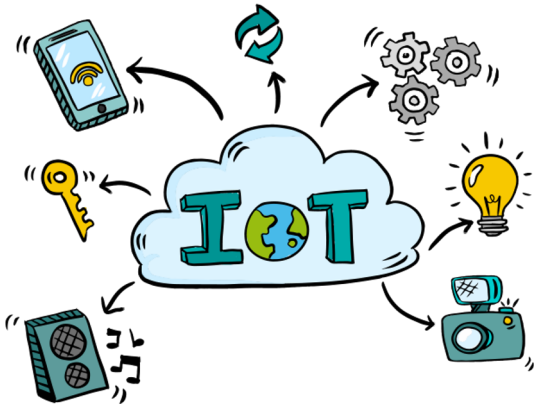
SaTC: CORE: Small: Robust Physical Layer Security with Channel Knowledge Uncertainty

Challenges in Federated Learning:

- Data Privacy:
  - Membership inference attack
  - Model inversion attack
- Communication Efficiency:
  - Analog Aggregation for Federated Learning more bandwidth efficient than Digital Schemes
  - Analog Aggregation needs Power alignment: requires coordination between users, and perfect channel knowledge at transmitters



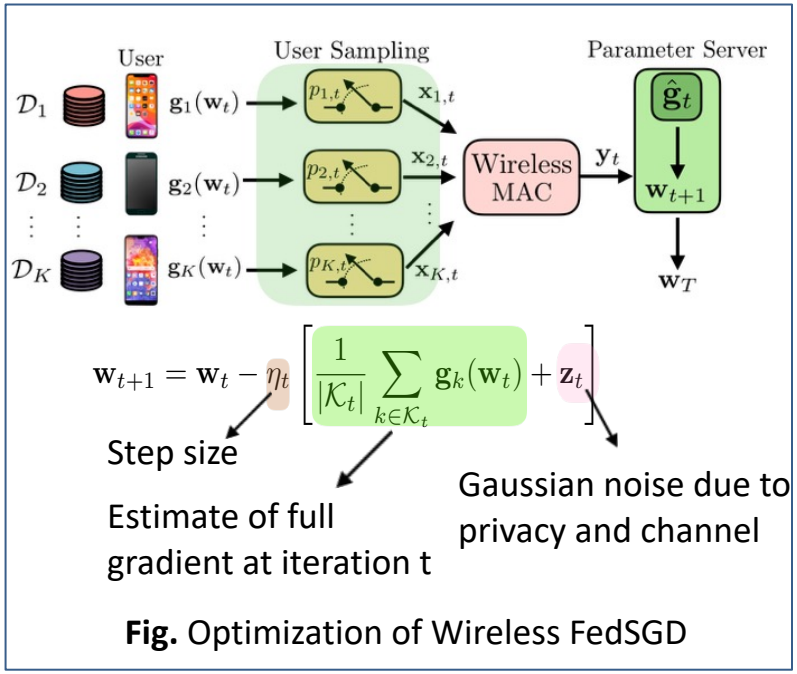


Fig. Optimization of Wireless FedSGD

Solutions:

- Harnessing the superposition property of wireless channel to improve bandwidth efficiency and privacy guarantees in federated machine learning.
- Proposed communication efficient schemes that require less coordination between users without the need of perfect CSI. Analyzed the convergence of training schemes for wireless federated learning.
- Showed the joint use of wireless aggregation and user sampling which leads to privacy amplification.

CNS1715947

PI: Ravi Tandon
Affiliation: University of Arizona

Scientific Impact:

- Distributed systems where data privacy can be a concern:
  - IoT Systems
  - Healthcare Networks
  - Edge Networks
  - Autonomous Vehicle Systems.

Broader Impact and Broader Participation:

- Fundamental understanding of privacy-preserving machine learning.
- Exploiting new benefits from wireless channels which can have impact in 6G and beyond.
- New curriculum and courses taught on distributed and private machine learning.
- Engagement with REU students and NSF IUCRC (BWAC @ Uarizona)