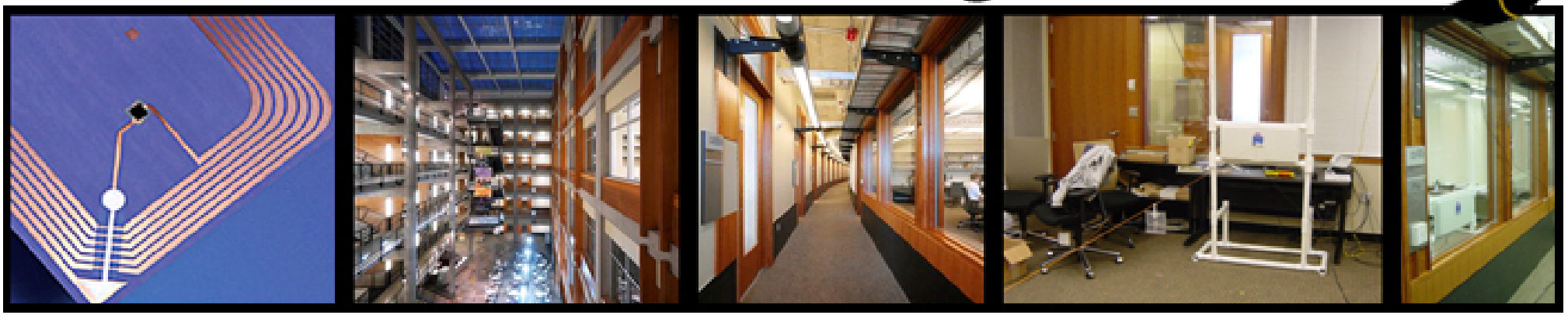
The RFID Ecosystem



Experimenting with a Pervasive RFID-based Infrastructure

Evan Welbourne

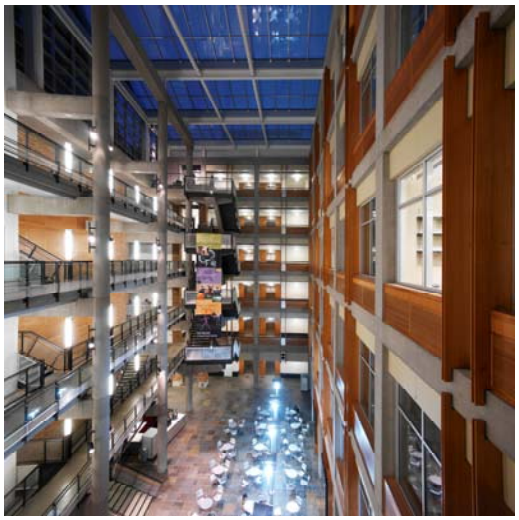
UW CSE Industrial Affiliates
October 30, 2006

RFID Ecosystem at UW CSE

http://data.cs.washington.edu/RFID

An infrastructure for RFID-based pervasive applications

- Create a microcosm of a world saturated with uniquely identifiable objects
- 100s of readers and antennas, 1000s of tags
- Explore applications, systems, and social implications
- Do it while there is still time to learn and adapt



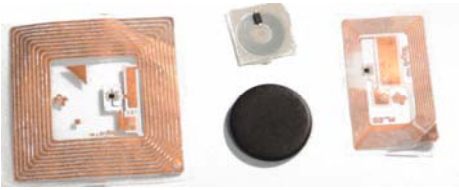
- Groups: Ubicomp, Databases, and others
- Participants include:
  - Magda Balazinska
  - Gaetano Borriello
  - Waylon Brunette
  - Brian DeRenzi
  - Nodira Khoussainova
  - Karl Koscher
  - Patricia Lee
  - Robert Spies

Overview

- Review of RFID Basics
- Applications
- Research Questions
- System Architecture
- Evaluation
- Future Work

Review of RFID Basics

http://data.cs.washington.edu/RFID



- Radio-frequency identification
  - Uses radio frequency (RF) signals to identify (ID) an object
  - Wireless, does not require line-of-sight

- Tags are attached to an object
  - ID *uniquely* identifies an object, not just its class
  - Can include other information:
    - Current state
    - Location
    - History
  - Tags are *active* (battery) or *passive* (no battery)

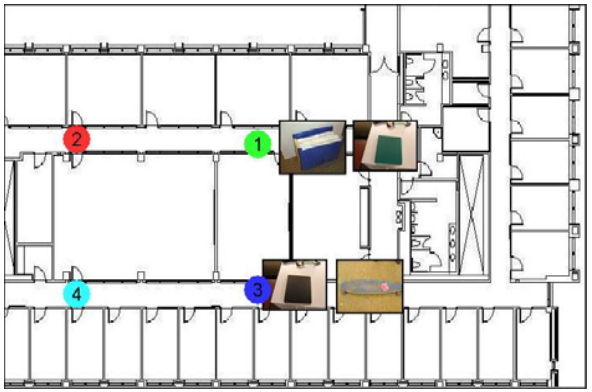
- Readers interrogate tags
  - Readers and their antennas are installed in a fixed position
  - Readers are equipped with networking and power

RFID Applications

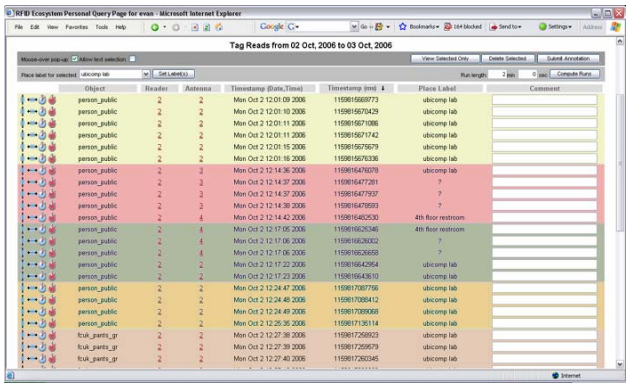
http://data.cs.washington.edu/RFID

- RFID in the supply-chain
  - Boosts throughput, makes for an agile supply chain

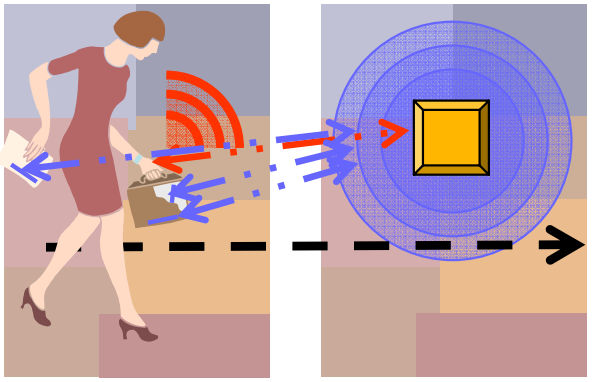
- Pervasive computing applications based on RFID
  - More consumer-oriented
  - Use a pervasive deployment of RFID technology
    - Everyday life setting
    - Personal objects and people are tagged
    - Seamless merging of the virtual and physical worlds



Personal object tracker



Web applications



Proactive Reminding

Research Questions

http://data.cs.washington.edu/RFID

- How to design an infrastructure for pervasive RFID apps?
  - Applications grow and evolve over time
  - People and objects are less predictable than the supply chain
  - Privacy and security are first class concerns
- How is the mass of data managed?
- How are applications with real-time demands supported?
- *Implications for technology, business, and society?*

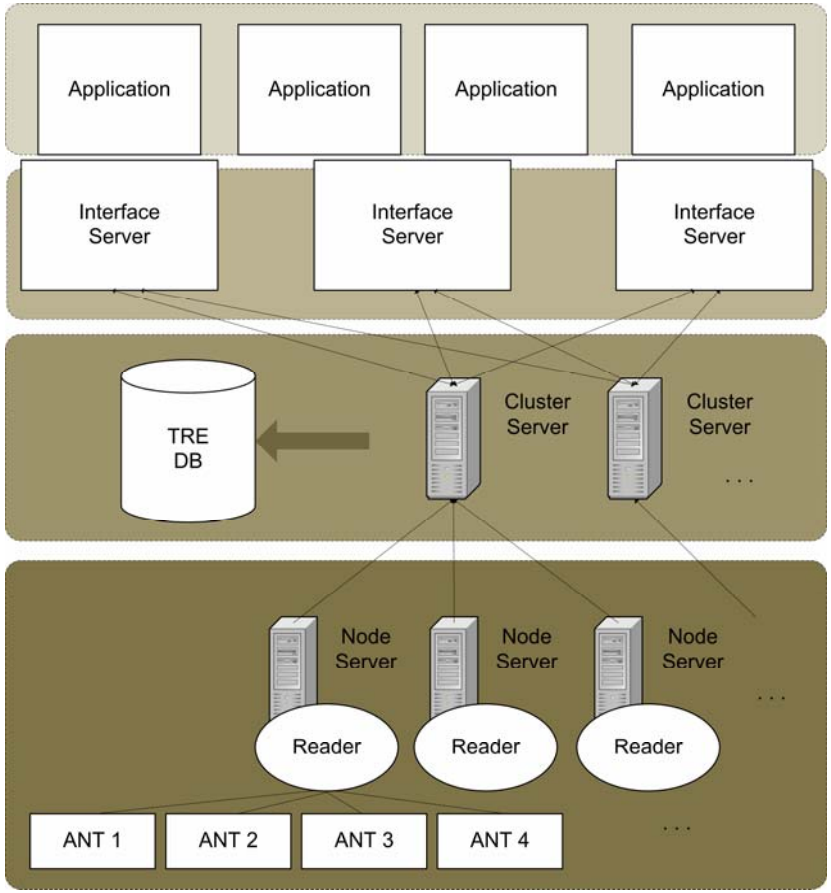
Overview

- Review of RFID Basics
- Applications
- Research Questions
- System Architecture
- Evaluation
- Future Work

System Architecture

http://data.cs.washington.edu/RFID

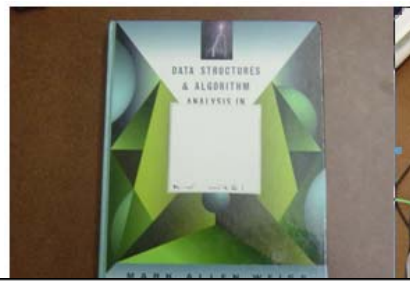
- ***Goals:***
  scalable, reliable, extensible, secure, and privacy-oriented
- Node Servers
  - Low-level filtering; forward tag reads
- Cluster Servers
  - Store tag reads, forward if appropriate
- Interface servers
  - Event generation, stream processing
- Application

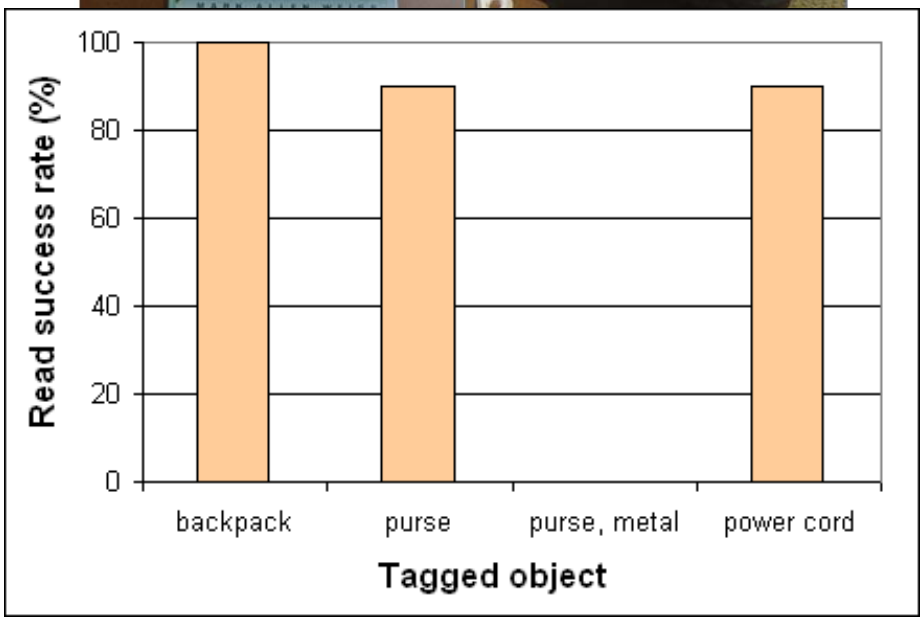


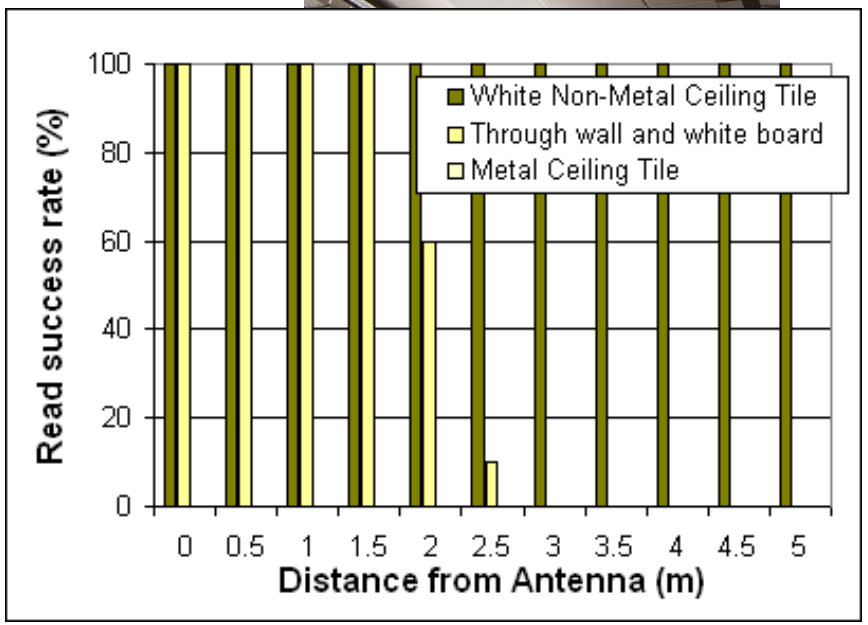
Laboratory Benchmarking

http://data.cs.washington.edu/RFID

- Characterize performance of equipment in optimal conditions
- Evaluate equipment in various deployment configurations







Pilot Study

http://data.cs.washington.edu/RFID

- 2 week pilot study to gain insight
  - 11 readers, 34 antennas hung in hallways
  - 6 participants
  - 54 tags registered

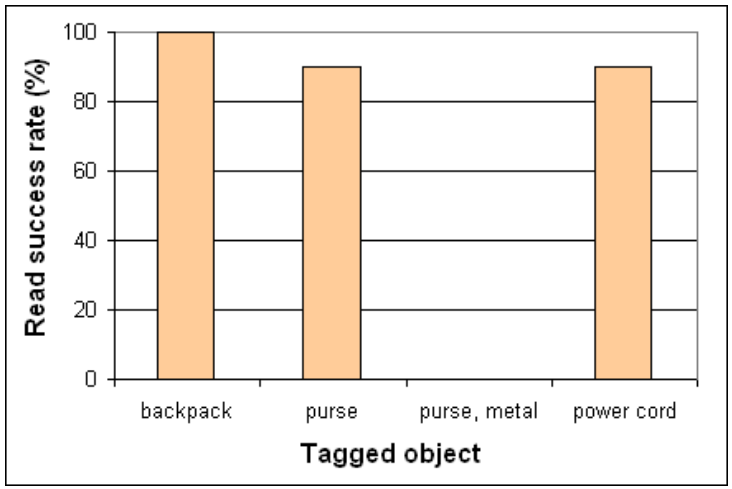
- Participants could query the data with a web application
  - “Where is object X?”
  - “Where is person Y?”
  - “How much time have I spent in the building this week?”

- A web diary and annotation system provided ground truth

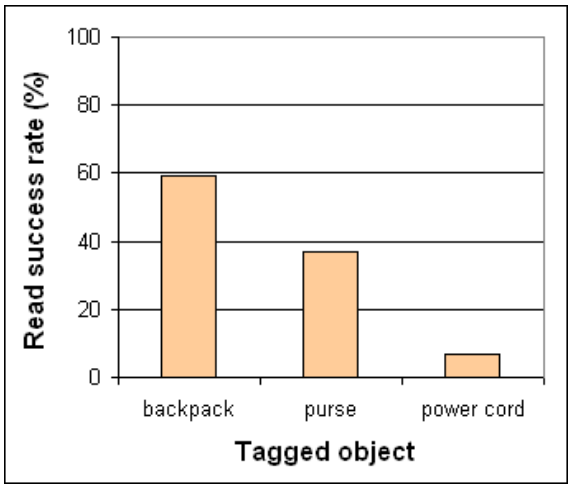
Challenge: Reliability

http://data.cs.washington.edu/RFID

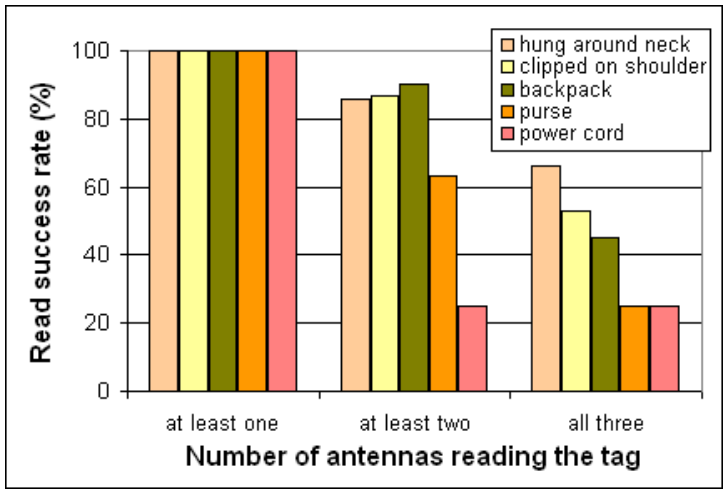
- Consider tag mounting/orientation and antenna configuration
- Exploit redundancy among antennas



Benchmark results



Pilot study results



Pilot study redundancy results

- Consider erroneous data and unpredictable streams

Other Challenges

- Remember health regulations
- Aesthetics matter
- Test each installation point
- Plan for broken tags
- Much can be inferred from objects carried and time of day
  - A simple script could detect lunch breaks with > 75% accuracy
- Typical location privacy concerns
- Must allow participants to delete any of their data at any time
- Must protect non-participants (RFID tags already pervasive)

Future Work

- Continue to develop techniques for increased reliability
- Refine the privacy model
  - Access control
  - Data anonymization and perturbation techniques
  - Location privacy techniques
- Incorporate phones with NFC technology for mobile readers
- Conduct longitudinal studies with a variety of applications
- And more…

Thank you!

http://data.cs.washington.edu/RFID

Also see our posters

- Ubicomp lab:
  - *RFID Ecosystem:*
    Experimenting with a Pervasive RFID-based Infrastructure
  - *Towards Privacy and Security in the RFID Ecosystem*
  - *A User Interaction Model for NFC Enabled Applications*
- Database lab:
  - *StreamClean: Near Real-Time RFID Data Cleaning*
- Questions…