Secure, Private, and Low-Latency Cloud Connectivity for IoT Applications

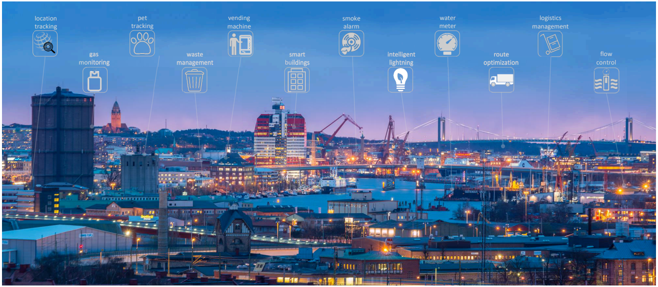
Giuseppe Durisi, Katarina Mitrokotsa

Chalmers, Sweden

January, 2020

Wireless-enabled IoT devices

Key enabler of future autonomous systems



source: IoTpool

- 5G ⇒ massive MTC; ultra-reliable, low-latency comm.
- Low-power wireless-area networks ⇔ LoRa-WAN, SigFox,...

How optimal are existing solutions?
How to optimally design IoT systems?

The IoT design problem

Communication perspective

- key challenge: how to transmit short data packets in an energy-efficiency way
- tool: information and communication theory

The IoT design problem

Communication perspective

- key challenge: how to transmit short data packets in an energy-efficiency way
- tool: information and communication theory

Computation perspective

- key challenge: how to maintain security and privacy while delegating computation to a cloud/edge server
- tool: cryptography

The IoT design problem

Communication perspective

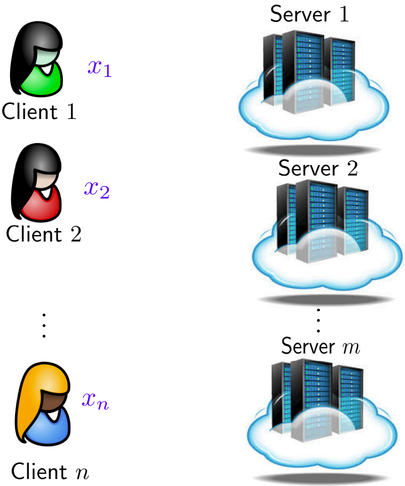
- key challenge: how to transmit short data packets in an energy-efficiency way
- tool: information and communication theory [Giuseppe Durisi]

⇕ This project

Computation perspective

- key challenge: how to maintain security and privacy while delegating computation to a cloud/edge server
- tool: cryptography [Katerina Mitrokotsa]

Aim of the project

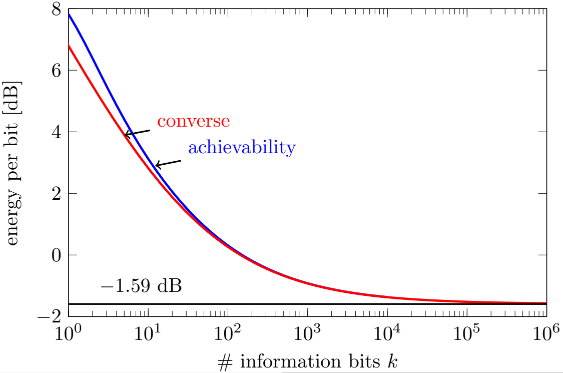


- massive number of clients
- computation assisted by multiple servers
- latency constraint
- security and privacy constraints

What is the maximum energy efficiency achievable at the client side?

Communication: Transmitting efficiently small packets

- Information payload is often small (≈ 100 bits)
- Energy consumption dominated by wireless transmission
- Minimum energy efficiency well-understood in the point-to-point case $\Rightarrow$ Finite-blocklength information theory



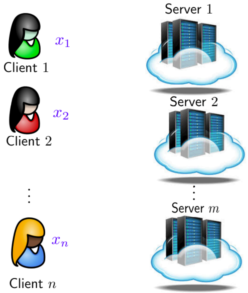
Energy efficiency in massive IoT deployments

- Massive number of sporadically active sensors
- Coordinated transmission inefficient from an energy perspective
- Uncoordinated access $\Rightarrow$ Classical information-theoretic results are not applicable

Information theory for massive uncoordinated multiple access

- very active area of research
- "... Supporting 10 users at 1 Mbit/s is much easier than supporting 1 million users at 10 bit/s..." [*Polyanskiy, 2019*]

Computation perspective: Security and privacy



- Computation on data from multiple clients
- Servers are not necessarily trustworthy
- Clients want to verify correctness of computation
- Clients have privacy requirements

Solutions

- Multi-client extension to verifiable delegation of computation protocols
- Verifiable homomorphic secret sharing

Status of the project

- Project started in October 2019
- Two postdoctoral researchers hired: Alejandro Lancho and Gustavo Souza Banegas
- Interest from industry!
- Focus of current investigations:
  - impact of protocols overhead on energy efficiency
  - scalability with number of clients
  - requirements on physical layer reliability
  - compatibility with uncoordinated access