Opportunistic Sensing: Security Challenges for the New Paradigm

Apu Kapadia, MIT Lincoln Labs
David Kotz, Dartmouth College and IISc
Nikos Triandopoulos, Boston University

Invited paper, COMSNETS 2009

Opportunistic sensing

- Leverage existing devices (e.g., cell phones)
- Carried by people, in daily life
- Large scale (millions of sensor nodes)
- Sensing human behavior or their environment

mobile node

carrier

Mobile nodes
with on-board and off-board sensors

accelerometer, light, Wi-Fi, Bluetooth

sleep

smog

Nike+ shoes

GPS

pulse-oximeter

eco-sensor
(concept)

Some systems

- CarTel (urban sensing, opportunistic networking)
- Urban Atmospheres
- Mobiscopes, Urbanet, SenseWeb
- CENS Urban Sensing
- MetroSense

at Dartmouth College

http://metrosense.cs.dartmouth.edu/

BikeNet

Ski-Scape

CenceMe

ObjectFinder

RogueFinder

AnonySense

Other applications

- Traffic (and road conditions) monitoring
- Environmental monitoring (incl. noise)
- CenceMe – social networks
- BikeNet – sensing bicycles and bike routes
- Mobile Media Metadata – maps of photos
- Locating lost objects (ObjectFinder)

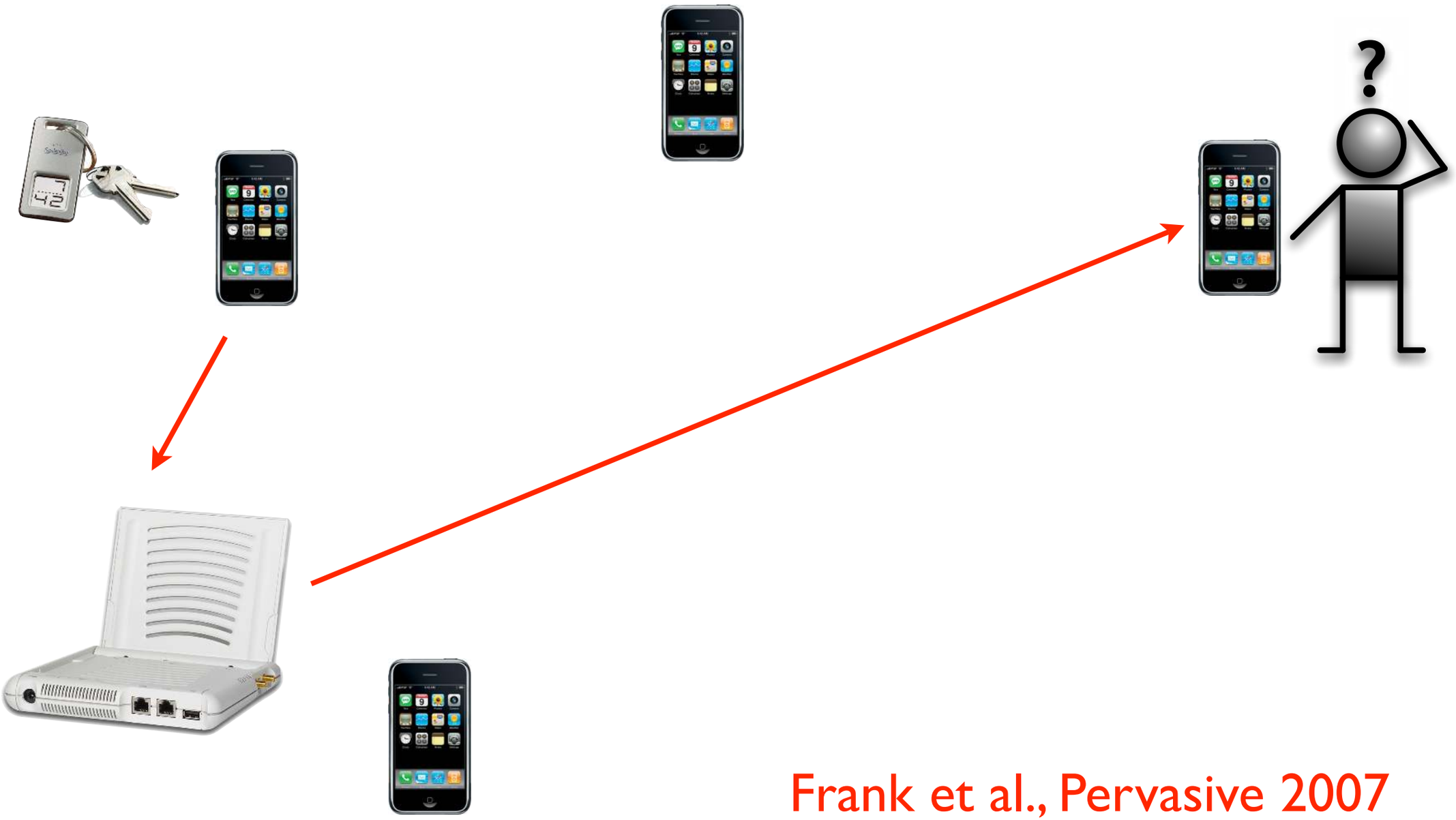
Example: ObjectFinder

Frank et al., Pervasive 2007

Example: ObjectFinder

Frank et al., Pervasive 2007

Example: ObjectFinder



Frank et al., Pervasive 2007

Contrast

"Traditional" sensor network

- sensing animals or things
- stationary nodes
- multi-hop network
- resource-limited nodes
- configured, deployed, operated by a single organization that uses the data
- simple threat model
- simple trust model

Opportunistic sensing

- sensing humans and human space
- mobile nodes
- single-hop network (WiFi, cell)
- competent nodes (e.g., phones)
- many organizations and individuals provide infrastructure, apps, and use data
- complex threat model – insider attacks likely
- complex trust model – many players

Security challenges

Confidentiality and privacy challenges

1. Context privacy
2. Anonymous tasking
3. Anonymous data reporting

Integrity challenges

4. Reliable data readings
5. Data authenticity
6. System integrity

Availability challenges

7. Preventing data suppression
8. Participation
9. Fairness

Confidentiality and privacy challenges

1. Context Privacy

The challenge:

- How do we collect and share people-centric sensor data while respecting carrier privacy?
- What *usable* abstraction and interface allows people control over their privacy? Note the wide range of sensor types and application scenarios.

Potential solutions:

- Specific solutions exist for some data types
- *Virtual walls* provides one general approach for usable access-control [Pervasive 2007]

2. Anonymous tasking

The challenge:

- How do we distribute sensing tasks to volunteer nodes and protect anonymity of node carriers?

Potential solutions:

- *AnonySense* provides anonymous tasking, under one threat model and trust model [MobiSys 2008]
- Such an approach misses opportunities for location prediction and reputation tracking to identify and task good candidates, and manage scale
- Attribute-based authentication of mobile node
- Trust negotiation (between app and mobile node)

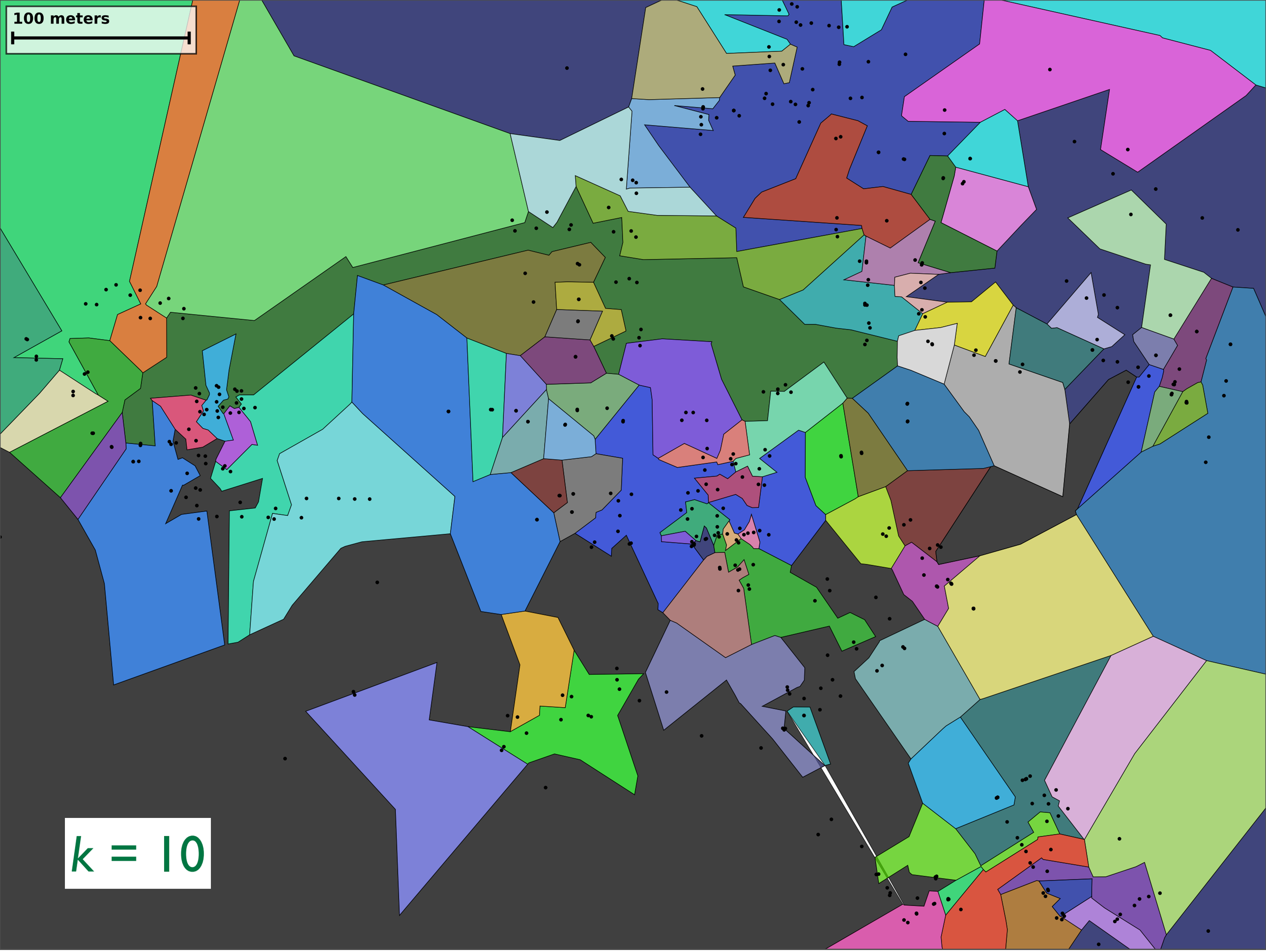
3. Anonymous reporting

The challenge:

- How do volunteer nodes submit sensor data without compromising their carrier's privacy?

Potential solutions:

- *AnonySense* provides identity and location privacy to nodes submitting sensor reports
- "Anonymizing networks" (e.g., Tor, MixMaster)
- *k*-anonymity through generalization or blurring
- Aggregation of multiple reports


100 meters
k = 10

Integrity challenges

4. Reliable data readings

The challenge:

- How do we obtain accurate, timely sensor data from untrustworthy nodes? Node carriers may be motivated to tamper with nodes, sensors, or data.

Potential solutions:

- *Trusted hardware* (TPM) can protect the software infrastructure of mobile nodes
- Redundant sensors, given sufficient sensor density, can detect anomalous readings
- Trusted sensors provide *ground truth* in some places
- Anonymous blacklisting [Tsang] can block repeat offenders from submitting future reports

5. Data authenticity

The challenge:

- How do we ensure the authenticity of sensor data, in the presence of data muling, delayed upload, and data blurring or data aggregation?

Potential solutions:

- *Group signatures* provide anonymous authentication
- Many solutions exist for secure data-aggregation in sensor networks, but none apply here
  - they all assume a static data-aggregation tree
- Need solutions for general topologies and general aggregation/blurring functions

6. System integrity

The challenge:

- How do we secure the mobile nodes from malicious tasks, or malicious system operators?
- How do we secure the sensing system from malicious applications, or mobile nodes?

Potential solutions:

- *Secure execution of mobile code* may allow mobile nodes to execute sensing tasks safely
- Trusted hardware (TPM) may allow nodes (or servers) to attest to the integrity of their software

Availability challenges

7. Preventing data suppression

The challenge:

- How do we avoid DoS caused by carriers who configure their nodes to drop tasks or reports?

Potential solutions:

- *Note that opportunistic sensing is best-effort by design.*
- Anonymous reputation systems

8. Participation

The challenge:

- What incentive do carriers have to participate, to allow their mobile node to be tasked by others?

Potential solutions:

- Seek applications with a direct benefit to the carrier
- Provide a clear representation of the privacy risk, and usable interfaces to control privacy risk and resource consumption
- *Privacy-aware hybrid payoff models* use game theory to balance users' utility from a service with privacy loss

9. Fairness

The challenge:

- How do we ensure fair allocation of system resources to multiple users and multiple applications?

Potential solutions:

- *Incentive-compatible peer-to-peer systems* research provides hints about how to prevent overuse or "free riding"

Summary

Summary

- Opportunistic sensing has great potential.
- Security and privacy challenges remain.
- Designers of opportunistic-sensing systems and applications should consider these challenges from the start.
- CS researchers should work with sociologists to understand what matters to people, and which solutions work!

Dartmouth College ISTS www.ists.dartmouth.edu

Thanks to our sponsors:

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Grant 60NANB6D6130

Grant 2006-CS-001-000001

BJA Bureau of Justice Assistance

Grant 2005-DD-BX-1091

I3P
Institute for Information Infrastructure Protection

Fellowship