Dependable opportunistic communication in a multi-tier sensor network architecture

Atul Prakash, Beng Heng, and Billy Lau
Computer Science and Engineering
University of Michigan

Vineet Kamat
Civil Engineering
University of Michigan

Contact: aprakash@eecs.umich.edu
Our past and on-going projects

- **Distributed systems:**
  - Collaboratories: Helped design perhaps the first large-scale scientific collaboratory: UARC project (NSF-sponsored).

- **Pervasive computing:**
  - Privacy policies in location-aware systems. High-performance policy evaluation where results depend on dynamic context (CCS’05)

- **Security:**
  - Detecting and preventing information leaks. (Oakland S&P, 2009 -- upcoming paper).

- **Whereabouts project:** [http://whereabouts.eecs.umich.edu](http://whereabouts.eecs.umich.edu) (location-aware computing, assisting blind people, indoor navigation, etc.)

- **Architectures for monitoring civil infrastructures (e.g., bridges, etc.):** New project
Motivation

• New project: sensor networks for monitoring physical infrastructure systems.
• Data collection problem:
  • Limited or no network connectivity
  • Power/cost constraints
  • Provide robust communication against sensor failures and security attacks

Similar problems of data collection in other domains from sensors in remote areas

Data communication architecture?
Approach - Multi-tier architecture

Option 1: Direct connectivity

- A bridge equipped with a network of sensors and a wireless gateway node
- Mobile data vehicle (collects data, sends data and software updates while driving to nearby sensors)

Option 2: Via-vehicle connectivity

- Data Server and Management Portal
Drive-by data collection

- High sensor densities: raw data: 100 MB to 10 GB of data/day

- Tiers:
  - Sensor ad hoc network <-> aggregator network
  - Aggregator network <-> vehicle
  - vehicle <-> back-end infrastructure
Requirements

- Opportunistic communication and data collection
- Cooperative data transfer
- End-to-end dependability
Challenges

• Buffered data at aggregators
• When to delete?
• Potentially large volumes of data
• Compression and prioritization
• Vehicle moving at highway speeds
Data buffering

- May not be safe to delete data upon transfer to the vehicle
- aggregators <-> back-end infrastructure: acknowledgement desirable
- potentially long latencies (weeks)
- security: authentication desirable
Data transfer to Moving Vehicle

- Vehicle moving at highway speeds over large span
- How does it collect data from the aggregators?
- We envision the need for cooperative data transfer algorithms — multiple aggregators must cooperate to transfer data to a moving vehicle
Security

- Can we involve citizens in data collection (using smartphones, etc.)?
- Security and reliability? Incentives? Data deletion policy?
- Detecting malicious sensors
- Privacy concerns in some cases
Summary

• Goal: design a robust and easy-to-deploy architecture for remote sensor networks

• We envision a:
  • multi-tier architecture, consisting of sensor network, network of aggregators, mobile data collection nodes, and back-end infrastructure

• Welcome opportunities for collaboration and finding synergies