SECURE WIRELESS AGILE NETWORKS

Wireless Traffic Analysis: From Centralized Learning to Federated Learning

Chuanting Zhang

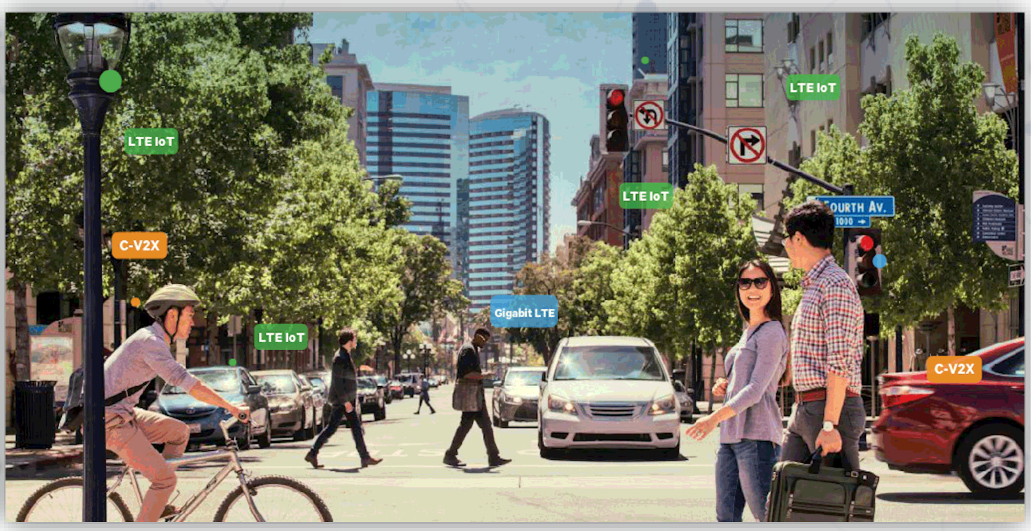
Senior Research Associate

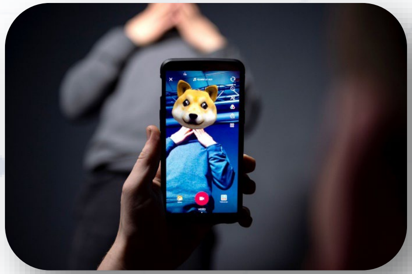
June 8th, 2022

Engineering and Physical Sciences Research Council TOSHIBA University of BRISTOL ROKE GCHQ

A Wireless World is A Better World

- Wireless communication is critical in shaping smart cities



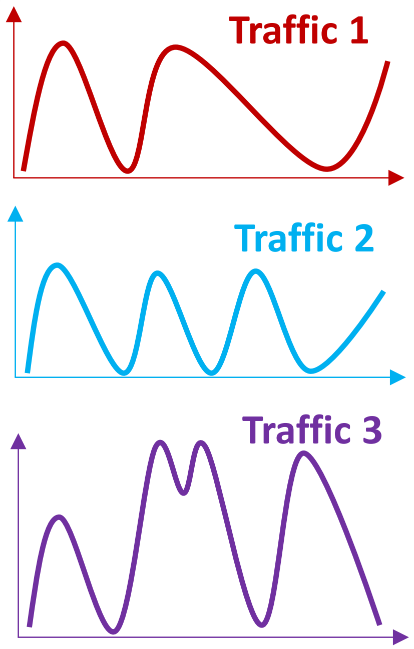


Images: Google

SECURE WIRELESS AGILE NETWORKS

Wireless Traffic Data

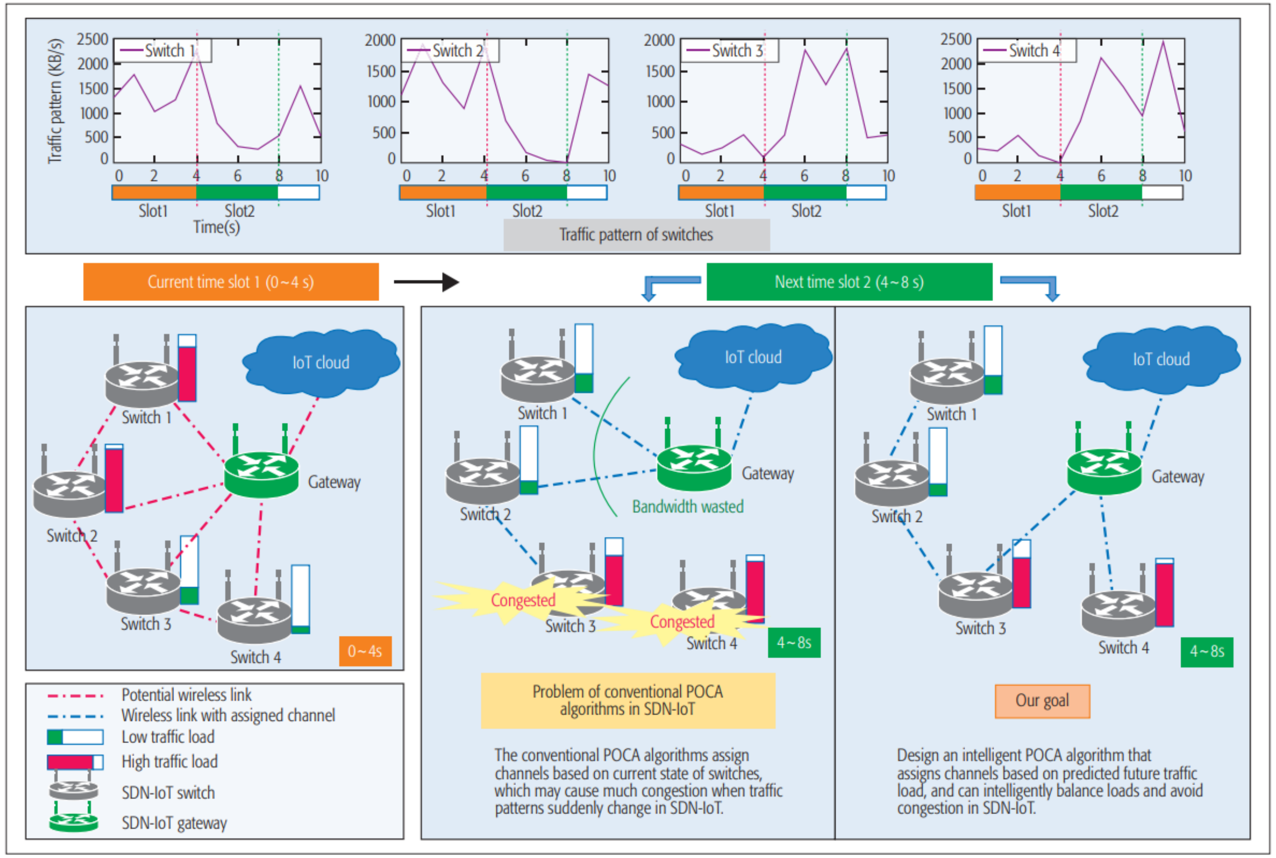
- Data is naturally generated with communications
- Many kinds of wireless traffic exist
  - Downlink/uplink rate
  - Number of connected users of a BS
  - Throughput
  - Packets of IoT sensors
  - …



Images: Google

Analysing Wireless Traffic is Important

- It contributes a lot for future intelligent wireless networks
  - ***Improve network management***
    - Dynamic network congestion control
  - ***Reduce operating expenditure***
    - Accurate radio resource purchase
  - ***Enhance energy efficiency***
    - Intelligent BS ON/OFF
  - ***Strengthen security***
    - Anomaly traffic detection



F. Tang, B. Mao, Z. M. Fadlullah and N. Kato, "On a Novel Deep-Learning-Based Intelligent Partially Overlapping Channel Assignment in SDN-IoT," in IEEE Communications Magazine, vol. 56, no. 9, pp. 80-86, Sept. 2018.

Two Kinds of Wireless Traffic

Traffic volume of a region/BS generated by subscribers

Radio signal of LoRa devices

Prediction

Identification

Centralized algorithm

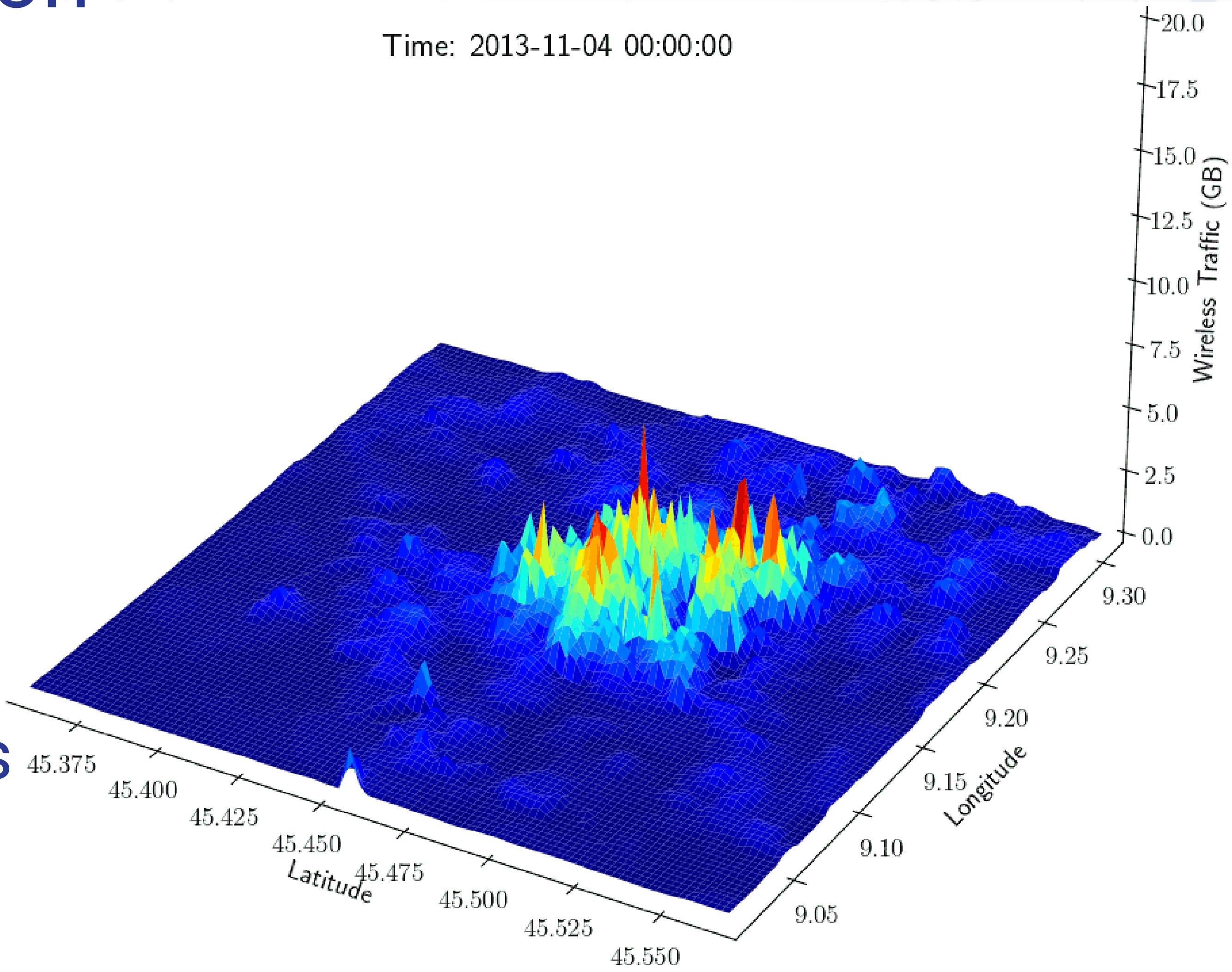
Decentralized algorithm

Decentralized algorithm

Wireless Traffic Prediction

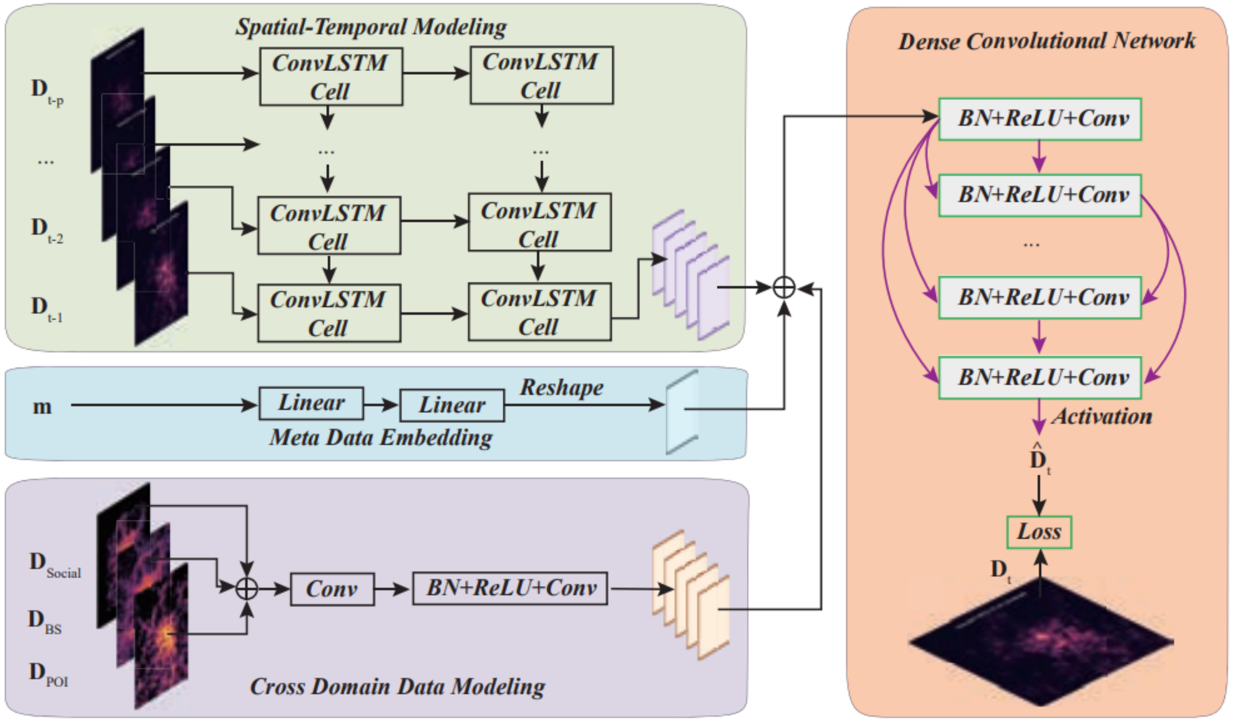
- Predict the traffic volume of the next time slot based on historical data

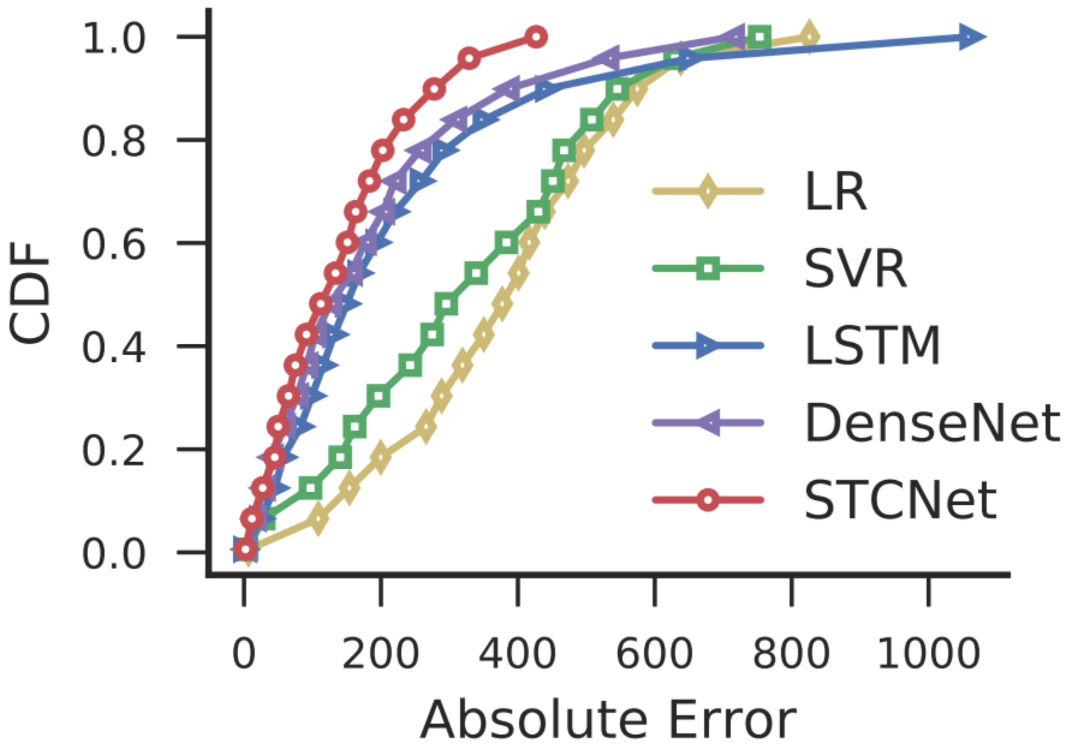
- Challenge: complex spatial and temporal traffic dynamics
- Right: city-wide traffic volume visualization of Milano



Centralized Wireless Traffic Prediction

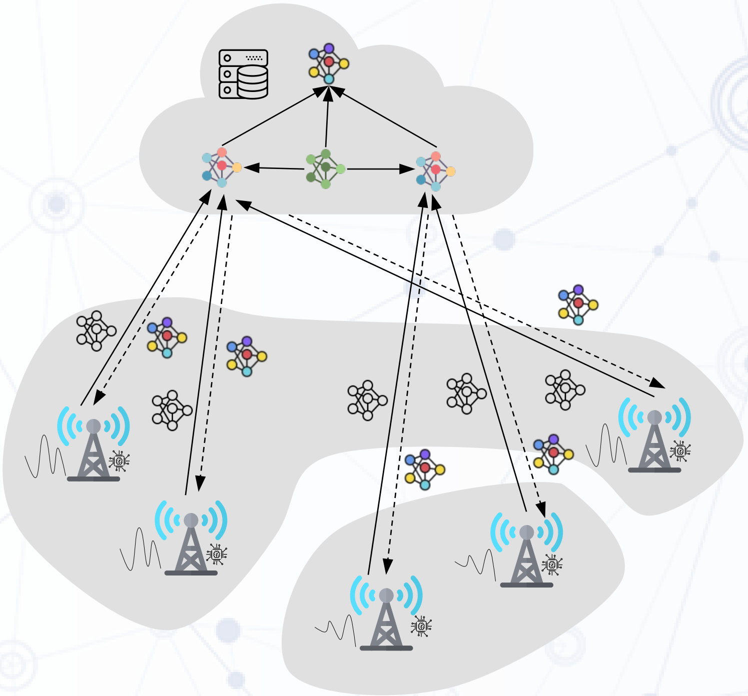
- Spatial-Temporal Cross-domain Network (***STCNet***)





Decentralized Wireless Traffic Prediction

- Prediction based on federated learning
  - BS clustering to capture spatial correlation
  - Quasi-global to reduce heterogeneity of wireless traffic
  - Dual-attention-based federated optimization



$$\arg\min_{w^{t+1}} \left\{ \sum_{c=1}^{C} \frac{1}{2}\alpha_c \mathcal{L}(w^t, w_c^{t+1})^2 + \frac{1}{2}\rho\beta\mathcal{L}(w^t, w_Q)^2 \right\}$$

Algorithms	MSE
LSTM	4.6976
FedAvg	4.7988
FedAtt	4.7645
Our	3.9266

Two Kinds of Wireless Traffic

Traffic volume of a region/BS generated by subscribers

+

Radio signal of LoRa devices

Prediction

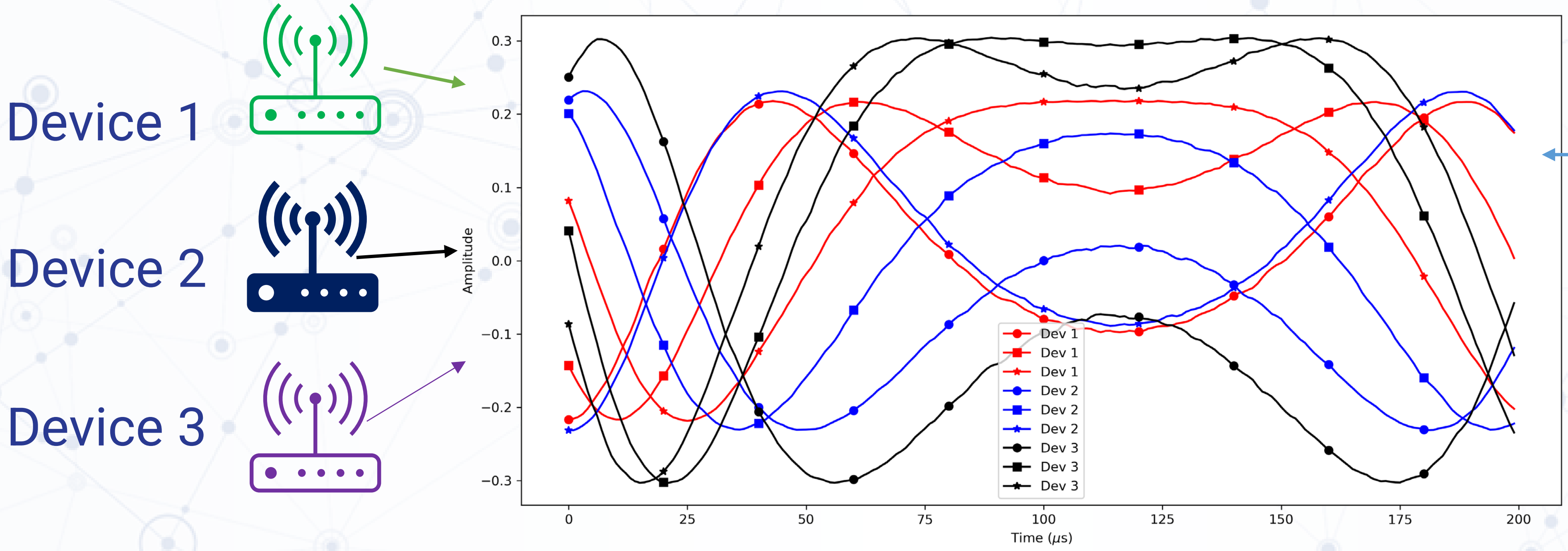
Identification

Centralized algorithm → ***Decentralized*** algorithm

Decentralized algorithm

Radio Frequency Fingerprint Identification

- RF Fingerprinting is a ***device authentication*** scheme that identifies devices based on their hardware fingerprint.



Identify which devices these signals belong to in high accuracy using a function *f*

Machine Learning for RF Fingerprinting

- State-of-the-art of ML-based RF fingerprinting

$$\theta^* = \arg\min \mathcal{L}(f(x;\theta), y)$$

True ***labels*** of the corresponding dataset, for example, 1, 2…

Loss function measuring the goodness of our learning function f, e.g., ***cross-entropy***, ***triplet loss***

The ***parameters*** of function f

Target model/function, e.g., ***CNN***, ***MLP***

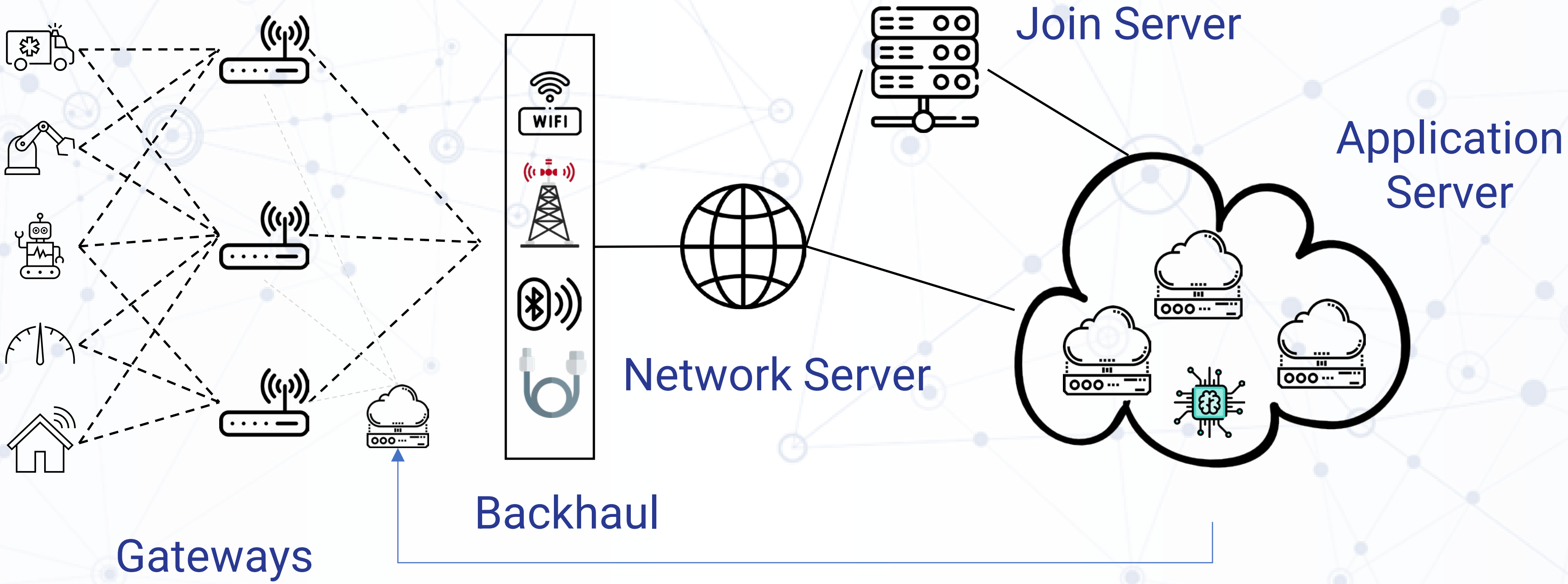
Dataset stored in a ***centralized*** server

Challenges of Centralized RF Fingerprinting

- Centralized RFF is inappropriate when ***data privacy and protection*** is a must; users are not incentivized to share data to a centralized entity (server) since their ***data may contain private information***;
- Unrealistic to assume that a centralized dataset is always updated with signal collections as ***new devices are continuously entering the market***;
- Prediction ***latency*** may high if multi-hops needed from the device to the server.

Solution: Decentralized RF Fingerprinting

- Push the learning and prediction from cloud (application server) to the edge server



Designed Algorithm

- A federated learning approach for RFFI

$$\theta^* = \arg\min \sum_{k=1}^{K} \mathcal{L}_k(f(x_k;\theta), y_k)$$

Local client

Divided into two steps

Edge server

$$\theta_k \leftarrow \theta_k - \eta(\nabla f(\theta_k;\mathcal{B}_k) + z_k)$$

Train with local data, thus no data-sharing is needed, and ***privacy is preserved***

Gradient randomization, thus ***security is guaranteed***.

$$\theta \leftarrow \theta - \alpha \sum_{k=1}^{K} \mathcal{C}(g_k)$$

Introduced ***gradient compressor*** to reduce communication between local client and edge server

Accumulated gradient at client k

Conclusion

- We designed both ***centralized*** and ***decentralized*** algorithms for ***wireless traffic prediction***. Both spatial and temporal dependencies are well modelled.
- We are working on FL-driven radio frequency fingerprint identification for LoRaWAN network. The designed algorithm ***keeps privacy*** of the data, ***guarantees security*** of the transferred information, ***achieves communication efficiency***.

SECURE WIRELESS AGILE NETWORKS

Thanks!

Questions?