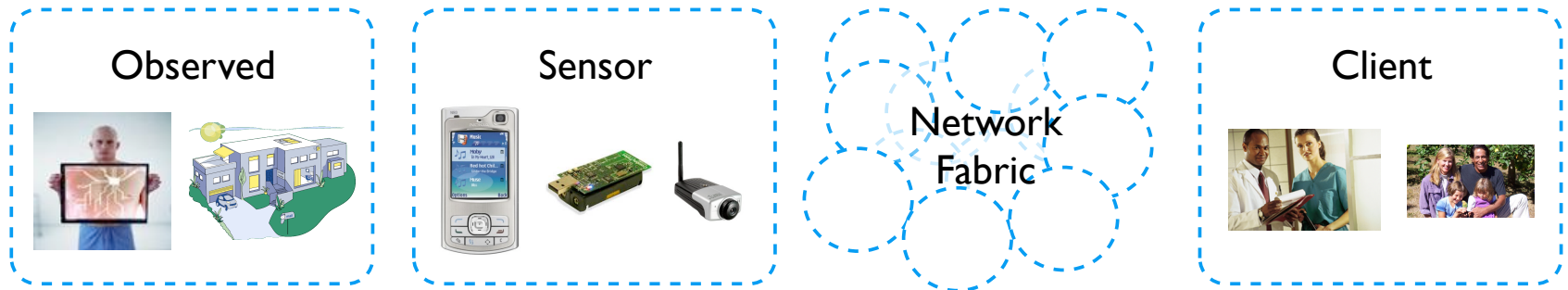


# FIND: Network Support for Selective Sharing and Verification of Sensor Data

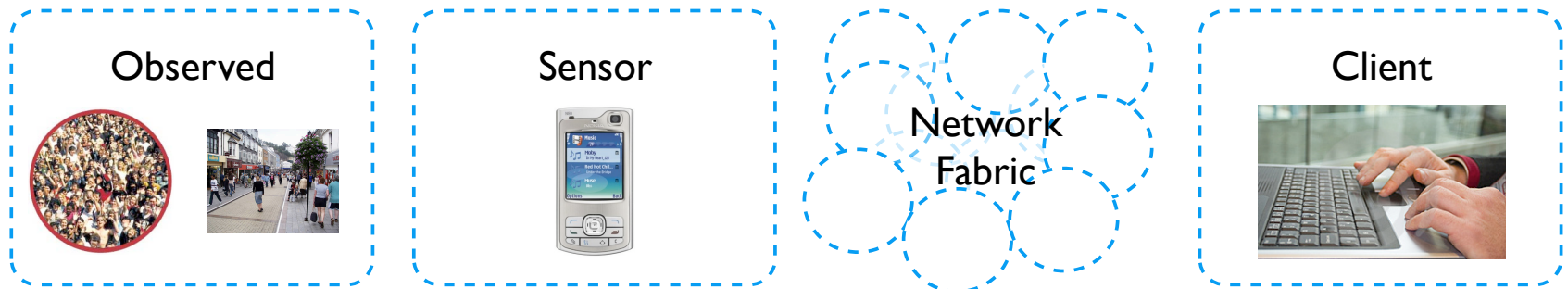
Mani Srivastava, Mark Hansen, Jeff Burke, Andrew Parker, Sasank Reddy, Ganeriwal Saurabh, Mark Allman, Vern Paxson, and Deborah Estrin

# Citizen Sensing Contexts

- Private Sensors in Private Space (personal, social)



- Private Sensors in Public Spaces (social, urban)



# Network Architecture

- Challenging questions posed by new sensing contexts require a new network architecture.

- Credibility

Network contributes to credibility of many autonomous individuals' data sources. Verified space-time context as network primitives.

- Dissemination

Make it easy for people to share and find data.

# Network Architecture

- Selecting Sharing

Respect privacy concerns of individuals while still encouraging sharing.

- Verification

Provide quality checks on data and context.

- Reliability

Aggregation-based reliability - “good enough equivalence.”

# FIND Architecture

## Mediator



Selective Sharing,  
Verification, Dissemination

## Subscriber



Data Sinks - Individual and Network Apps

## Sensor



Data Sources

## Registry



Discovery and Binding

## Client



End User Applications

# Network Components

## Sensors

- Sources of data at the edges of the network (acoustic, image, vital sign, etc...)

## Subscribers

- Sinks of sensor data.
- Individual users interested in data streams and event notifications.
- Network applications for achieving, aggregation, distillation, and signal search.

# Network Architecture

## Mediators

- Provides selected in-network functions on data streams.
- Selective sharing policy enforcement and negotiation on behalf of a publisher or subscriber.
- Performing anonymization by removing identification information.
- Verification
- Enhancing streams with attested contextual information.
- Performing simple range/proximity checks.
- Dissemination
- Stream replication and reliability

# Network Architecture

## Client

- Clients are end-users that go to sites that have already crawled or aggregated data.

## Registry

- Network entities that help subscribers discover and bind with sensor data streams.
- Provide a service similar to DNS.
- Maps the query via a tuple space search process to return a handle to the sensor data stream (or, in general, a set of handles)

# Data Privacy and Quality

Data contributors like to exercise control over resolution

- Reveal location only in terms of ZIP code
- Reveal time only in terms of hour or day
- Reveal only as part of a large enough group

Data and its context more valuable if verified

- Subscribers want to know the context of measurements were taken, and whether they can be corroborated
- Verification at a resolution the contributor is comfortable with

# Selective Sharing and Verification

## Observer's Perspective

- Enforcement of rules of sensing and sharing to preserve privacy
- Access to collected data, say in how it is shared

## Sensor's (Publisher's) Perspective

- Enforcement of rules of sharing to preserve privacy using identity and context, resolution
- Increased assurance via quality checks on published data stream, and addition of attested contextual information of specified resolution. For instance, Location, time, measurements from other sensors

# Selective Sharing and Verification

## Subscriber's perspective

- Verify validity and authenticity of sensor data and its context
- Audit trail from network
- Learn and feedback reputation of publisher

## Service Provider's perspective

- Encourage and facilitate responsible sensing and sharing practices

# Context Resolution Control

Sensor data without context is useless. But, too much context runs against desire for anonymity and privacy

Mediators control the resolution of context information revealed to a subscriber

- Deliberately reduce fidelity of location, time, and other derived context according to rules specified
- Deliberately add jitter to packets to combat fingerprinting and localization using drifts and latencies
- Add indirection to hide identity
- Different for different subscribers, or sets of subscribers

# Verifying and Attesting Context

Higher trust in context that network directly measures

- Location and time stamping of measurements
- Can be maliciously manipulated due to physical coupling
- Space-time semantics built in network fabric

Other application-specific context measured by sensors

- Verification based on application-defined rules
- Device fingerprinting

# Verifying and Attesting Context

Done near the sensors

- Exploit source proximity, physical medium, and locality
- Mediator functions in wireless APs and edge routers
- Complement statistical techniques employed closer to subscribers

# Current Work

## SensorBase.com

- A sensor logging service to store, view, and search for sensor data.

## ESP Framework

- A standard method to find sensor systems (registry) and also interact with them.

## Image/Sound Scape

- Prototypes for controlling resolution and filtering of cell phone based sensor data.