Sensor Networks and Embedded Sytems

Stephen Wicker – Cornell University
Deirdre Mulligan – UC Berkeley

Overview

- Multi-institutional, multi-disciplinary research
  - Networked Sensors
    - Public Surveillance
    - Structural Integrity
    - Medical Sensing
    - Power Systems
    - Software Tools
  - Privacy
    - Privacy policies for Public Camera Networks and Power systems
    - Privacy-Respectful Camera Networks
    - Privacy: Context vs. Content
    - Perception of Public Spaces: privacy and policing
  - Security
    - Attack Taxonomy
    - Security Co-Design
    - Trustworthy Networking

Products

- Workshops
- Publications
  - ICC, INFOCOM, MOBIHOC, IPSN, SECON, HCI, …
  - ACM Trans. On Sensor Networking
- PhD Student Exchanges between Cornell, Vanderbilt, and Berkeley
- Group Proposals for Additional Funding
  - Networking Technoloy and Systems - Networking of Sensor Systems (Nets-NOSS)
    - Cornell, Berkeley, Smith
  - CyberTRUST
    - Illinois, Berkeley, Cornell, Vanderbilt
  - San Francisco
    - Expanded Berkeley team
- Public Sector Policy Development

Research: Networking Technology

- Camera Networks
  - Platforms
  - Localization
  - Policy
- Medical Networks
  - Platforms
  - Transport Technologies
- Power Systems
  - Demand-Response
  - Transport Technologies
  - Policy
- Software Tools

Camera Motes: Overview

- Berkeley, CMU Collaboration with ITRI (Industrial Technology Research Institute) in Taiwan to design Wireless Camera Motes
  - Hardware Platform
  - Software Programming Environment
  - Library of Computer Vision algorithms for Motes
- Study Security Issues
  - High packet loss rate
  - Communication traffic specific to in-network processing for vision algorithms
  - Managing Access Permissions to Video Images

Camera Networks: Policy

- Policy Development
  - Constitution Project
  - DHS/ PIAB: privacy impact assessment
  - San Francisco; Fresno
- Policy Research
  - Public Records Act requests
    - Few policies
    - Limited articulation of purpose
    - Limited study
  - Role in policing/terrorism
    - Study of San Francisco's implementation
  - Theoretical: police and democracy
    - Relationship around technology between police, society, other branches of government
- Privacy sensitive design
  - Tracking without identity
    - Respectful Cameras
    - Motion features

Camera Localization

- Berkeley/CMU
- Goal: Many cameras viewing a scene; want to find their position and orientation with respect to each other
- Assumptions:
  - Cameras are synchronized
  - Frame rate can sample motion adequately
- Challenges:
  - No prior knowledge of the scene
  - Fixed features may not be available in pairs of cameras

Medical Sensor Networks

- Joint work between Berkeley, Cornell, and Vanderbilt (both ECE and Medical School)
- MedSN system for continuous patient monitoring
  - Wireless sensor network of medical sensors for continuous monitoring of patients
  - End-to-end solution including local fusion, real time generation of notifications, and integration with MyHealth@Vanderbilt Patient Portal and Electronic Medical Record
  - Usability and Privacy sensitive co-design
- Johnson Art Museum Testbed
  - Refinement of testbed software
  - Development of additional components for deployment of a heterogeneous network

MedSN Progress

- Explored the suitability of various technologies and architectures for the system, resulting in two appropriate scenarios
  - Tiered network utilizing several classes of network technology
    - Single-hop PAN linking sensors and intermediate nodes placed throughout the home
    - WLAN linking intermediate nodes and fusion center in the home
      - fusion center serves as generator for real time notifications
    - WAN linking fusion center and Patient Portal
  - Tiered network utilizing a 3G mobile phone
    - Single-hop PAN linking sensors and mobile phone
    - Mobile phone serves as personal fusion center and communication device

Testbed Progress

- Testbed Deployment at Cornell (supports medical effort with Vanderbilt and privacy effort with Berkeley)
  - Implementation of TinySec for MicaZ
  - Implementation of MAC layer power saving for MicaZ
  - Implementation of power aware routing in network
  - Implementation of HP Jornada based sound actuation overlay network
  - Deployment of PIR overlay network using Crossbow security motes
- Joint Publications

Power Consumption and Privacy

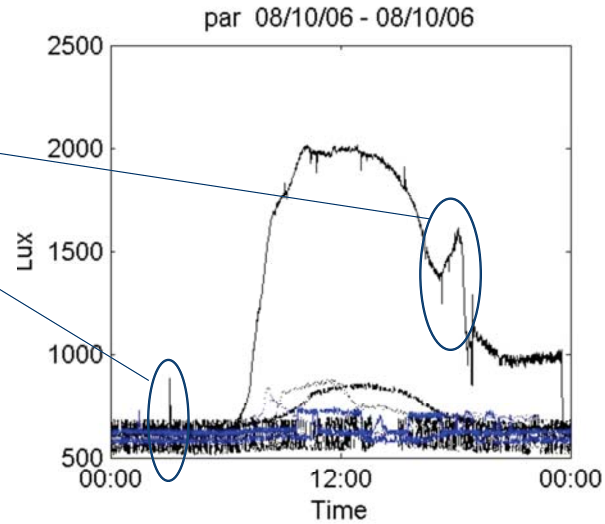
- Joint effort between Berkeley, Cornell, Smith, CMU
- SCADA: Supervisory Control and Data Acquisition
  - Acquire power consumption data
    - Improve efficiency of power markets
    - Improve reliability of power system
    - Implement demand/response mechanisms
- Increased interest in greater resolution
  - Finer grained control over small generators
  - Better predictive capability for demand/response systems
- Privacy issues
  - Sensor acuity and revelation of private information
    - Home, employees, business information
  - Law, regulatory and standard reform proposals
    - Privacy protective data mining
    - Data retention and use policies
    - Device specifications
- Joint Nets_NOSS Microgrid Proposal

Problem

- Power grid is not completely elastic
  - Household and business activities reflected in variations in power consumption
  - Demand variations are visible on local lines as fluctuations in current and voltage
- Power demand over time reveals personal activities
  - Sleep habits
  - Work habits
  - Presence of certain medical equipment
  - Some illegal activities (Kyllo)
- New players, new configurations create new opportunities for use, disclosure and manipulation of information
  - Patchy regulatory and legal structure
  - Limited attention to security or privacy in architecture
  - Benefits of data being limited by privacy concerns
  - Potential public policy nightmare if breach occurs

Revealing Data…

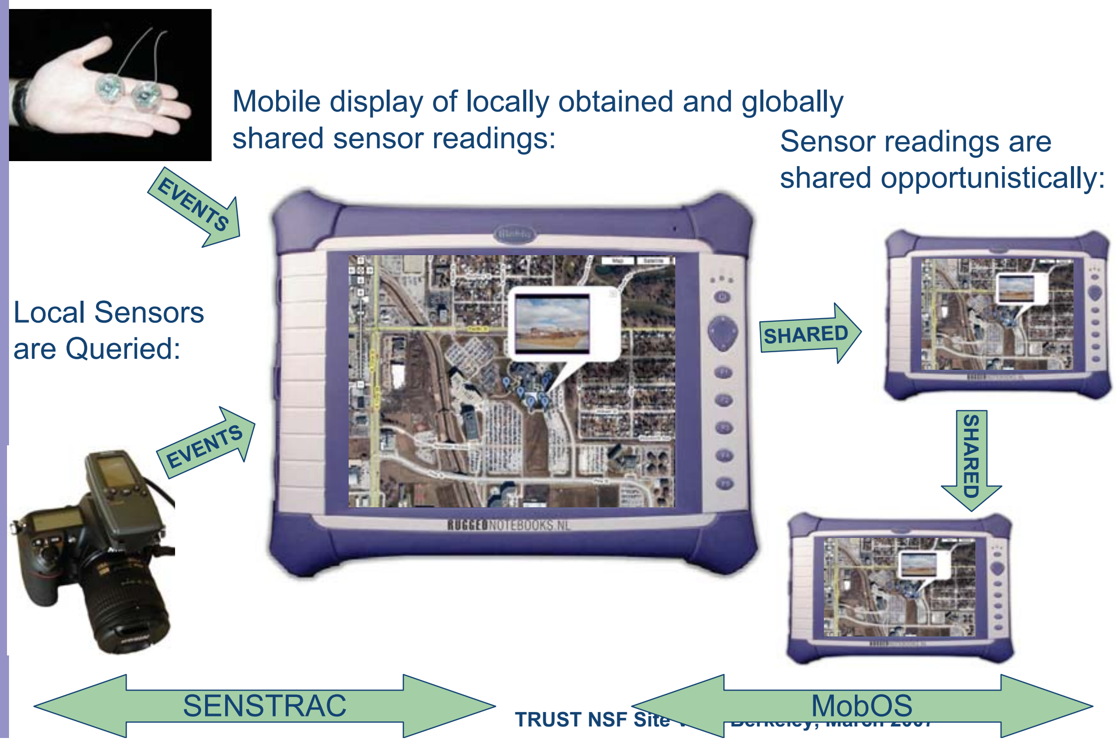
- Light sensors provide indication of power usage associated with lights.
  - We know when everyone goes to bed.
  - Here we see Dad getting up to take care of baby.
- Data from Nathan Ota, UC Berkeley
- Similar data sets obtained by Adrian Perrig, CMU



Software Tools: Research Goals

- Building systems that provide the end user with well known abstractions for deploying sensor networks and embedded systems:
- Secure, opportunistic file system for mobile ad-hoc networks (MobOS)
  - Effectively and securely share data in the absence of traditional all-to-all wired network infrastructure
- Publish/Subscribe system to query sensor nodes from a mobile node (SENSTRAC)
  - Users subscribe to sensor or interest, and sensor publish sensor readings
  - Which sensors to query changes as the user moves through the area.

Sharing of sensor readings in real time



Privacy

- Integral Part of Previous Technology Projects
- Additional Foci
  - Camera Networks
  - RFID
  - Public Perception
  - Testbeds
    - Johnson Art Museum, Cornell Campus
    - San Francisco

A Look at Privacy and Security in the Network

- Privacy Issues with Public Sector Camera Networks
  - Policing, technology and democracy
    - theory
    - Policies, procedures, system design
  - Expectations of people
  - Technical Solutions
    - De-identification (person/background
    - Abstraction of data (ex. Symbols, numbers..)
- Security Issues and Attacks in Camera Networks
  - Means to secure network and data
  - Attacks:
    - Physical Tampering
      - Removing/disabling camera
      - Feedback Loop
    - Tampering with data sending/Storage
      - Encryption attacks
      - Watermarking attacks

Respectful Cameras

- Joint work with: Jeremy Schiff, Ken Goldberg, Jennifer King, and Deirdre Mulligan
- Goal: Method of privacy protection by de-identifying faces of people in the scene

- Adaboost
- Statistical Classifier
  - Training Phase
    - Input is features and labeled data
  - Classifying Phase
    - Pixel -> "marker" / "no marker"
  - Linear function of weak classifiers
- Situational interviews to determine effect on perceptions of risks and benefits

Privacy in Sensor Networks: Transactional Confidentiality (I)

Sameer Pai, Marci Meingast, Tanya Roosta, Sergio Bermudez,
Stephen Wicker and Shankar Sastry; Cornell & UC Berkeley

Overview Of Devices Used In A Sensor Network

- Motes: Low-cost, low-power, limited memory, low-bandwidth, miniature data-gathering devices
- Sensors are a set of transducers
  - Light, temperature, barometric pressure, magnetometer, etc.
  - Biosensors with biomimetic membrane attached to a transistor gate
  - Sensors can also be cameras and other capture devices
- Wireless communication and processing via a radio processor board
  - Multihopping communication (no central authority)
  - Limited processing power

Sensor Network Privacy

- Privacy is "the state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right"
- Sensor network privacy preservation can be broken into two components:
  - Content Confidentiality
    - Based explicitly on the contents of messages
  - Transactional Confidentiality
    - Based implicitly on the communication and routing of messages
    - This is rarely the focus of current literature on sensor network privacy

Content Versus Transactional Confidentiality

- **Content** is the meaning of information contained within data flowing in the network
- **Content confidentiality** entails disallowing those external to network from accessing the meaning of network data
- **Transactional information** is information gathered as a consequence of generation, transmission, and routing of data in the network
- **Transactional confidentiality** entails disallowing adversaries from inferring network application information from the creation and flow of network data

Transactional Confidentiality In Public Policy and Law Literature

- Our definition of transactional confidentiality is similar to transactional confidentiality/privacy in Public Policy and Law Literature
  - Internet based examples
    - Click-trails, clickstreams, cookies, web bugs, file-access logs
  - Cellular Network example
    - Cell-phone usage records
    - Legislation to criminalize phone record theft and use
- Lack of literature considering this type of privacy for sensor networks

S. Pai, M. Meingast, T. Roosta, S. S. Sastry, S. Wicker "Privacy in Sensor Networks: A Focus On Transactional Information," Submitted to IEEE Security and Privacy Magazine, 2006

Security

- Taxonomy
- Co-Design

Taxonomy of Security Attacks in Sensor Networks

Tanya Roosta, Alvaro Cardenas, Shiuhpyng Shieh, Shankar Sastry, UC Berkeley

Motivation

- Unique challenges:
  - Random Topology
  - Secure aggregation
  - Context privacy
  - Scalability of security schemes
  - Power and computation efficiency
    - e.g. Code size of the security algorithm

Security Objectives

- Confidentiality
- Authentication
- Integrity
- Freshness
- Secure Group Management
- Availability
- Graceful degradation

Attacks on Protocols/Applications

- Denial of service attacks
- Traffic analysis
- Key management protocols
- Sybil Attack
- Reputation-Assignment Schemes
- In-Network Processing
- Time Synchronization Protocols

Threat Model/Trust Model

- Mote-class Attacker
  - Controls a few ordinary sensor nodes
  - Attacker has the same capabilities as the network
- Laptop-class Attacker
  - Greater battery & processing power, memory, high-power radio transmitter, low-latency communication
  - The attacker can cause more serious damage

Cryptography

- Cryptography is the first line of defense
- Schemes in sensor networks:
  - TinySec: symmetric key cryptographic algorithm
  - TinyECC: Elliptic Curve Cryptography (ECC)
- Cryptography can solve many security problems (e.g. authentication) but not all, e.g.
  - Traffic analysis
  - Captured nodes

Time Synchronization Attacks

- Time synchronization is critical piece of infrastructure for sensor networks
- Effect of attacks on applications/services:
  - Localization
  - TDMA-based Channel Sharing
  - Estimation: tracking
- We are currently implementing the attacks on a real test-bed and are evaluating their effects on the tracking application

Threat Model/Trust Model (cont.)

- Outsider Attacks
  - Passive eavesdropping
- Insider Attacks: compromised node
  - Node runs malicious code
  - The node has access to the secret keys
- The only trust assumption is that the base station is trustworthy

Attacks on the Sensor Mote

- *Non-invasive*: The embedded device is not physically tampered with
  - Side-channel attack
- *Invasive*: Reverse engineering followed by probing techniques to extract cryptographic keys and exploit software vulnerabilities
- Countermeasures:
  - Randomization
  - Hardware tamper-resistance

Extending the Taxonomy

- Define metrics to quantify the following security requirements:
  - Confidentiality
  - Integrity
  - Availability
- Defining an analytical frameworks based on:
  - The goal of the adversary
  - Goal of the administrator
  - Capabilities of the adversary and the administrator
  - Cost of different attacks

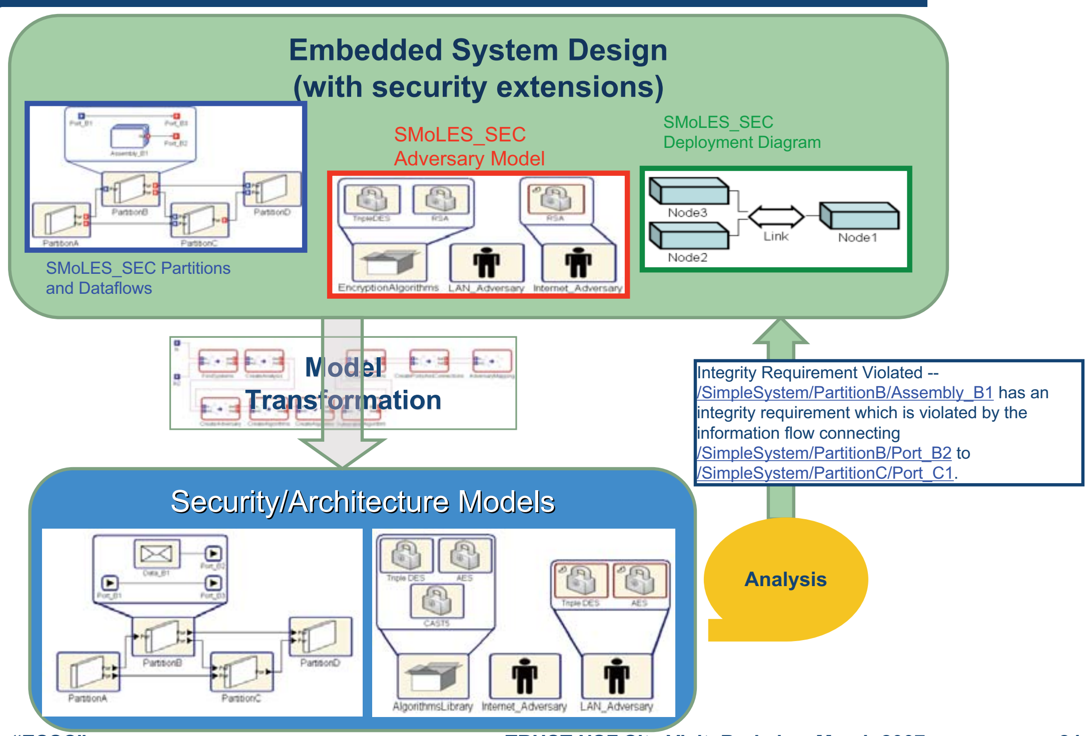
Embedded System Security Co-Design

- Vanderbilt
- Embedded (a.k.a. cyber-physical) systems **must** be designed with security considerations in mind
  - Interactions between embedded system properties (response-time, bandwidth, data lifetime) and computer security issues
  - Co-design: security and para-functional aspects are interwoven in the design and need to be addressed together
- Research topics
  - Design and implementation of security modeling aspects in DSMLs
  - Security property verification of design-models
  - Metamodel composition for integrating security modeling into embedded system design languages
- Students:
  - Matt Eby, US
  - Jan Werner, Poland

Research Products

- Education Contributions:
  - Courseware material – Learning modules on the TAO Portal
    - Security in Embedded System Design - Security Modeling and Analysis
    - Security in Embedded System Design - Role-based Access Control in Embedded System Models Case Study
    - Security in Embedded System Design - Security Modeling and Analysis Case Study
- Software tools:
  - SMAL: Security Modeling and Analysis Language: Modeling language and Analysis Tool
  - SMOLES-SEC: A Simple Modeling Language for Embedded Systems with Security Extensions
  - SMOLES-SEC/SMAL: Integrated toolchain

Embedded System Security Design Modeling and Analysis- Toolchain



Reputation/Trust Systems For Sensor Networks: Towards Intelligent Design & Game Theoretic Analysis

General Reputation System

Building blocks of a reputation system are:

- Reputation systems can be used to identify corrupted nodes
- "watchdog" and "Second hand information" mechanisms identify bad behaviors, and they are is application dependent

Sensor Network Applications

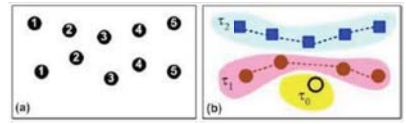
In sensor networks, reputation systems can be effectively used to improve:

- Intrusion Detection
- Data Quality Assessment
- Confidentiality Protection
- Tracking
- Routing

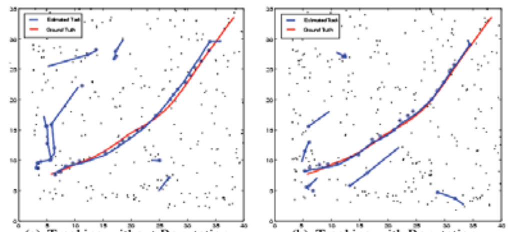
Components of Our Approach

Our reputation system consists of the following components:

- Do a robust cleaning of the data
- Detect the node type
- Dynamic update of the node type



S. Oh, S. Russell, and S. Sastry. "Markov Chain Monte Carlo Data Association for General Multiple-Target Tracking Problems"



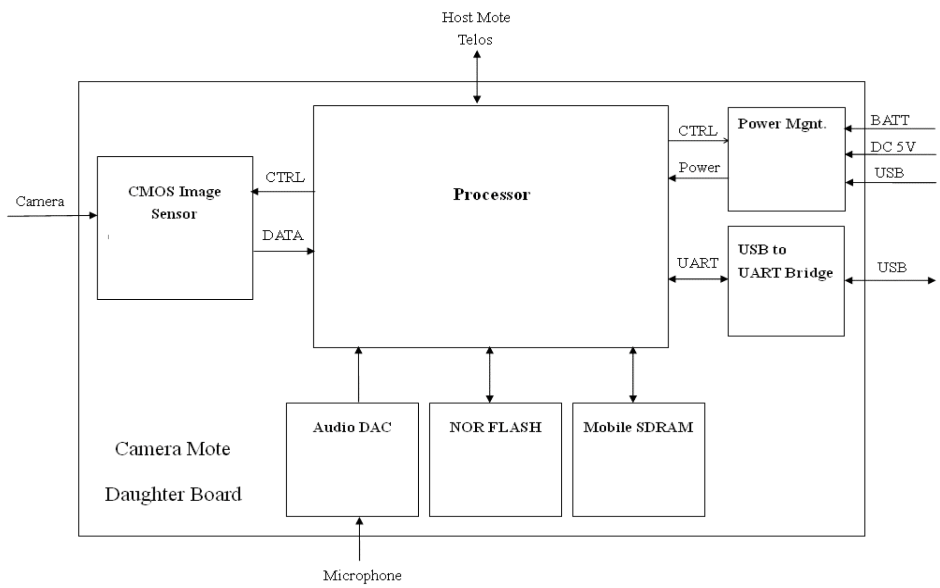
(a) Tracking without Reputation (b) Tracking with Reputation

Tanya Roosta, Marci Meingast, Shankar Sastry. "Distributed Reputation System for Tracking Applications in Sensor Networks". In proc. of International Workshop on Advances in Sensor Networks 2006, San Jose, CA.

TRUST/ESN Emphases in 2007-2008

- Cross-Layer Integration
  - Technology + Software + Testbeds + Policy
- Increased multi-institutional use of sensor networking testbeds
  - Expansion of Cornell testbed
  - Health care facility testbed in Nashville
- Increased PhD student exchange
  - Significant impact on join publications
- Policy development
  - Camera networks
  - Power monitoring

Camera Mote Daughter Board



Source: ITRI

Camera Mote Characteristics

- Loose Restrictions on Computation, Power, Memory, Camera Resolution
- Use Physical/Data Link Layers that more easily enable Mesh-Networking
  - IEEE 802.15.4
  - Scalability (network size)
- Closer to Real Platform than Conglomeration of Parts
  - Remove USB communication
- Not focused on developing novel OS/Abstractions
  - 1 MCU for image processing, 1 MCU for networking
- Multi-Sensor Fusion
  - Focus on microphone + video
  - Multi-tier may be incorporated later

Motion Features

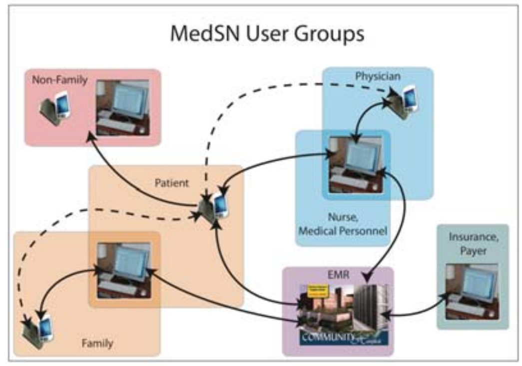
- Motion features to localize
  - Not as effected by lighting conditions
    - Except at extreme illuminations
  - Can work when no fixed features are identifying enough
    - Outdoor environments
    - Non-textured Backgrounds
    - No distinguishing features
  - Can be used with different projection models
    - Heterogeneous camera setup in testing

Motion Features

- Spatio-Temporal Volumes:
  - Same type of action (i.e. walking, running) seen in two cameras
  - Build a spatio-temporal volume from the images of the sequence
  - Find the affine transformation that aligns the sequences
- Drawbacks:
  - Cannot handle out of plane rotation of cameras

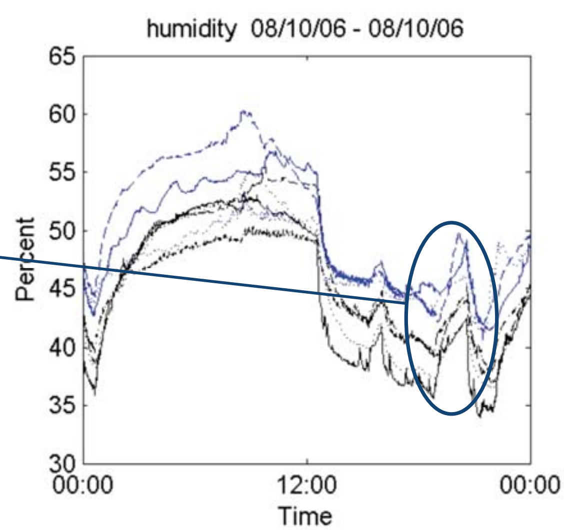
MedSN Progress

- Examining various models for users involved and their method of access/integration in system
  - Physician and support staff
  - Patient
  - Patient family
  - Non-family
  - Insurance/Payer
- Collaborative effort with Vanderbilt, Berkeley
- Agreement for testing at Nashville assisted living facility
- Joint Publications



Related Data

- Humidity data is useful when air conditioners are in use.
  - Increased efficiency
  - Also indicates when people are talking



Privacy in Sensor Networks: Transactional Confidentiality (II)

Sameer Pai, Marci Meingast, Tanya Roosta, Sergio Bermudez,
Stephen Wicker and Shankar Sastry; Cornell & UC Berkeley

Transactional Confidentiality In Engineering Literature (I)

- Transactional information can be gathered using multiple methods:
  - Carrier frequency of communication

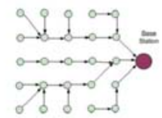
Photo	Commonly Used Name	Frequency Range
	MICA (sometimes refered to as MICA1)	902 to 928 MHz 433.1 to 434.8 MHz
	MICA2	868 to 870, 902 to 928 MHz 433.1 to 434.8 MHz 313.9 to 316.1 MHz
	MICA2DOT	868 to 870, 902 to 928 MHz 433.1 to 434.8 MHz 313.9 to 316.1 MHz
	MICAz	2400 to 2483.5 MHz
	Cricket	433.1 to 434.8 MHz

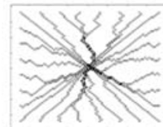
Transactional Confidentiality In Engineering Literature (II)

- Transactional information can be gathered using multiple methods:
  - Message generation
    - Rate and time of message generation can give information of the events being monitored by network
  - Message size
    - In-network aggregation and dynamically changing message size can inform an external observer about network and what it is monitoring

Transactional Confidentiality In Engineering Literature (III)

- Transactional information can be gathered using multiple methods:
  - Routing
    - Allows for tracing of messages to a source or sink node within the network by an external observer





Examination of Transactional Privacy In Existing Sensor Systems

- Health Care Applications
  - Examination of Harvard's CodeBlue medical sensor network
- Energy Usage Monitoring
  - Examination of Dezem System for Monitoring Electrical Energy Consumption
- Monitoring Environmental Phenomena
  - Examination of Greater Duck Island habitat monitoring system

A Public Art Museum Deployment of a Sensor Network Testbed

Sameer Pai, Kirsten Boehner, Phil Kuryloski, Stephen Wicker, Geri Gay
Cornell

Goal:
Actuate on collected data by providing real-time feedback to individuals within the museum.

Goal:
Understanding the implications of individual privacy brought out by the public-space deployment of increasingly higher fidelity sensor systems.

Goal:
Act on these implications in the design of the system by protecting user privacy using multiple methods and continually iterate value-sensitive design process

User Feedback

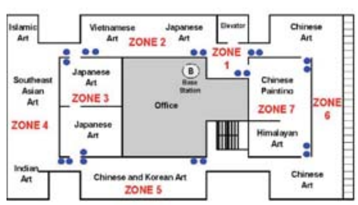
Second tier of networked Jornada PDAs equipped with stereo speakers are used to play sound clips based on collected data

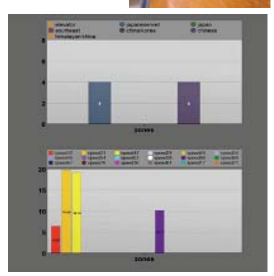
The Jornadas collectively generate an artistic soundscape based on real-time data that is collected by the sensor network.

Network actuation allows for user feedback and human-computer interactive system control.

Privacy protections:

- No collection of Personally Identifiable Information
- Confidentiality Protected (Encryption, Authentication, and Rapid Deletion of Data)
- Notifications of data collection
- Consent sought to collect data





S. Pai, G. Gay, S. Wicker, and K. Boehner "A Sensor Network Testbed in a Public Museum Space: Technology, Art, and the Privacy Horizon," Submitted to the 5th International Conference on Pervasive Computing, May 2007

TRUST for Large Scale Sensor Networks

Signal processing and Information Theoretic Perspectives

Lang Tong, T. He, P.Venkitasubramaniam, and O.Kosut
School of Electrical and Computer Engineering, Cornell University

Objectives

- Investigate fundamental limits on sensing, communications, and networking in the presence of Byzantine sensors.
- Develop robust algorithms to detect abnormal traffic patterns
- Design networks with secrecy constraints.

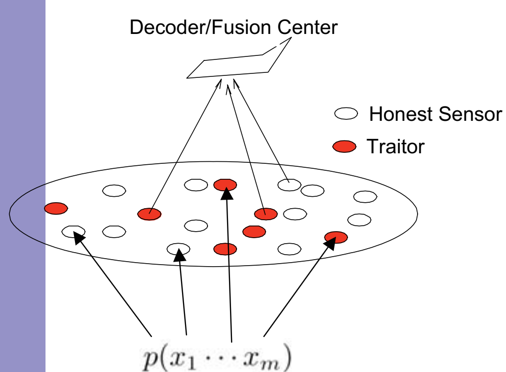
Publications

- 1 J. paper to appear, 2 submitted, 6 conference papers.

Accomplishments

- Distributed source coding in the presence of Byzantine nodes.
- Capacity of cooperative sensing in the presence of Byzantine nodes.
- Developed robust algorithms for stepping-stone attacks
- Developed scheduling algorithms to hide routing information
- Testbed development for mobile sensing

Distributed Source and Channel Coding in the Presence of Byzantine Sensors



Approach

- Information theoretic approach to characterize fundamental limits.
- Variable-rate coding with randomized transmissions

Challenges

- Fusion center collects information from network of sensors or embedded systems over noisy channels
- An unknown number sensors are reprogrammed by malicious intruder

Results

- Source coding:
  - Achievable SW region for fixed rate encoders.
  - All achievable sum rates for variable rate encoders.
- Capacity for collaborative fusion.

O. Kosut and L. Tong, "Distributed source coding in the presence of Byzantine sensors", submitted to IEEE IT transactions, Feb 2007
O. Kosut and L. Tong, " capacity of cooperative fusion in the presence of Byzantine sensors, " Allerton'06 Oct. 2006

Techniques to Secure Routing

- Prevention
  - Harden protocols by restricting participants' actions
  - Typically employs cryptography
  - Only forestalls known attacks
- Detection & Recovery
  - Monitor behavior for malicious activity
  - Eliminate malicious participants
  - Must be able to distinguish anomalous behavior and accurately assign blame
- Resilience
  - Maintain availability even under unpredicted attacks
  - Provide graceful performance degradation

Secure Sensor Network @ CMU

- Funded students
  - Cynthia Kuo (US citizen)
  - Abhishek Jain (citizen of India)
- Research emphasis
  - Sensor network privacy
  - Secure sensor network communication
  - Secure sensor network routing

Privacy Issues

- Miller v. United States
  - No privacy interest in data held by 3rd parties
- Indifference: The technologists don't care
  - "So we have to spend more time with lawyers?"
    Leaders of SCADA standards body, 2006
- Ability to structure architecture and policy to limit privacy and security risks while gaining information to aid in conservation and load control efforts
- Two way channel into the home and businesses with the ability to control appliances