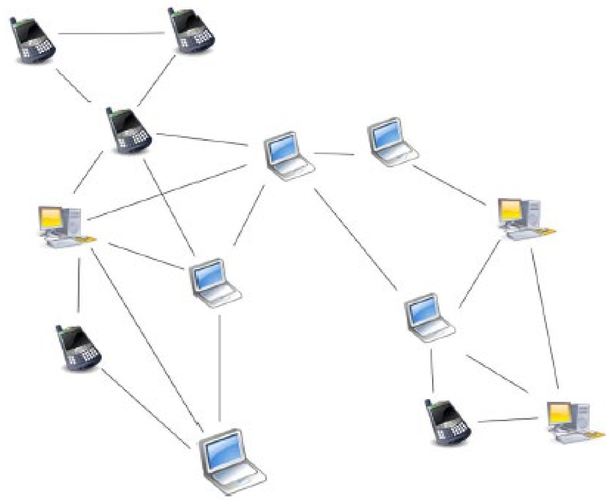
CPS: Medium: Secure Computing and Cross-Layer Anomaly Detection in the Internet of Things

Soummya Kar (PI, CMU), José M. F. Moura (co-PI, CMU), Swarun Kumar (co-PI, CMU)

AWARD #: CNS-1837607

Challenge:

- A cross-layer approach to secure distributed computation and learning in wireless P2P IoT type settings, with heterogenous, mutually-distrusting entities.
- Existing approaches are mostly fragmented, not co-optimized for application algorithms and hardware; lack of secure ML techniques for fully distributed, less coordinated and ad-hoc platforms.



Solution:

- ***Algorithmic Resilience --*** Resilient distributed computation algorithms for general machine learning tasks with multimodal streaming data over arbitrary, possibly sparse, communication networks.
- ***Hardware-based Authentication --*** A neural network based wireless fingerprinting solution for anomaly detection, specifically in the context of Sybil attacks.
- ***Integration --*** A framework for cross-layer integration of resilient approaches and a proof-of-concept testbed consisting of a network of LoRaWan devices performing distributed ML tasks.

Broader Impact:

- An integrated cross-layer approach for secure ML and decision-making in distributed networked CPS.
- Application to infrastructure systems (e.g., smart grid) and IoTs for data analytics at the edge.
- Graduate curriculum integration; engagement of undergraduates through honors projects; recruitment of minority PhD students