Internet of Things

Session 1: Tarek Abdelzaher and Ramesh Govindan
Session 2: Saurabh Bagchi and Prashant Shenoy

Input solicited: **https://bit.ly/nsfiot19**

Represented Areas/Interests in the Room

Lesson #1: IoT is an interdisciplinary field as evidenced from the breadth of research interested represented among session attendees:

- Cyber-physical systems
- Sensing, devices and systems issues in sensing
- Distributed systems
- Cloud computing
- Edge computing
- Machine learning
- Smart city applications
- Reliability/resilience
- Privacy and security
- Resource constrained environments
- Networking, and network measurements
- Content distribution
- Crowdsensing
- Wireless and Mobility
- Robotics
- Mobile health
- Fault-tolerant real-time
- Real-time databases
- Cross-layer measurements
- Energy efficiency
- PKI

What is IoT?

The research challenges discussed in this session are motivated by an application construct that spans systems and networking. This construct was characterized as:

Physical devices interacting over wireless networks in social/human contexts to offer a human-centric application value.

There is some overlap with the following but IoT is also distinct from: "embedded systems" "control systems"

Application Drivers

Enhance our spaces:

- Smart homes/buildings
- Smart places (campus, hospital, etc)
- Smart and connected communities
- Smart cities

Empower our things:

- Smart appliances
- Medical devices/assisted living
- Swarms/drones for rescue and disaster response
- Intelligent vehicles and smart transportation

Advance our sectors:

- Digital/precision agriculture
- Smart manufacturing
- Smart health
- Energy and smart grid
- Security and monitoring

Integrate humans and technology:

- Crowdsourcing

Core Analytical Foundations

IoT builds on advances in several areas, including distributed systems, sensing, localization, and control but adds new constraints, opportunities, and thus solution spaces driven by *physical embedding*, *dirty/lossy data*, *scale*, *heterogeneity*, *interoperability*, and *composability*. Thus new problems arise:

By key component:

- ***Sensing: fundamental time/capacity trade-offs:***
  - Information-theoretic limits for IoT contexts (related to age of information)
  - Fundamental limits (e.g., meeting timeliness guarantees, density of sensors to recreate an event)
- ***Data processing/Learning:***
  - When does AI help IoT? When are more classical approaches sufficient? How to adapt those to the resource constrained environment of IoT? How to add predictability and explainability?
- ***Actuation:***
  - Different from classical control loops in the lack of predictability/timing in the loop (high variance).
  - Uncertainty makes it hard to offer tight guarantees/bounds using classical control theory approaches.

By key system property

- ***Resource efficiency:***
  - Energy harvesting,
- ***Security, privacy, trust, and safety:***
  - Solutions for IoT settings (scale, heterogeneity, humans-in-the-loop, resource constraints, power, …)
  - Reliability analysis of large IoT systems/big-data systems
- ***Human-in-the-loop challenges:***
  - Accounting for/using humans in different roles: sensors, controllers, actuators (decision makers), etc.
  - Economic incentives.
  - Human-computer interfaces.
- ***End-to-end assurances, compositionality.***

Architectural Challenges

- ***Open architecture:*** Horizontal integration, as opposed to vertical silos
    - Standardization of platforms for sensing/processing/actuation
    - Standardization of software stacks for sensing/processing/actuation
    - Operating systems for IoT
- ***Intelligence:*** Where to put how much intelligence - IoT device, edge, cloud?
    - How to decentralize operation?
    - How to cooperate even in the absence of connection to "mother ship"?
- ***Multiple trust domains:*** Applications may be distributed - no single owner. How to develop collaborative services across trust boundaries in IoT systems?
- ***Compositionality, modularity, and complexity reduction:*** Architectural principles for time-scale separation; Architectures for compositionality; Technologies to ensure temporal order/ correctness (e.g., using blockchain); Naming, service discovery, and standard APIs. Handling lack of visibility into the system, while ensuring guarantees. Multi-use devices.
- ***Scale and heterogeneity:*** How can we support the range of information processing required in IoT systems? How can we design these architectures to scale to large smart and connected community (smart city) environments?

Systems and Networking Issues

- Predictable operation under unpredictable conditions and resource constraints
- Mobility and intermittent connectivity
- Systems must be able to operate under multiple different wireless technologies (5G, LoRa, next gen 802.11)
- Devices are *not* all universally addressable ⇒ brings in management challenges
- Problem diagnosis in a lightweight manner, e.g., lightweight record and replay
- Data management - collection, analytics, anonymization; huge volumes of data over time; real time stream processing; in-sensor analytics

Cross-disciplinary Issues

Hardware:

- What new kinds of sensors should we consider?
- How will the device energy landscape change in the future, and how does that affect IoT systems?

Machine learning:

- How can we best use ML in IoT?
- What challenges does IoT pose for ML?

Reliability and security:

- What are domain-specific reliability challenges?
- What are domain-specific security challenges?

ML, Reliability, and Security: Domain-specific Issues

ML in IoT

- *Benefit*: Learn automatically from the large number of devices and sensor streams
- *Challenges*: Learn in frequency domain, with spatial correlations
    - Do it on resource-constrained devices
    - Perform inference in real-time
    - Lots of unlabeled data ⇒ use techniques for automatic labeling
    - Privacy preserving ML

Reliability and Security

- Fine-grained authentication and revocation; fine-grained transition of trust boundaries
- Allow data access based on correct privilege level; strong requirements for data isolation
- Key management at very large scales, where adversarial physical access is possible
- Safety critical operation (in some application domains)
- Privacy becomes a first-order concern

Ethical decision-making in IoT operation (e.g., decisions in autonomous driving when accident is inevitable)

Role of industry in IoT research

Understand industry business models that lead to IoT challenges.

Industry is incentivized by some applications (e.g., smart factories), not others (e.g., environmental change, etc).

Academia can fill in where there is no strong industry financial incentive, yet benefit to society.

How can academia drive the industrial adoption of IoT?

- Help in standardization; beyond transport mechanism
- Provide strong privacy controls

Experimentation and Testbeds

Questions

Do we have benchmarks or problem models?

What are successful examples of IoT testbeds? What are desirable characteristics of a (future) IoT testbed?

What kinds of shared experimental infrastructure (reusable software, datasets) do we need?

Discussion

Testbeds plus traces for evaluation; Focus on reproducibility

Some testbeds may be controlled and some may be under physically unpredictable environments

- Time shared access

US-Ignite like effort for IoT deployments and testbed

Benchmarks for IoT for performance comparisons; industry contributed testbeds/benchmarks

Education

Questions

Is the IoT industry being well-served by our current curricula?

What would constitute an effective undergrad degree or MS specialization in IoT?

Discussion

- Ethics education
- Security and privacy
- Degree versus specialization versus individual courses
- Forensics for IoT devices: industry demand for such course material
- Lack of textbooks

Summary of IoT Discussion Topics

1. Core Foundations
2. Architectures for IoT
3. Systems and Networking Issues
4. Human-centric/social issues
5. Application Areas
6. ML, Reliability, and Security
7. Role of Industry
8. Experimentation and Testbeds
9. Education