Secure Distributed Coded Computations for IoT: An Information Theoretic and Network Approach

PIs: Yingying Chen[1], Salim El Rouayheb[1], Hulya Seferoglu[2]

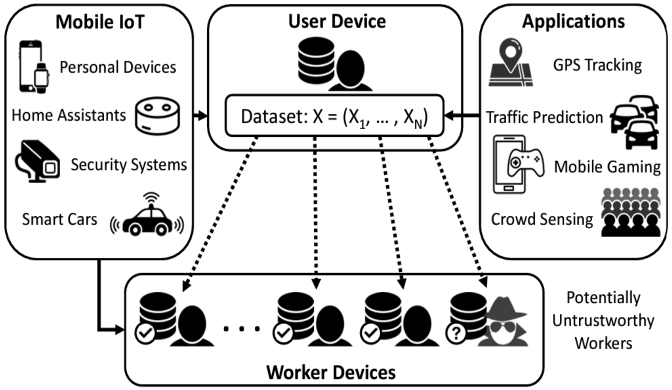
[1]Rutgers University, [2]University of Illinois at Chicago

Background

- Many coded computation algorithms have been proposed for big data applications to securely partition and distribute matrices to parallel worker devices. However, these proposals have yet to be adapted for mobile platforms beyond theoretical means.
- Commercial devices such as smartphones and tablets are much more limited in resources compared to platforms in data centers, requiring special design considerations.
- We study existing distribution schemes from an operational complexity and security viewpoint in several mobile IoT networks, identifying performance bottlenecks regarding communication and computation costs. From our findings, we propose new, scalable algorithms optimized to handle the unique constraints of mobile IoT.

Challenges

- Adapting computationally heavy cryptographic solutions for mobile IoT with limited or shared resources.
- Preservation of data privacy in untrustworthy networks.
- Optimizing matrix multiplication energy efficiency.
- Scalability for heterogeneous mobile IoT devices.



Scientific Impact

- Data such as images, audio, and text can be represented as matrices to facilitate efficient computation, especially in the domains of distributed machine learning, computer vision, and signal processing.
- Secure distributed matrix multiplication (SDMM) is capable of providing information theoretic security across a scalable and heterogenous IoT network.

Solution

Four Phases to Secure Distribution:

1. Quantization: Master converts input data from real to finite domain.
2. Encoding and Secret Sharing: Master encodes data and weight vector using random noise, then distributes.
3. Polynomial Approximation and Local Computation: Workers perform calculations using the encoded data. Calculations assume data is in polynomial form, therefore approximation function is needed.
4. Decoding and Model Update: Master collects results from workers, decodes the data, and updates weight vector.

Algorithm is lightweight as both encoding and decoding phases are sparse and each coded sub-matrix involves a single matrix addition.

Broader Impacts

- Optimized computations yield measurably faster, energy-efficient mobile computing, allowing for next-generation IoT networks and applications in health monitoring, smart cities, and driverless cars where data volumes can be large or frequently attacked.
- The educational plan will include (i) integrating research in course material, (ii) recruiting undergraduate students in summer intern-ships at WINLAB, and (iii) dis-semination via workshop organization.
- Billions of users now use billions of mobile devices daily for tasks such as navigation, entertainment, banking, etc. Such tasks may be computationally intense or involve sensitive data, requiring fast and secure computation.