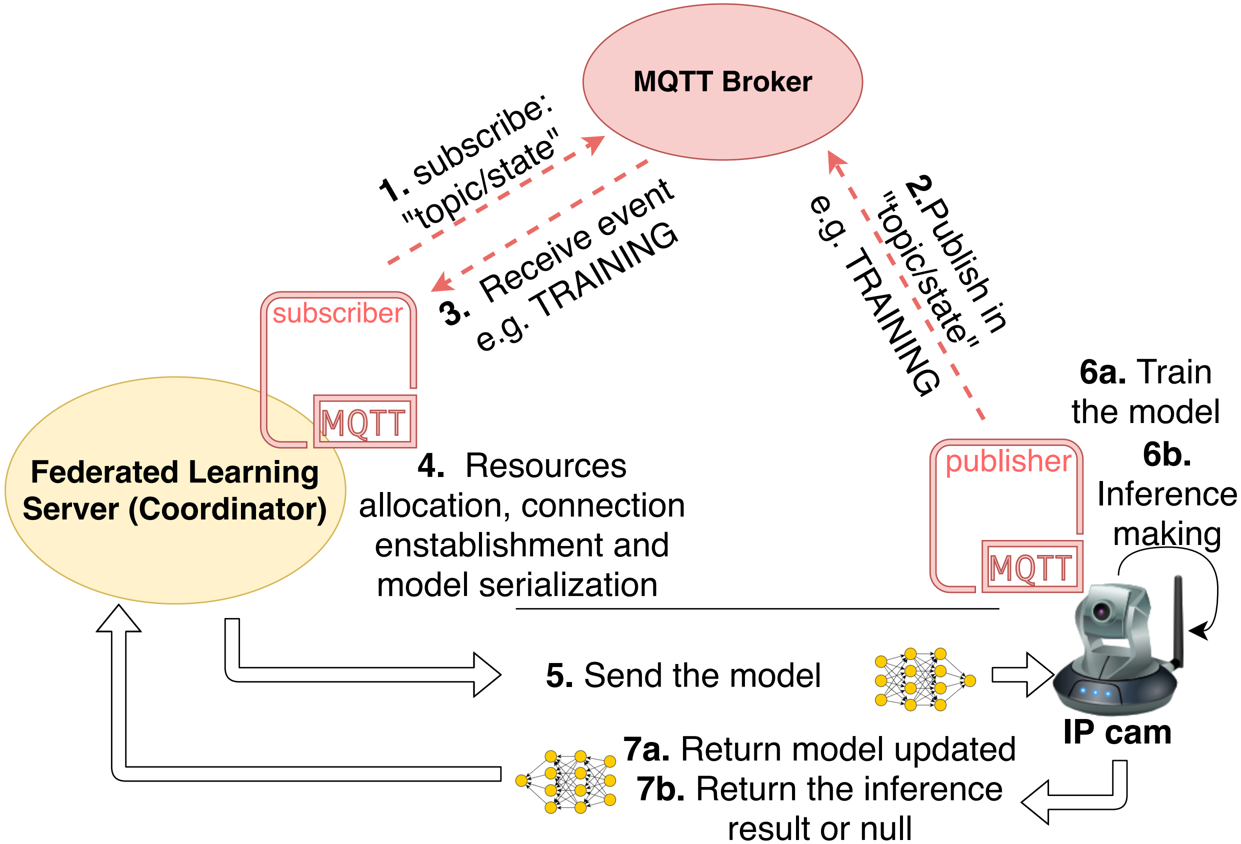
Systems Context - the problem

- 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…

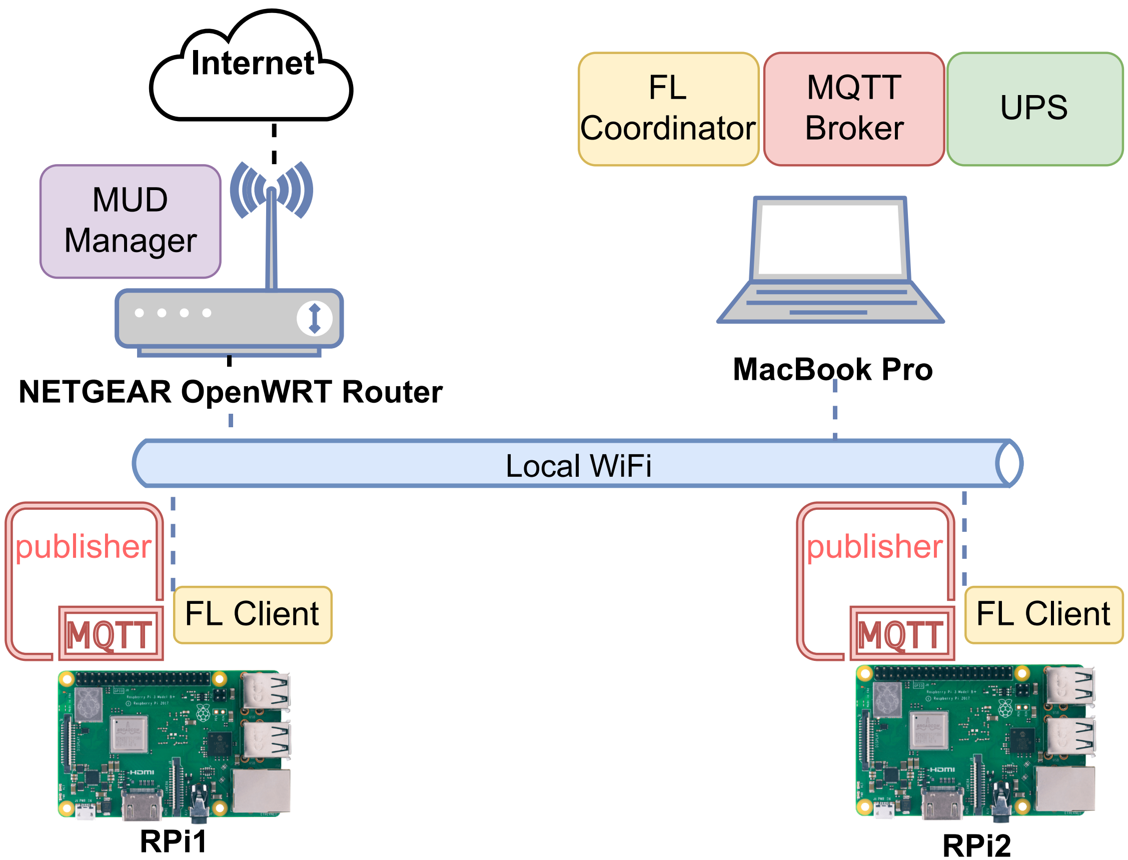


Model acquisition



1.

Experimental Platform

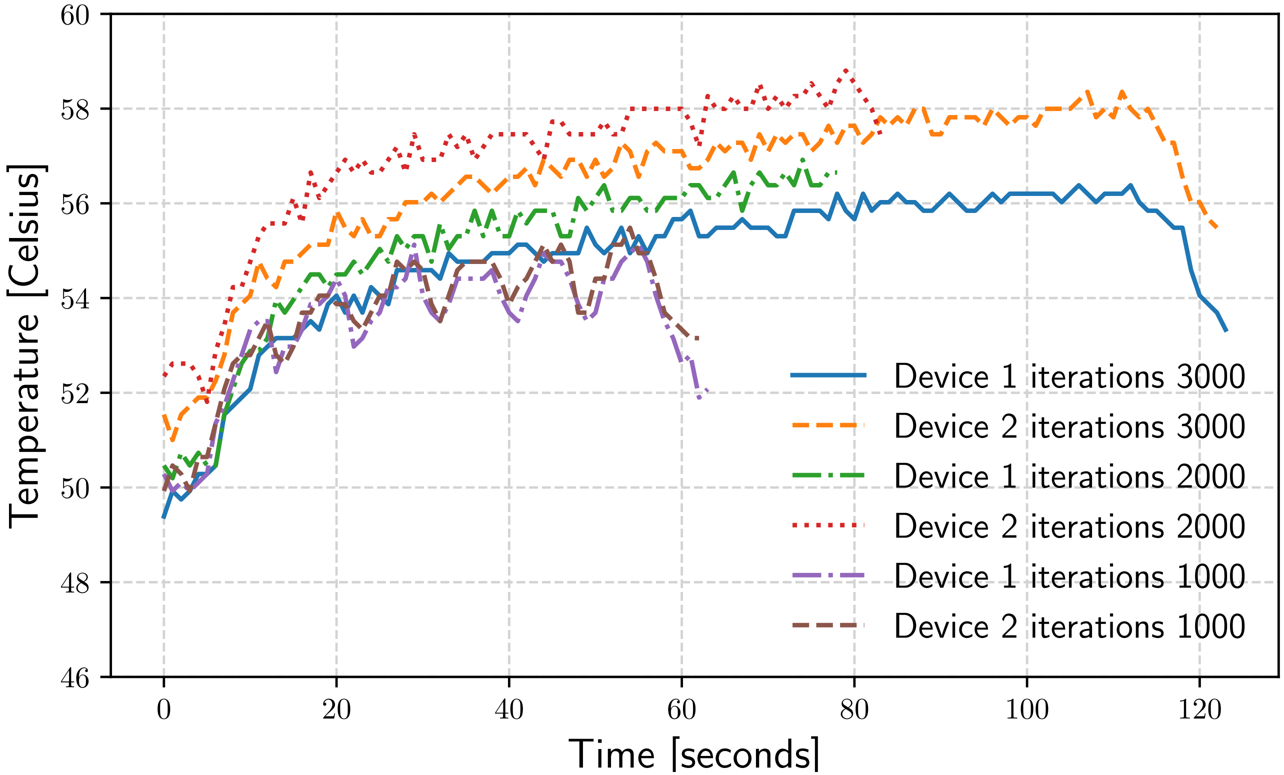


1.

Evaluation

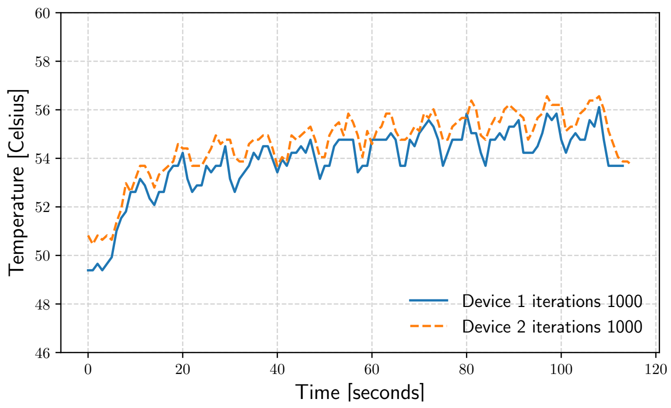
- Open Source botnet id dataset
- feed forward neural net - 2 hidden layers - see paper

Some results

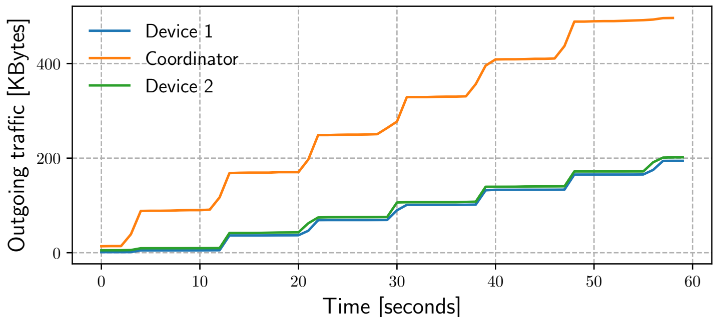


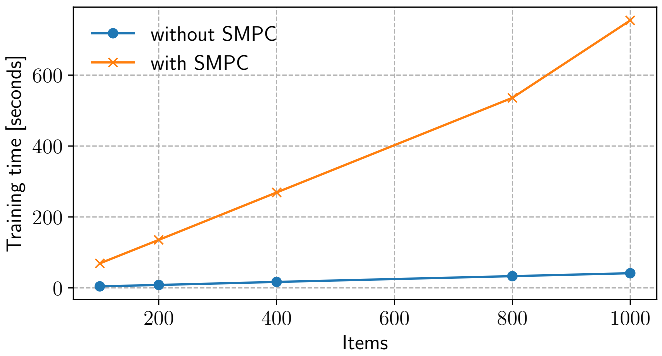
1.

More details



1.





Any Questions?

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