The RFID Ecosystem

Challenges for Pervasive RFID-based Infrastructures

Evan Welbourne, Magdalena Balazinska, Gaetano Borriello, Waylon Brunette
Computer Science & Engineering
University of Washington

PERTEC Workshop, PERCOM 2007
White Plains, NY
March 19th, 2007
An infrastructure for RFID-based pervasive applications

- Create a microcosm of a world saturated with uniquely identifiable objects
- 7 floors, 90,000 sq. ft.
- 100s of readers, 1000s of tags
- Explore applications, systems, social implications
- Groups: Database, Security, Ubicomp, and others

Participants:
- Yaw Anokwa
- Magda Balazinska
- Gaetano Borriello
- Waylon Brunette
- Garret Cole
- Nodira Khoussainova
- Tadayoshi Kohno
- Karl Koscher
- Travis Kriplean
- Patricia Lee
- Caitlin Lustig
- Vibhor Rastogi
- Robert Spies
- Dan Suciu
- Jordan Walke
- Evan Welbourne
Overview

- Applications
- System Architecture
- Benchmarking & Pilot Study
- Results
- Update & Work in Progress
- Conclusion

http://rfid.cs.washington.edu/
Pervasive RFID Applications

http://rfid.cs.washington.edu/

- What can we do if we tag everything?
- Seamless merging of the virtual and physical worlds

- Personal Object Tracking and Search
- Personal Time Use Diary with Analysis
- Proactive Reminder Systems
- Smart Spaces
- Activity Recognition
What’s New?

http://rfid.cs.washington.edu/

- How to design an infrastructure for pervasive RFID apps?

- Key Problems:
  
  **Shared with supply chain:**
  - Many data sources
  - Unreliable sensors
  - Massive amounts of data

  **New:**
  - Diverse, evolving applications
  - Many more distinct users
  - Data sharing and privacy
  - Less predictability
Goals: Privacy-oriented, Reliable, Extensible, Scalable

Application

Interface servers
- Streams and event detection
- Provisioning

Cluster Servers
- Privacy policies enforced
- Storage

Node Servers
- Low-level smoothing
Pilot Study

- 2 week pilot study to gain insight
  - Gen 1 technology
  - 11 readers, 34 antennas hung in hallways
  - 6 participants
  - 54 tags registered

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

- A web diary and annotation system provided ground truth
Finding: Deployment Logistics

http://rfid.cs.washington.edu/

Laboratory vs. Reality

- Significant difference between laboratory studies and reality

- Consider erroneous data and unpredictable streams
  - StreamClean system for probabilistic smoothing of data
Finding: Deployment Logistics

http://rfid.cs.washington.edu/

Antenna Mounting Configurations

Data from Benchmarking

- Consider the material properties of mounting configurations
- Leverage different kinds of redundancy

Data from Pilot Study
Finding: Privacy

- Easy inference using objects carried and time of day
  - A simple script could detect lunch breaks with > 75% accuracy

- Location privacy concerns

- Users want control of their data

- Must protect non-users as well!

- Really need a privacy policy in place during data collection
  - Physical Access Control (PAC) Policy
Deployment phase 1
- Gen 2 technology
- 35 readers, 150 antennas
- 100 tags
- Floors 2 - 6
- 200,000 TREs per week

Web application framework

Asset tracking application
Ongoing Projects

Applications
- Design and evaluation

Privacy
- Policies
- Formal methods for data privacy
- Evaluation through user studies

Reliability
- Data cleaning
- Probabilistic data management

Performance
- Stream processing
- Data model and warehousing

http://rfid.cs.washington.edu/
Conclusions

Requirements are much different than supply chain
RFID research grounded in the real world pays off

Physical challenges:
- Greater than expected
- Specific to the environment

Privacy challenges:
- Many possible models/controls
- Difficult to find evaluation metrics

System challenges:
- Inaccurate data
- Long-lived applications
- Historical data need to summarize - How?
Thank you!

Please see http://rfid.cs.washington.edu for more details

Questions?
Possibly for use in discussion.
Goal:
- Reasonable peer-level privacy policy that allows user studies
- Practical to implement
- Extensible for greater utility

**Physical access control (PAC)**
- Each user carries a personal ID tag
- Users can only obtain information about events that occurred when & where the user was physically present
- Constrains privacy concerns to those found in wearable computing
- *This is a baseline policy*: additional permissions may be granted
Fine-grained (row-level) access control is necessary for PAC

- Human activity is inherently fine-grained

Standard techniques:

- Access control lists
- Virtual Private Database (Oracle 9iR2)
- Authorization views (Rizvi, Mendelzon, Sudarshan, and Roy)

We introduce *materialized authorization views*

- Hybrid of access control lists and authorization views
Materialized PAC Views

http://rfid.cs.washington.edu/