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 :-}
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?

Systems Context - the problem
Co-learn context...
Model acquisition

1. Subscribe: “topic/state”
2. Publish: “topic/state”
3. Receive event e.g. TRAINING
4. Resources allocation, connection establishment and model serialization
5. Send the model
6a. Train the model
6b. Inference making
7a. Return model updated
7b. Return the inference result or null
Experimental Platform

Diagram:
- Internet
- MUD Manager
- NETGEAR OpenWRT Router
- MacBook Pro
- UPS
- Local WiFi
- FL Coordinator
- MQTT Broker
- publisher
- FL Client (RPi1/RPi2)
- MQTT
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 targeted 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](https://doi.org/10.1145/3378679.3394528)
- alt: ppfl
- Federated PCA