Berkeley Engineering

Educating Leaders. Creating Knowledge. Serving Society.

Embedded Intelligence: Sensor Networks and Beyond

Shankar Sastry

Dean of Engineering

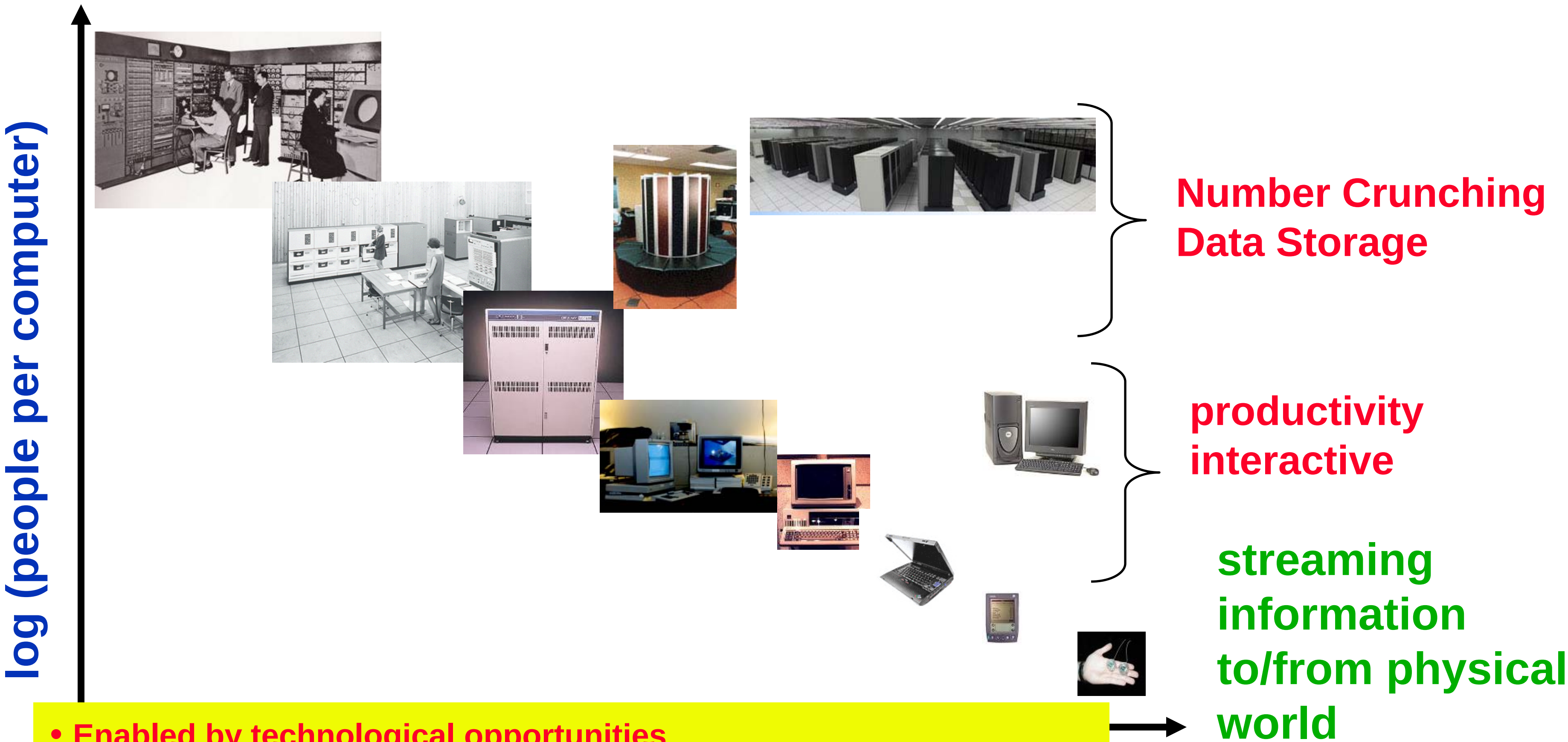
University of California

Berkeley CA

CITRIS

er for Information Technology Research in the Interest of Society

Bell's Law –
new computer class per 10 years

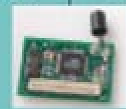


- Enabled by technological opportunities
- Smaller, more numerous and more intimately connected
- Ushers in a new kind of application
- Ultimately used in many ways not previously imagined

Outline

- Tech Push: operating systems, hardware, programming, networking
- Applications Pull: Instrumenting the World
- Whither Wireless Sensor Networks: Multi-target tracking and Pursuit Evasion Games
- Heterogeneous Sensor Networks, Camera networks, health care
- Expanding the Vision: 1000 Radios a Person
- Closing the Loop: Cyber Physical Computing
- Attacking Sensor Webs: Cybersecurity

Mote Evolution

Mote Type Year	*WeC* 1998	*René* 1999	*René 2* 2000	*Dot* 2000	*Mica* 2001	*Mica2Dot* 2002	*Mica 2* 2002	*Telos* 2004
								
Microcontroller								
Type	AT90LS8535		ATmega163		ATmega128			TI MSP430
Program memory (KB)	8		16		128			48
RAM (KB)	0.5		1		4			10
Active Power (mW)	15		15		15		60	0.5
Sleep Power (μW)	45		45		75		75	2
Wakeup Time (μs)	1000		36		180		180	6
Nonvolatile storage								
Chip	24LC256				AT45DB041B			ST M24M01S
Connection type	I^2C				SPI			I^2C
Size (KB)	32				512			128
Communication								
Radio	TR1000				TR1000	CC1000		CC2420
Data rate (kbps)	10				40	38.4		250
Modulation type	OOK				ASK	FSK		O-QPSK
Receive Power (mW)	9				12	29		38
Transmit Power at 0dBm (mW)	36				36	42		35
Power Consumption								
Minimum Operation (V)	2.7		2.7		2.7			1.8
Total Active Power (mW)	24				27	44	89	38.5
Programming and Sensor Interface								
Expansion	none	51-pin	51-pin	none	51-pin	19-pin	51-pin	10-pin
Communication	IEEE 1284 (programming) and RS232 (requires additional hardware)							USB
Integrated Sensors	no	no	no	yes	no	no	no	yes

Berkeley Open Experimental Platform

- **Focused on low power**
- **Sleep - Majority of the time**
  - Telos: 2.4µA
  - MicaZ: 30µA
- **Wakeup**
  - As quickly as possible to process and return to sleep
  - Telos: 290ns typical, 6µs max
  - MicaZ: 60µs max internal oscillator, 4ms external
- **Process**
  - Get your work done and get back to sleep
  - Telos: 4MHz 16-bit
  - MicaZ: 8MHz 8-bit
- **TI MSP430**
  - Ultra low power
    - » 1.6µA sleep
    - » 460µA active
    - » 1.8V operation

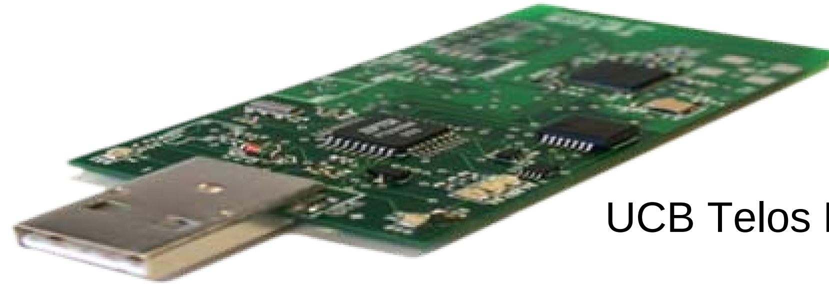
- **Standards Based**
  - IEEE 802.15.4, USB
- **IEEE 802.15.4**
  - CC2420 radio
  - 250kbps
  - 2.4GHz ISM band
- **TinyOS support**
  - New suite of radio stacks
  - Pushing hardware abstraction
  - Must conform to std link
- **Ease of development and Test**
  - Program over USB
  - Std connector header
- **Interoperability**
  - Telos / MicaZ / ChipCon de

UCB Telos

Xbow MicaZ

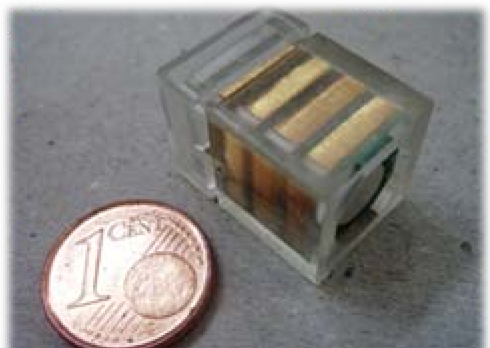
Major Progress Over Past Years

Philips Sand module

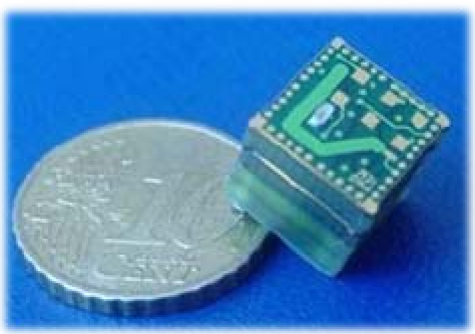


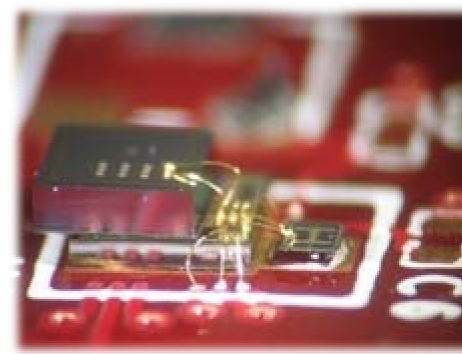
UCB Telos Mote

UCB PicoCube



IIMEC e-Cube



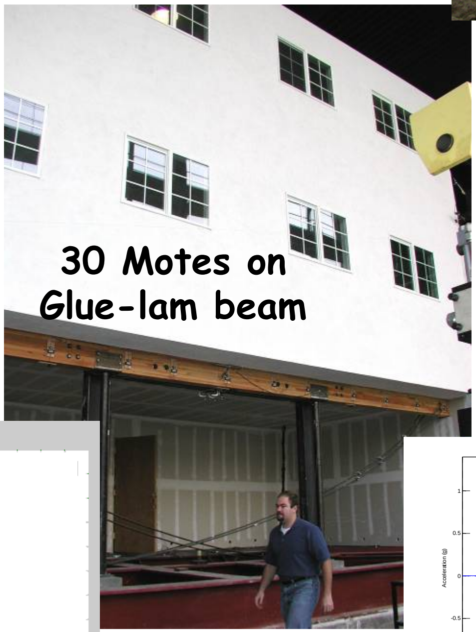


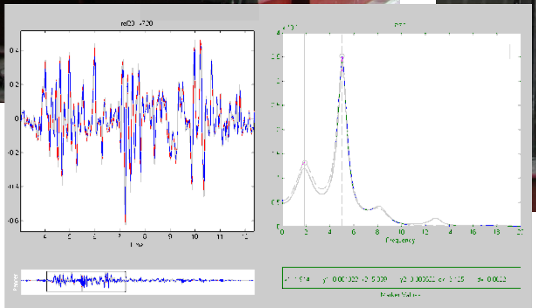
UCB mm^3 radio

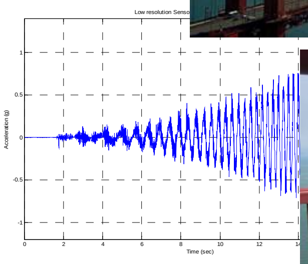
[Ref: Ambient Intelligence, W. Weber Ed., 2005]

Structural Monitoring
Glaser, Fenves

- **Dense Instrumentation of Full Structure**
  - Cost is all in the wires
- **Leads to in situ monitoring**
- **Self-inspection and Diagnosis**

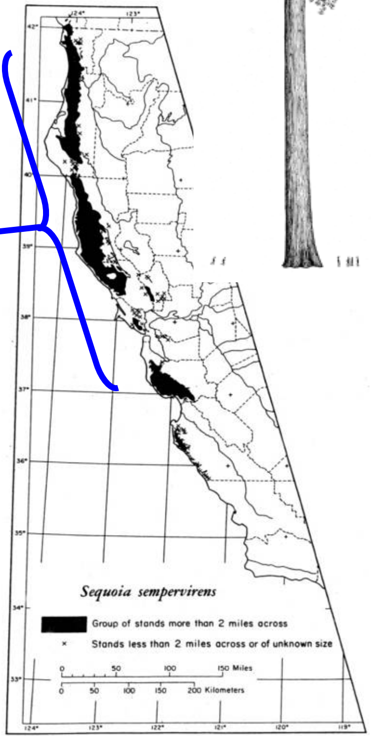


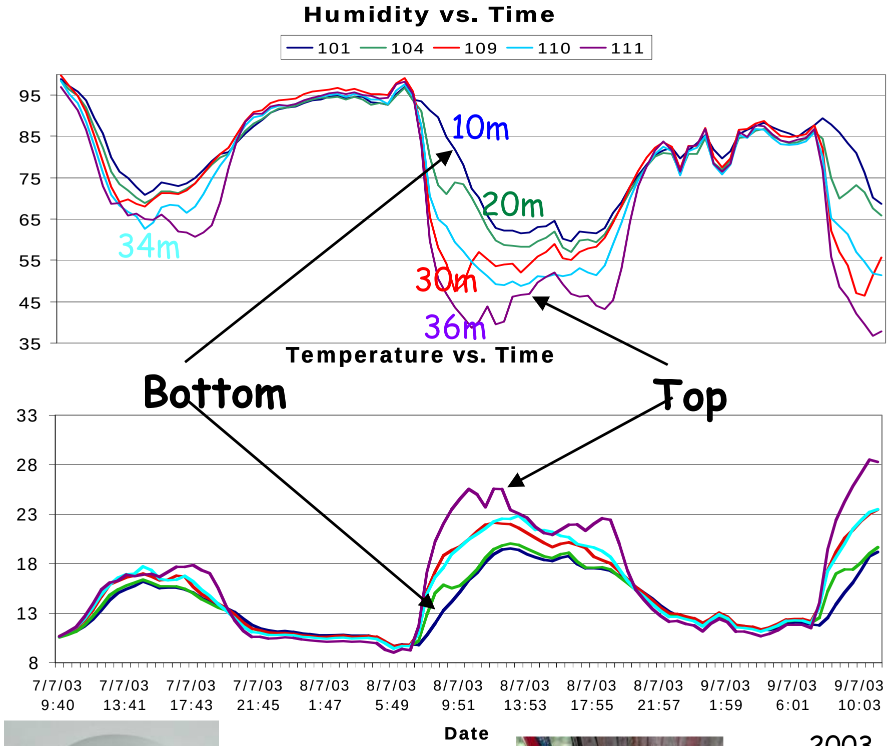


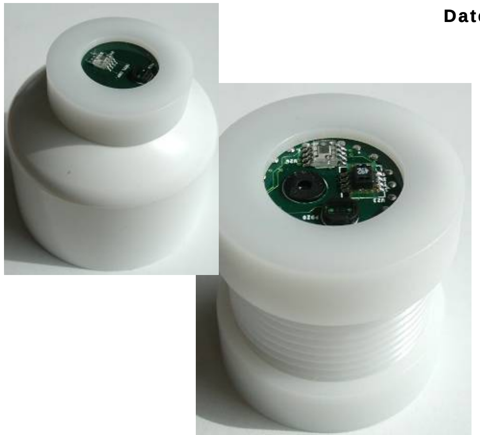


Forest Ecophysiology
Dawson

- **How TREES shape the hydrological cycle?**
  - 2/3 of fresh H2O recycled through forests
- **Microclimatic Drivers of Plant Dynamics**
- **Influence climate**



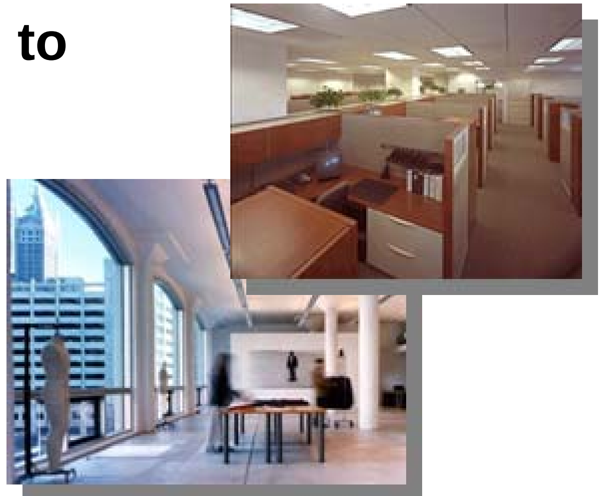


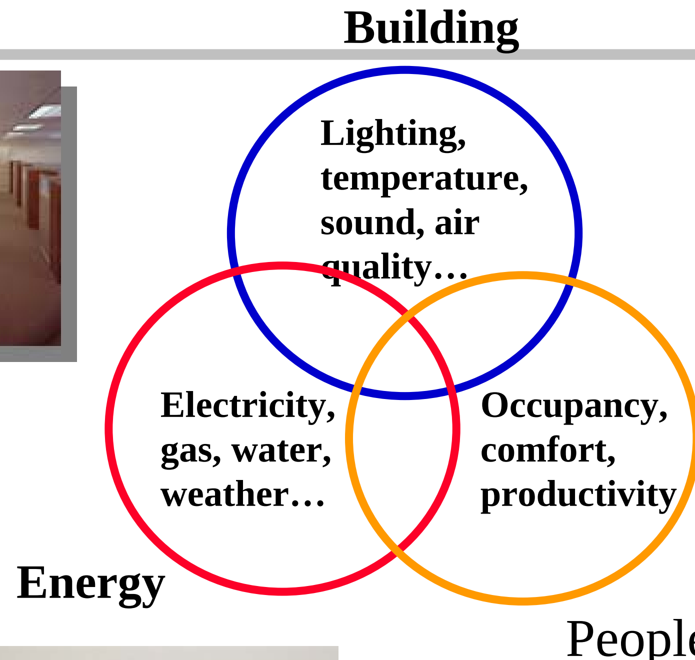


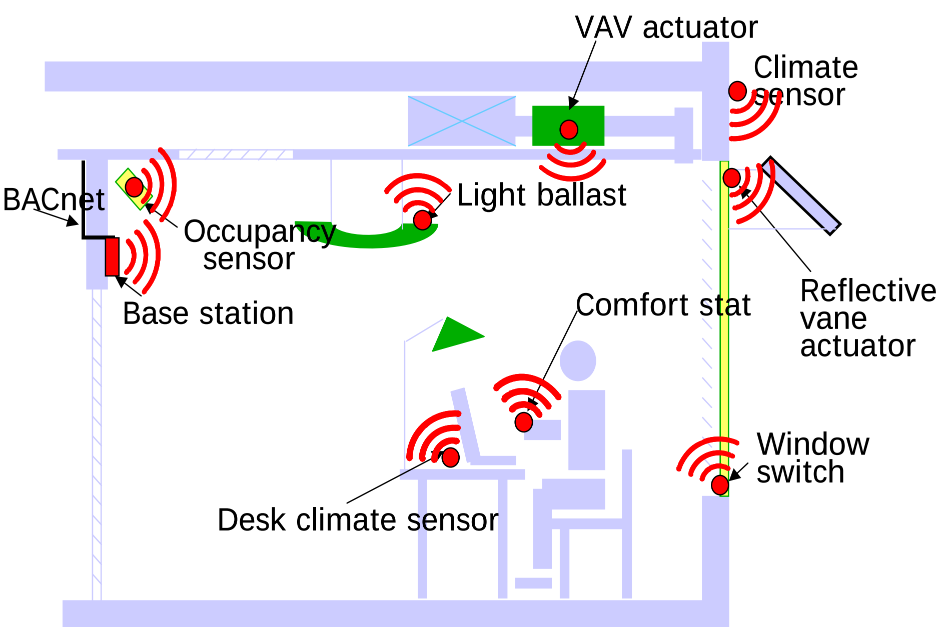
2003, unpublished

Built Environments
Arens

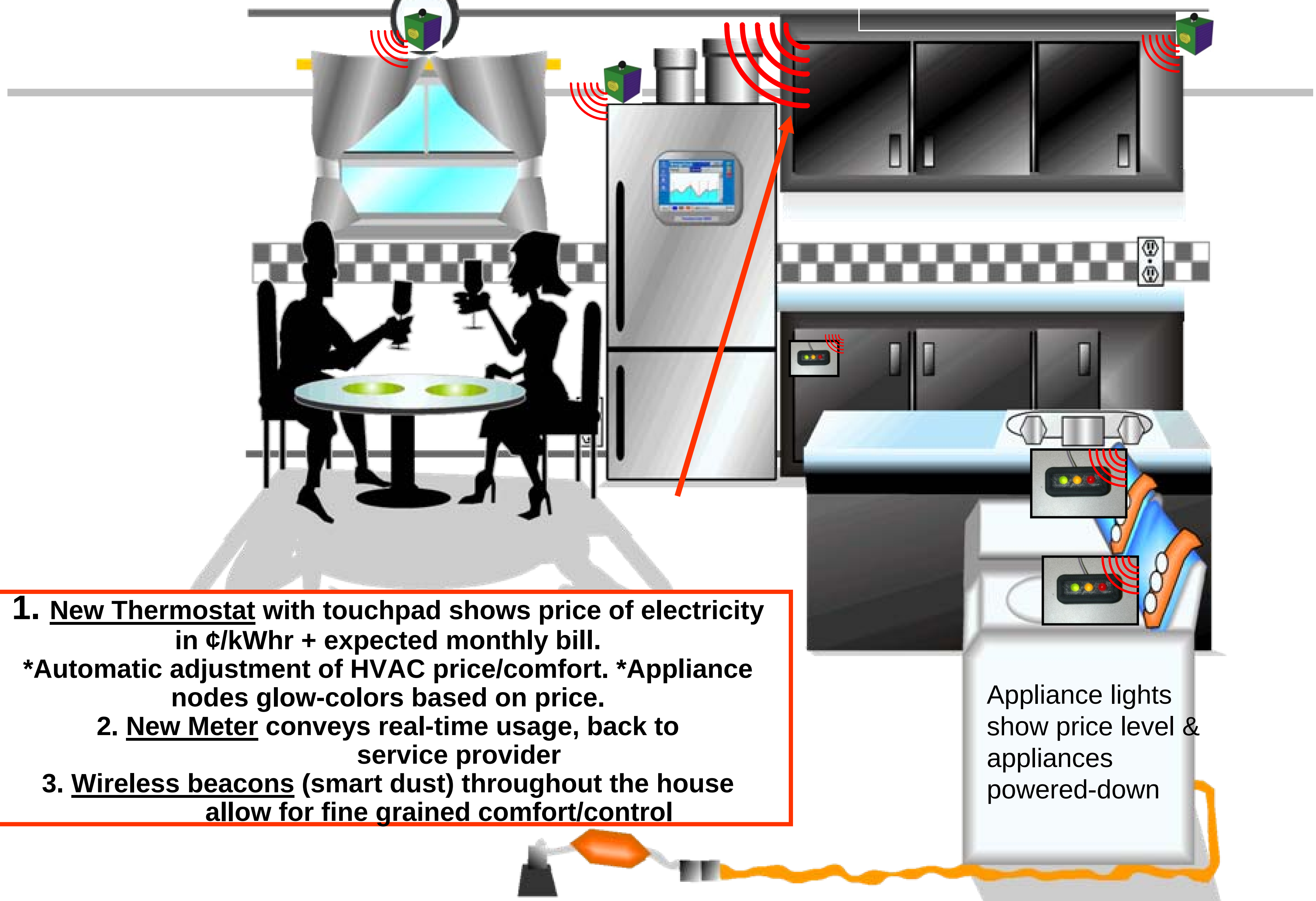
- **2/3 of US energy used to maintain our bldg environment**
  - 40% lighting
- **Inefficient, unhealthy, uncomfortable due to lack of sensing and control**







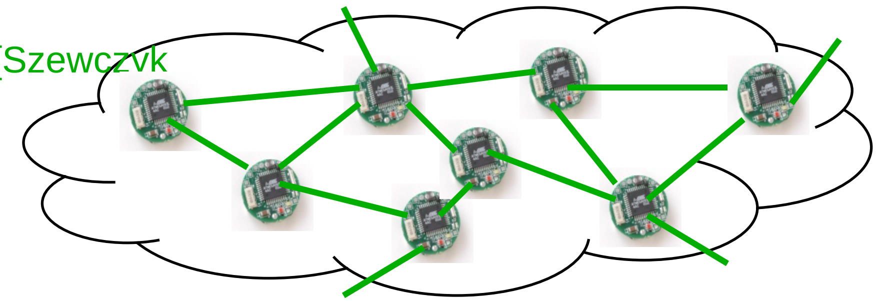
Demand Response in a "smart home"

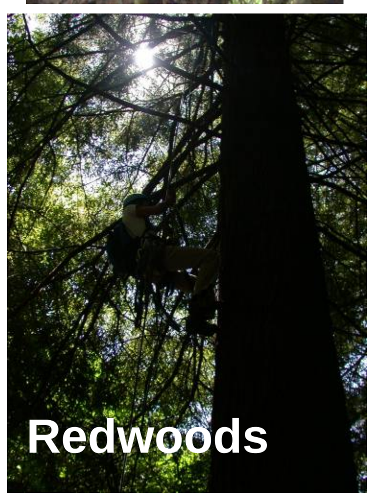


1. **<u>New Thermostat</u> with touchpad shows price of electricity in ¢/kWhr + expected monthly bill.**
***Automatic adjustment of HVAC price/comfort. *Appliance nodes glow-colors based on price.**
2. **<u>New Meter</u> conveys real-time usage, back to service provider**
3. **<u>Wireless beacons</u> (smart dust) throughout the house allow for fine grained comfort/control**

Ubiquitous Instrumentation

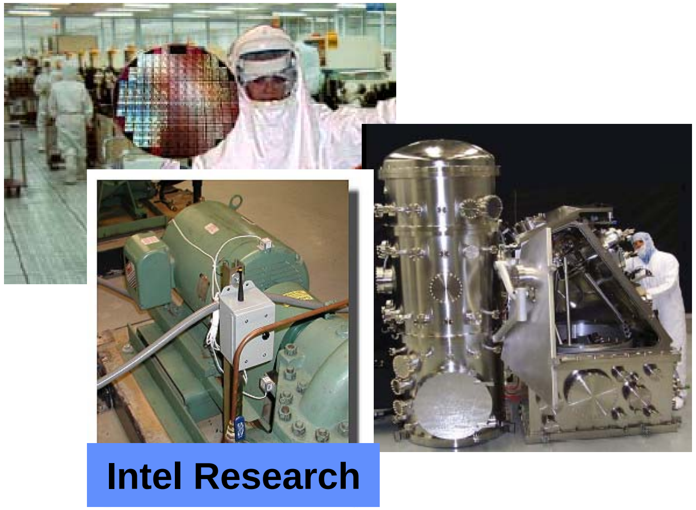
- Understanding phenomena:
  - Data collection for offline analysis
    - Environmental monitoring, habitat monitoring [Szewczyk et al., 2004]
    - Structural monitoring [Pakzad et al., 2005]

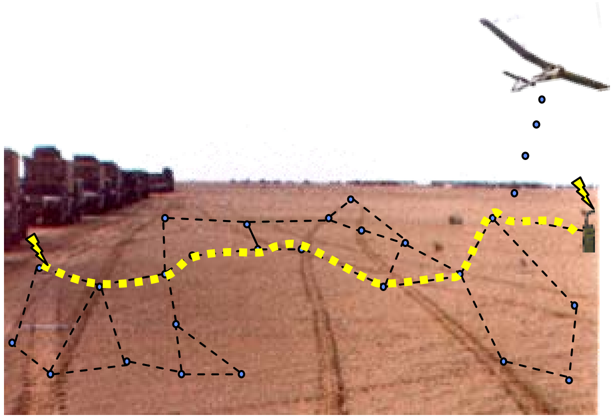




Sensor Webs Everywhere

- **Understanding phenomena:**
  - **Data collection for offline analysis**
    - » **Environmental monitoring, habitat monitoring [Szewczyk et al., 2004]**
    - » **Structural monitoring [Pakzad et al., 2005]**
- Detecting changes in the environment:
  - Thresholds, phase transitions, anomaly detection
    - » Security systems, surveillance [Brooks et al., 2004; Arora et al., 2004], health care
    - » Wildfire detection [Doolin, Sitar, 2005]
    - » Fault detection, threat detection

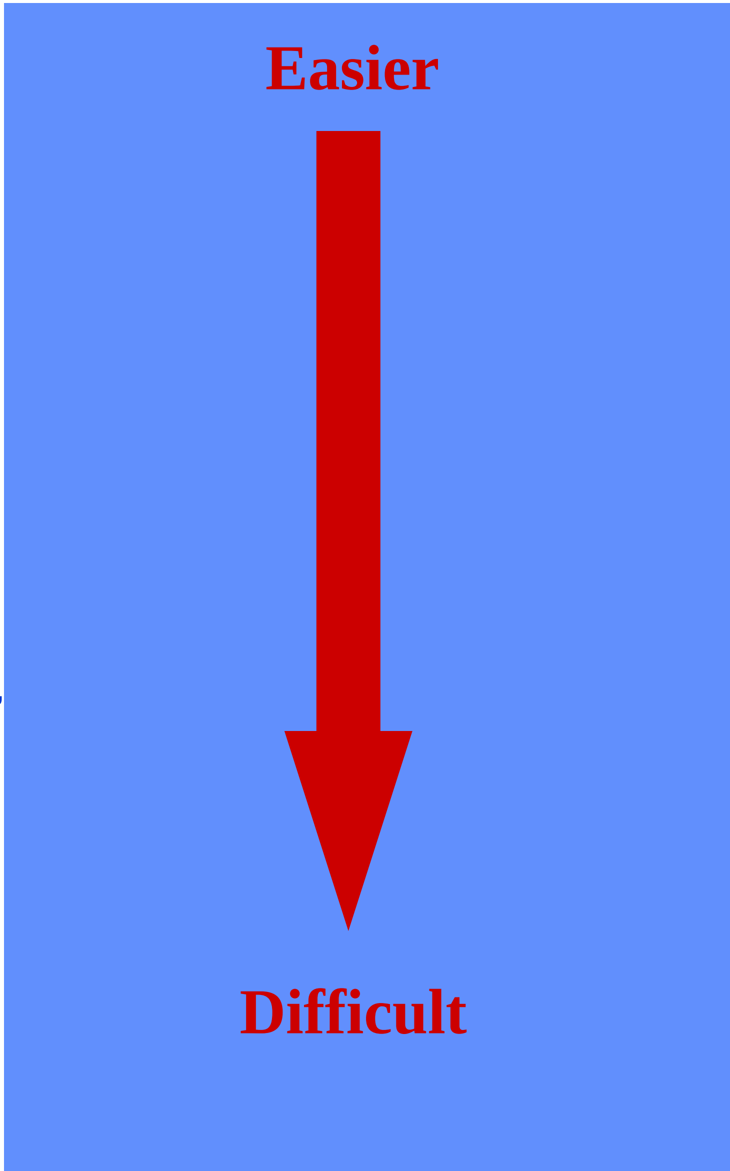




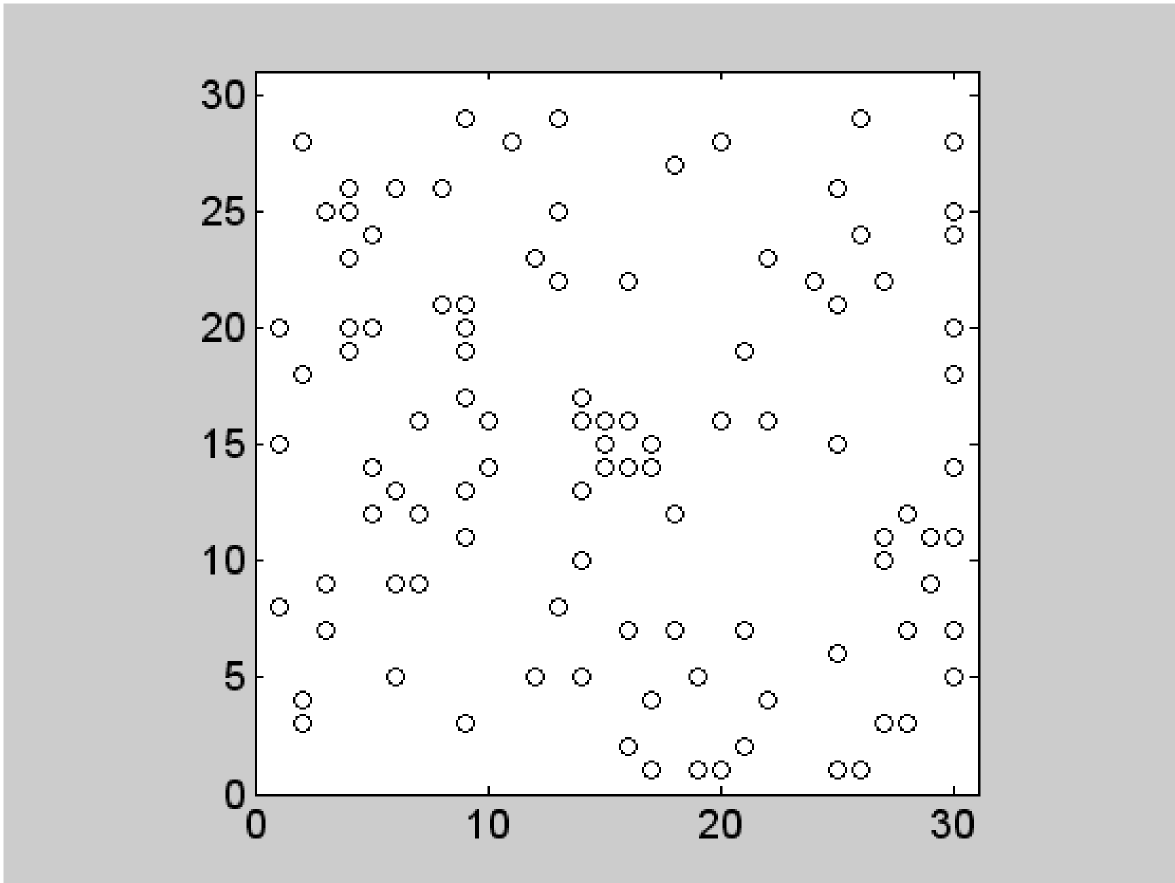
Health Care

Sensor Web Applications Taxonomy

- **Understanding phenomena:**
  - **Data collection for offline analysis**
    - » **Environmental monitoring, habitat monitoring [Szewczyk et al., 2004]**
    - » **Structural monitoring [Pakzad et al., 2005]**
- **Detecting changes in the environment:**
  - **Thresholds, phase transitions, anomaly detection**
    - » **Security systems, surveillance [Brooks et al., 2004; Arora et al., 2004]**
    - » **Wildfire detection [Doolin, Sitar, 2005]**
    - » **Fault detection, threat detection**
- Real-time estimation and control:
  - Traffic control [Nekovee, 2005], building control [Kintner-Meyer, Conant, 2005], environmental control
  - Manufacturing and plant automation [Willig et al., 2005], power grids, SCADA networks
  - Service robotics [LaMarca et al., 2002], pursuit evasion games, active surveillance, search-and-rescue, and search-and-capture, telesurgery, robocup
  - Multiple Target Tracking and Pursuit Evasion games



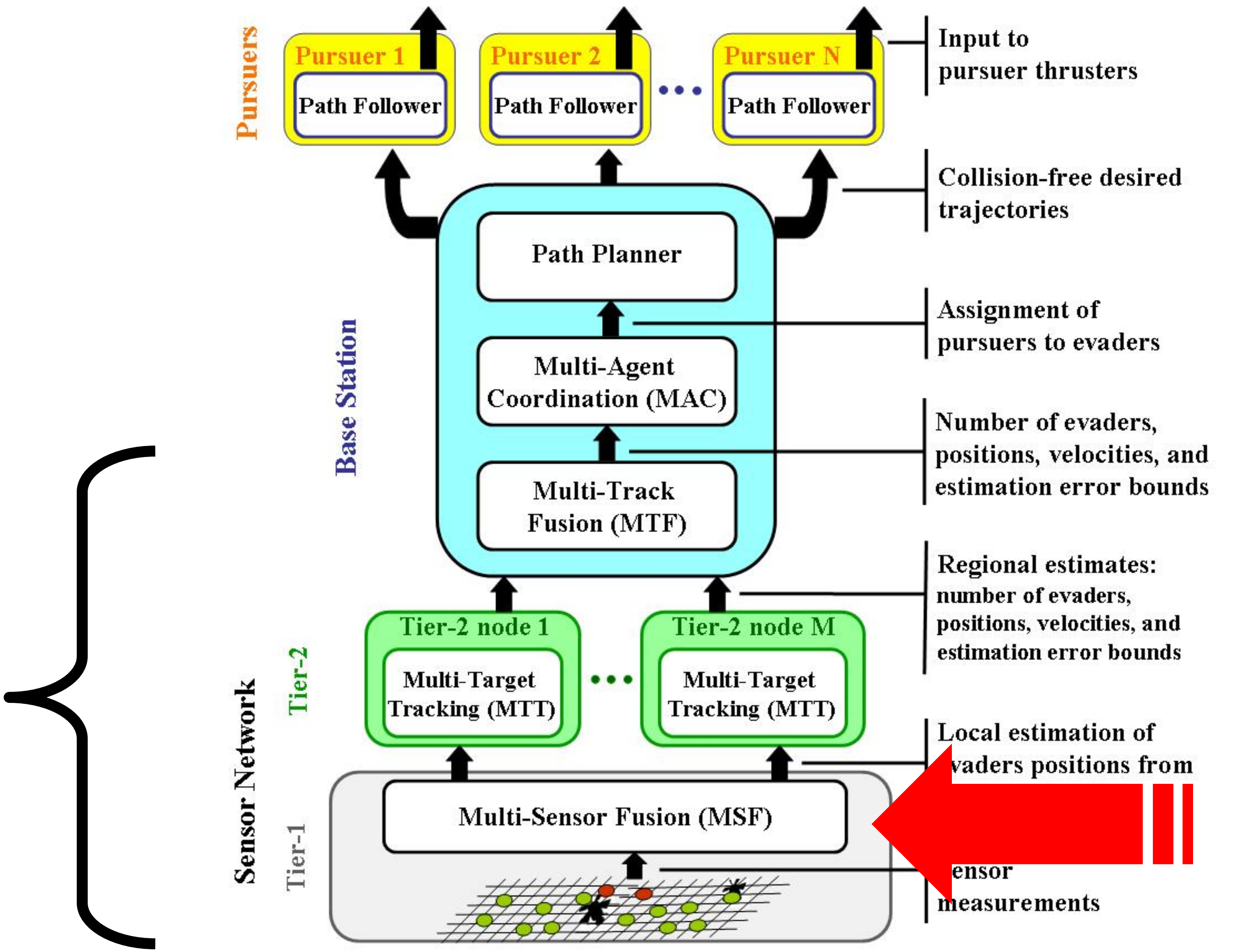
What About False Alarms?



LochNess*:
A Real-Time Sensor Network-Based Control System

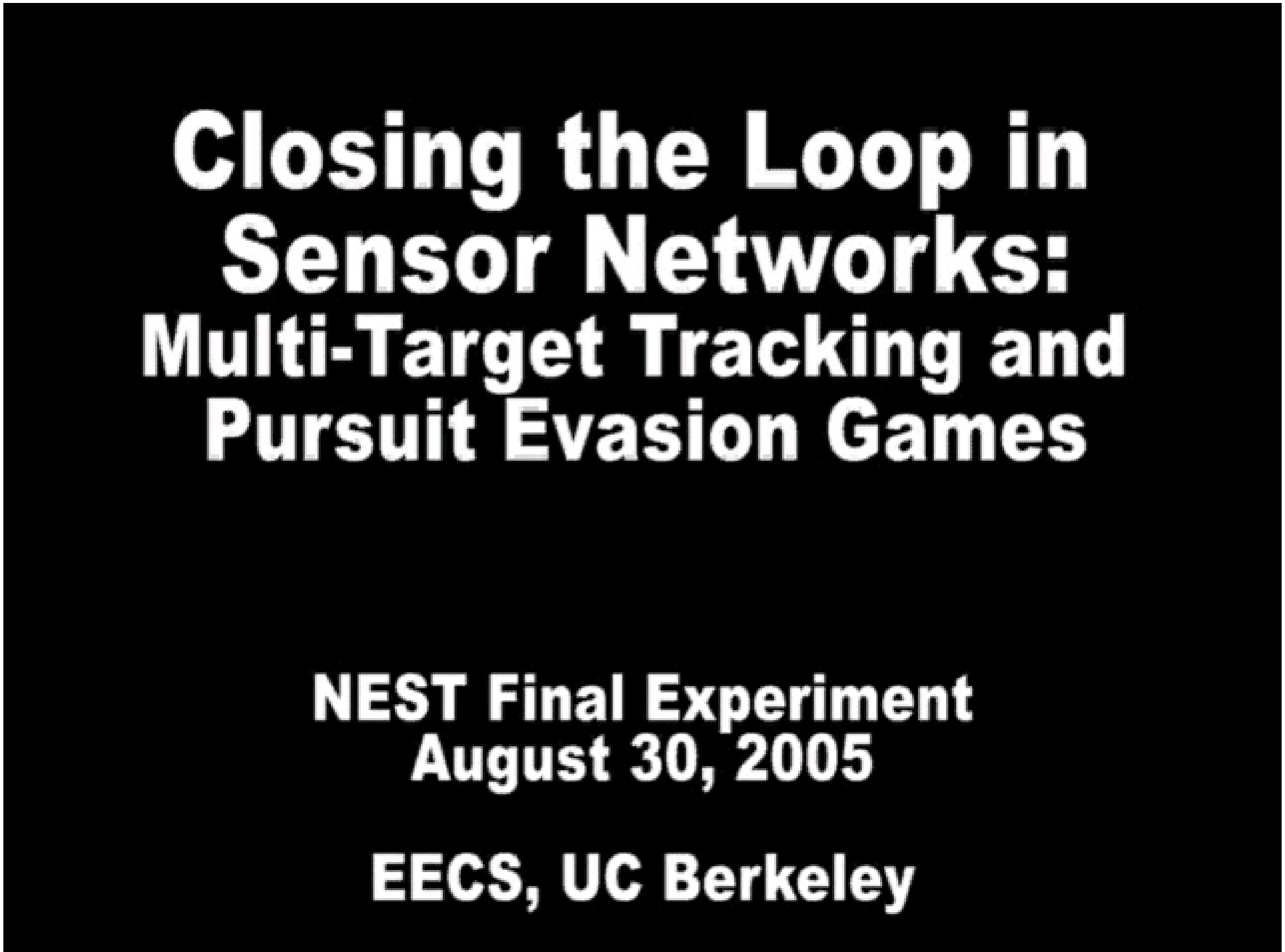
Hierarchical architecture for real-time operation

Multiple layers of data fusion for robustness and to reduce communication load

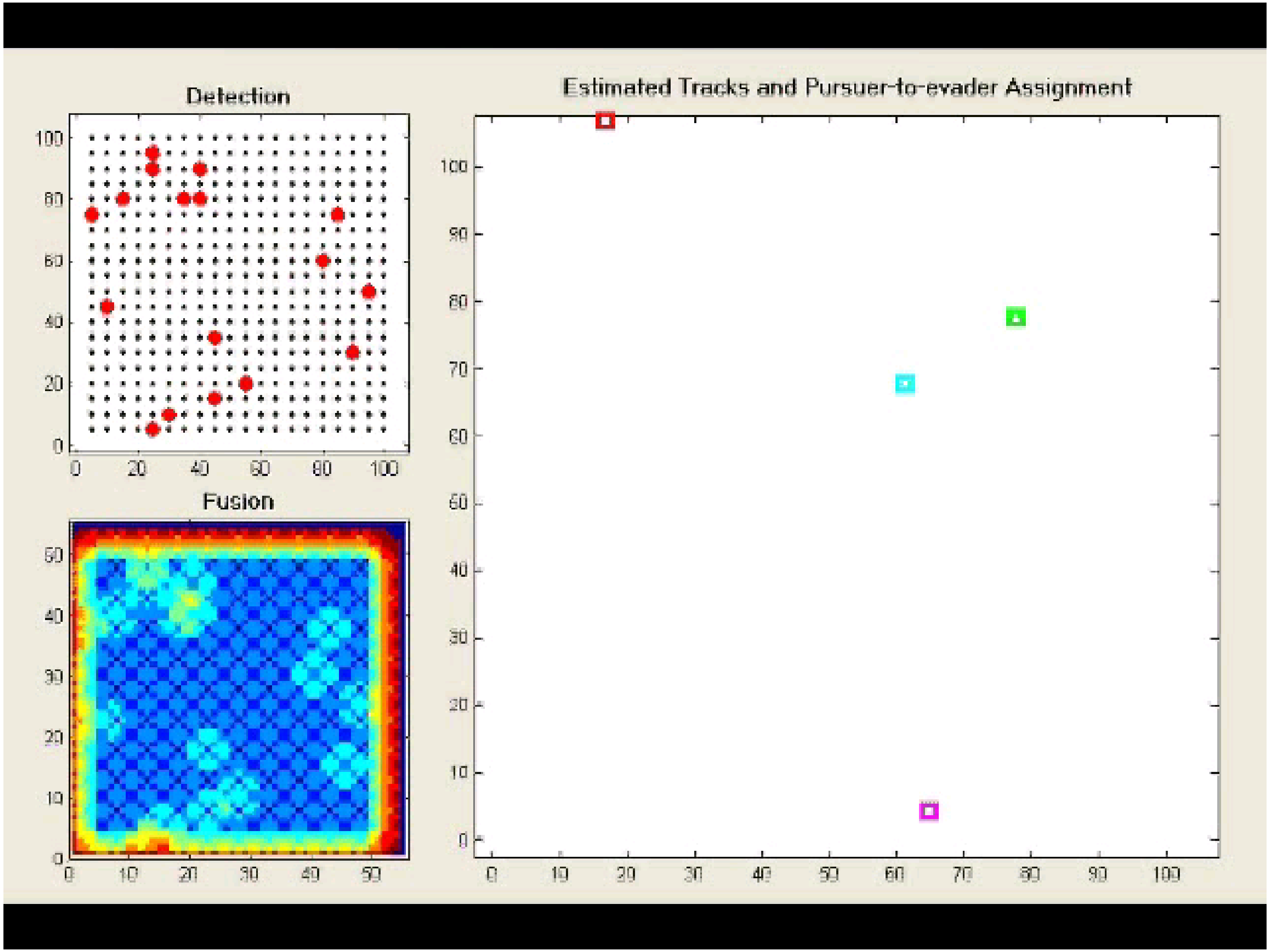


* LochNess (Large-scale "On-time" Collaborative Heterogeneous Networked Embedded SystemS).
[Oh, Schenato, Chen, Sastry, PIEEE, 2007]

NEST Demo Movie



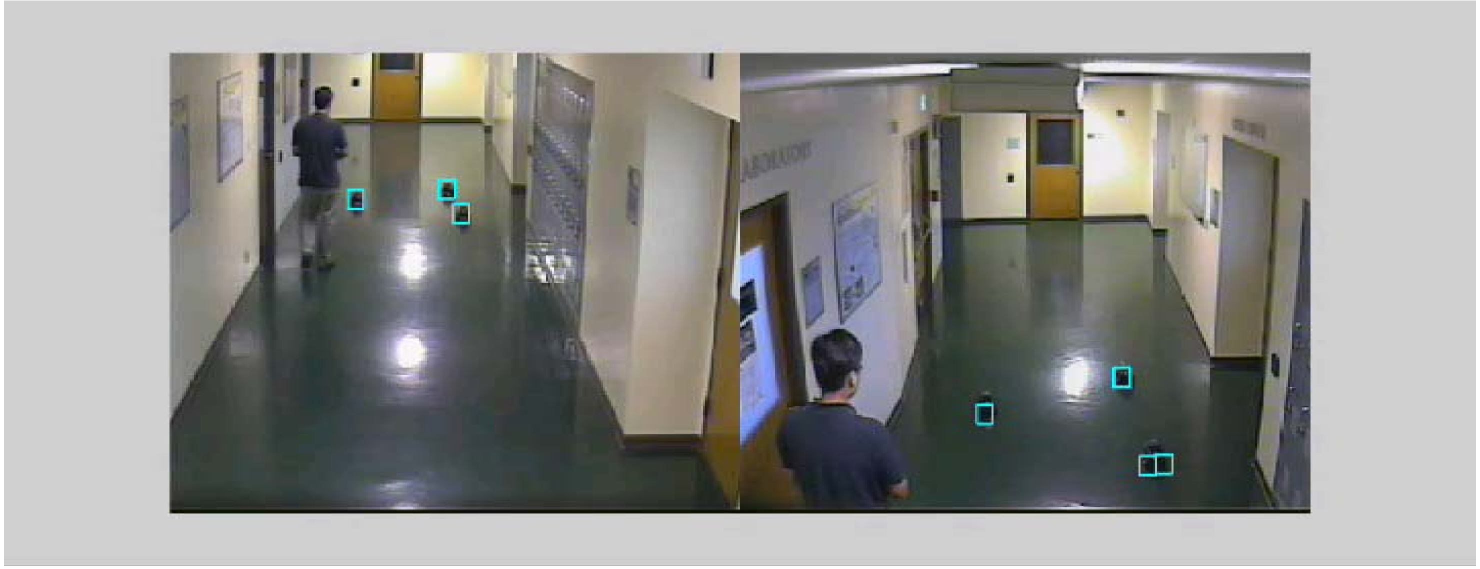
Sim+Demo Movie



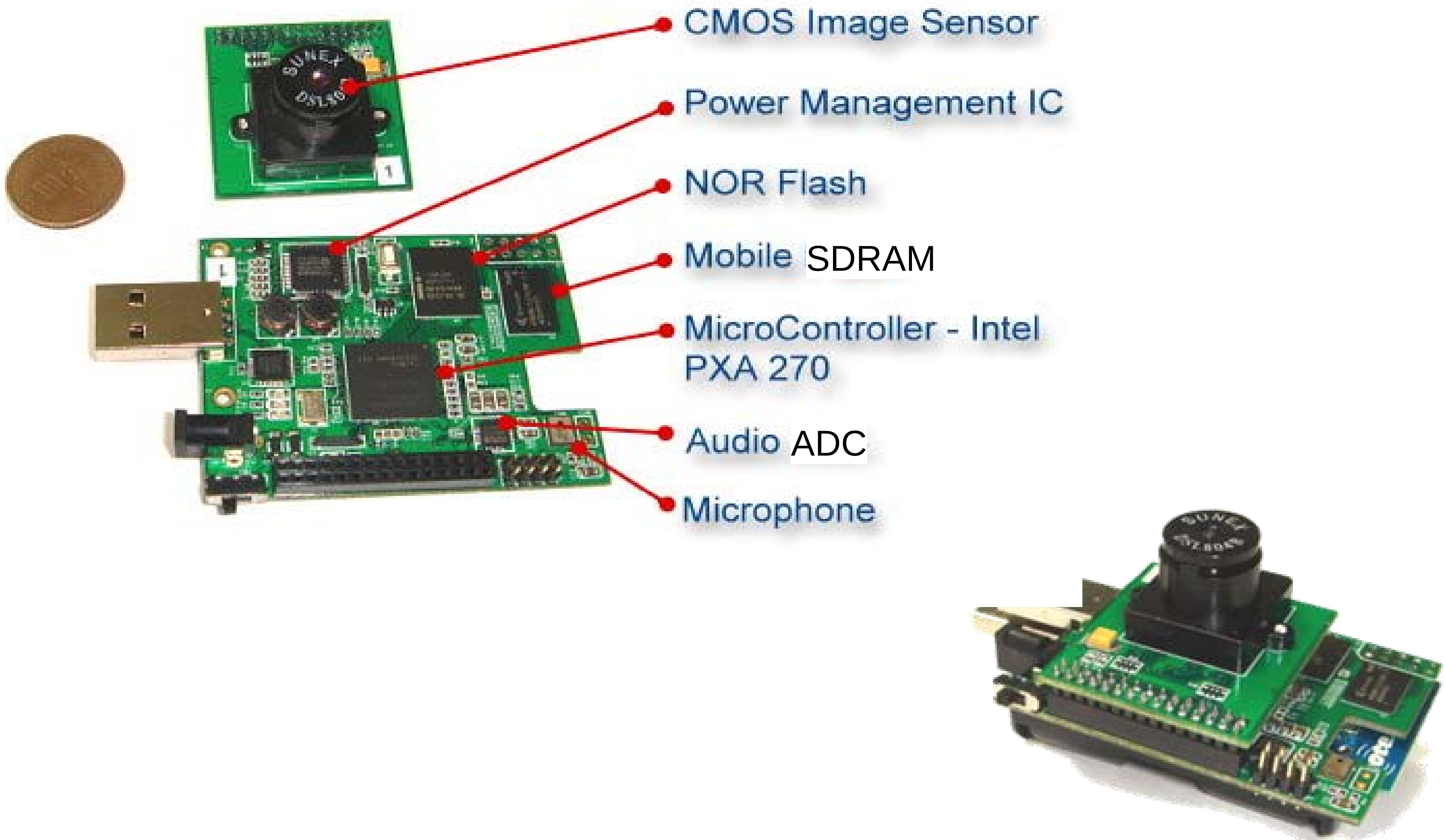
Dropping Motes from the Air

Heterogeneous Sensor Webs

Low-bandwidth, high-bandwidth, & mobile sensors



UCB/ITRI Camera Mote Daughter Board

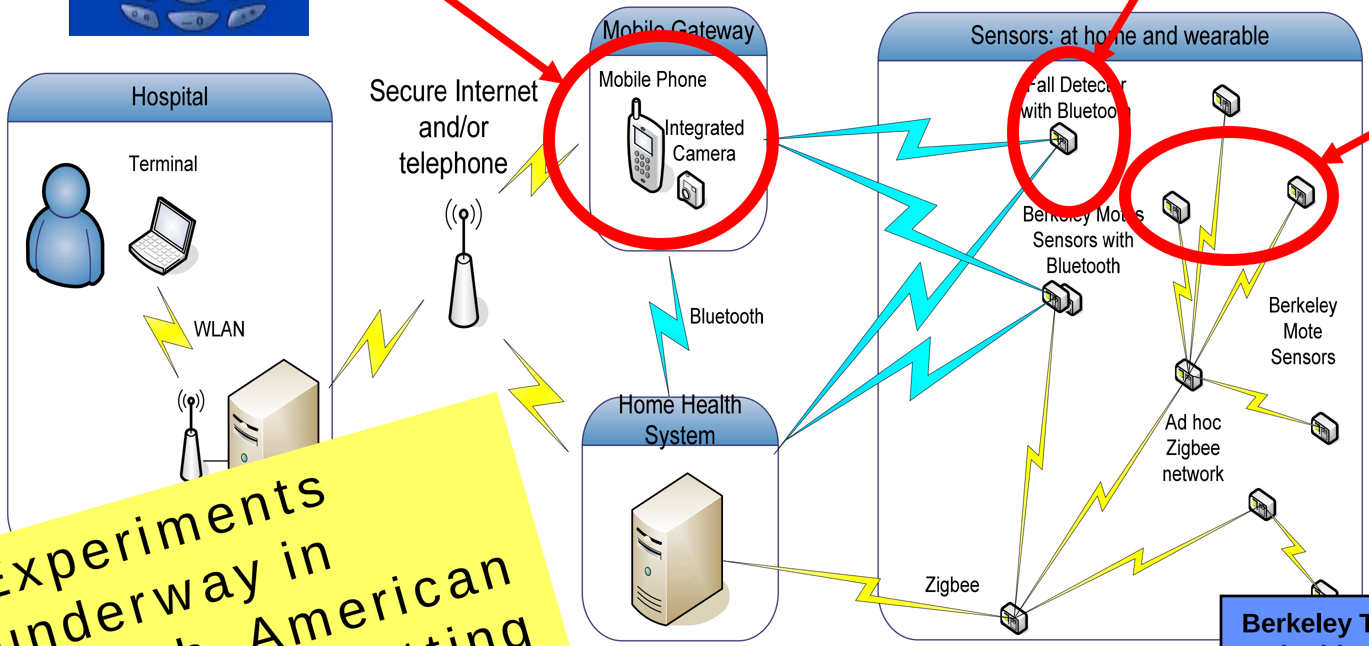


The ITALH S

Records continuous sensor data
Fall Detection algorithms
Radio communication (Bluetooth)
Triggered Reporting

Wearable Fall Detector

Fixed Sensors



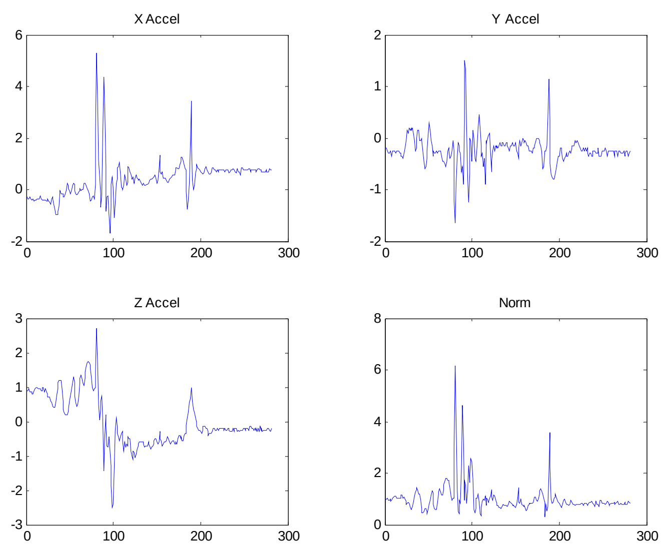
Berkeley Telos Motes with sensors embedded in living environment

Experiments underway in Finnish- American Elder Care setting in Sonoma, CA

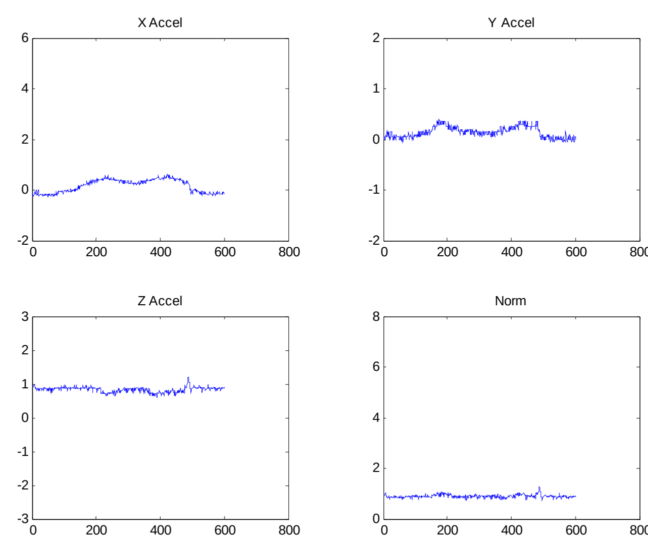
First Sensors: the IVY Project Fall Detectors

- Senior Citizens Community in Bay Area
  - Collecting “normal” activity data from elderly residents
  - Accelerometer data and video cameras for truth data
- UCB Judo Club
  - Collecting “fall” data
- Off line algorithm development: False Alarms big issue

Falling Trained Judoist

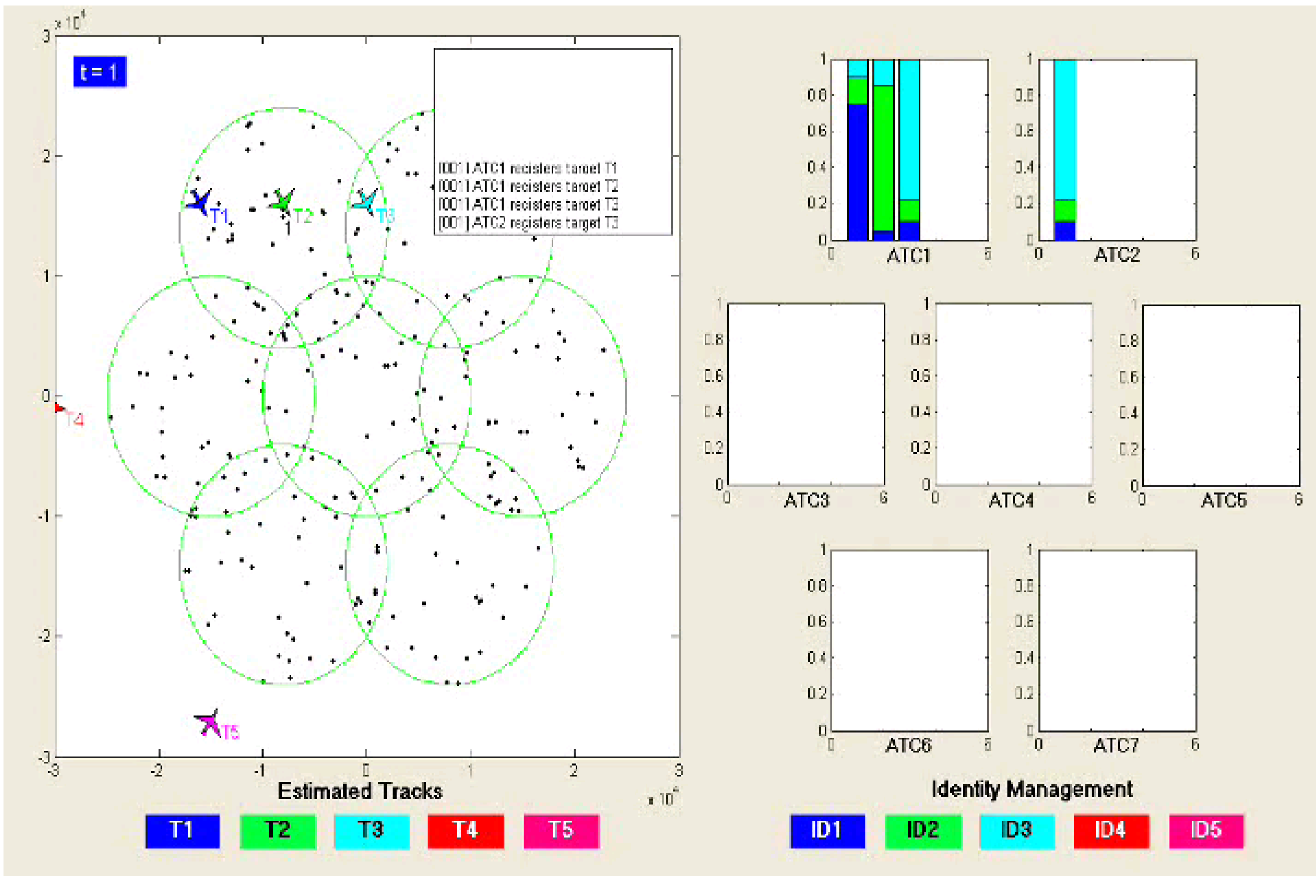


Sitting-Septugenarian



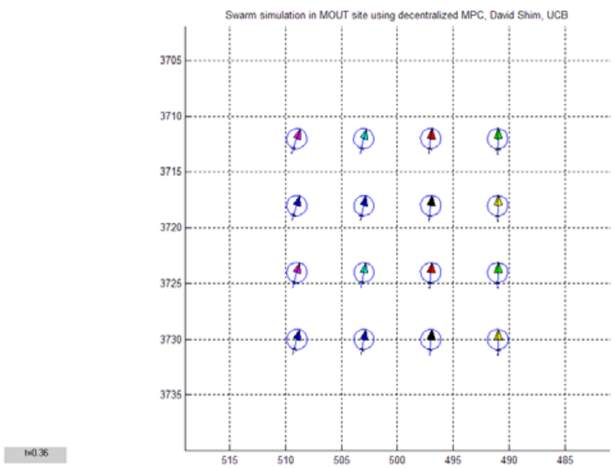
Sensor Webs in Air Traffic Control

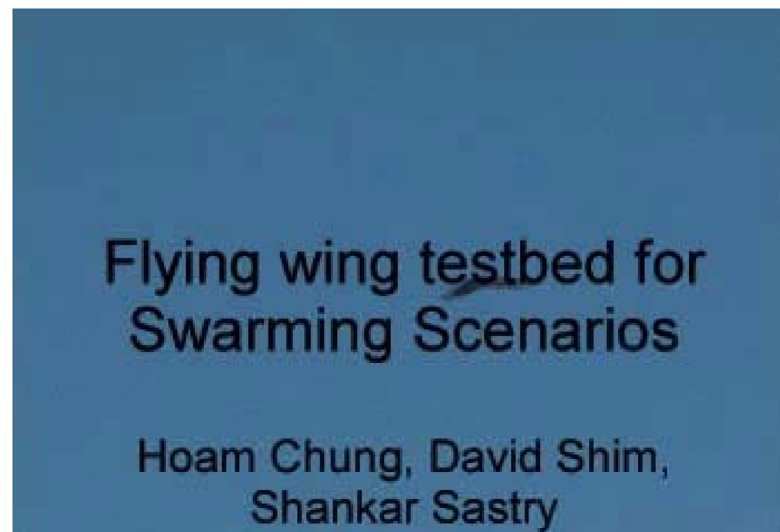
Air Traffic Control*



* [Oh, Hwang, Roy, Sastry AIAA and Oh, Schenato, Chen, and Sastry, Journal of Guidance, Control, and Dynamics (to appear), Hwang, Balakrishnan, Tomlin, IEE

Swarms of Mobile Sensor Webs





Expanding the Vision: A 1000 Radios Per Person

Jan Rabaey, David Tse and Shankar Sastry

The Emerging IT Scene

The Technology Gradient: Computation

Driven by Moore's Law

Driven by "More Than Moore" and "Beyond Moore"

The Technology Gradient: Communication

Mostly wired

Almost uniquely wireless

1,000 Radios per Person!

The Birth of "Societal IT Systems (SiS)"

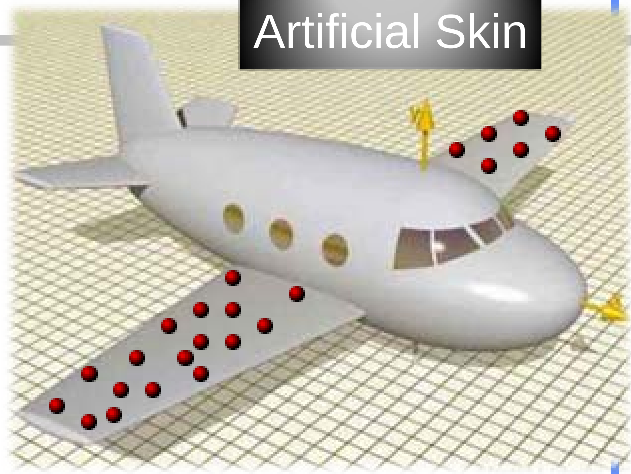
"A complex collection of sensors, controllers, compute nodes, and actuators that work together to improve our daily lives"

- **The Emerging Service Models**
  - **Intelligent data access and extraction**
  - **Immersion-based work and play**
  - **Environmental control, energy management and safety in "high-performance" homes**
  - **Automotive and avionic safety and control**
  - **Management of metropolitan traffic flows**
  - **Distributed health monitoring**
  - **Power distribution with decentralized energy generation**

Societal IT Systems –
What it means for Wireless

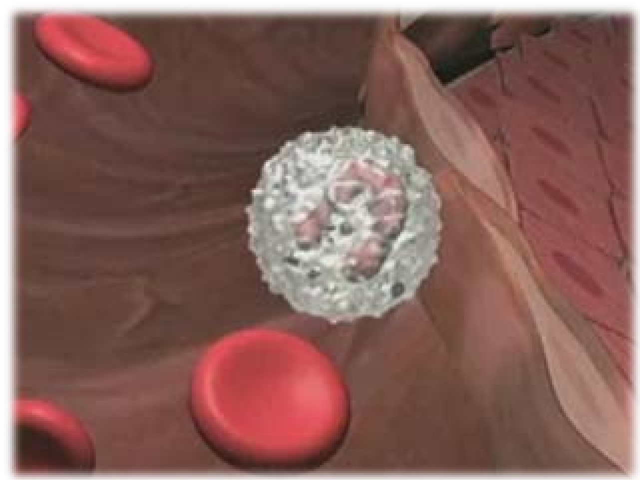
- **From the Very Small**
  - **Ubiquitous, Pervasive**
  - **Disappearing**
  - **Perceptive, Ambient**
- **To the Very Large**
  - **Always connectable – whatever happens**
  - **Absolutely reliable**
  - **Scalable, Adaptive, Flexible**

Major Progress but True Immersion Still Out of Reach


Artificial Skin


Interactive Surfaces


Smart Objects


"Microscopic" Health Monitoring

Another leap in size, cost and energy reduction

SiS Wireless – The Very Large

- **Reliable universal coverage at all times!?**
  - **7 trillion radios will quickly run out of spectrum …**
  - **Wireless is notoriously unreliable**
    - » **Fading, interference, blocking**
  - **Mobility requires dynamic reconfiguration**
  - **Heterogeneity causes incompatibilities**
    - » **Large number of standards to co-exist**
    - » **Devices vary in form-factor, size and energy source**


TOP STORY

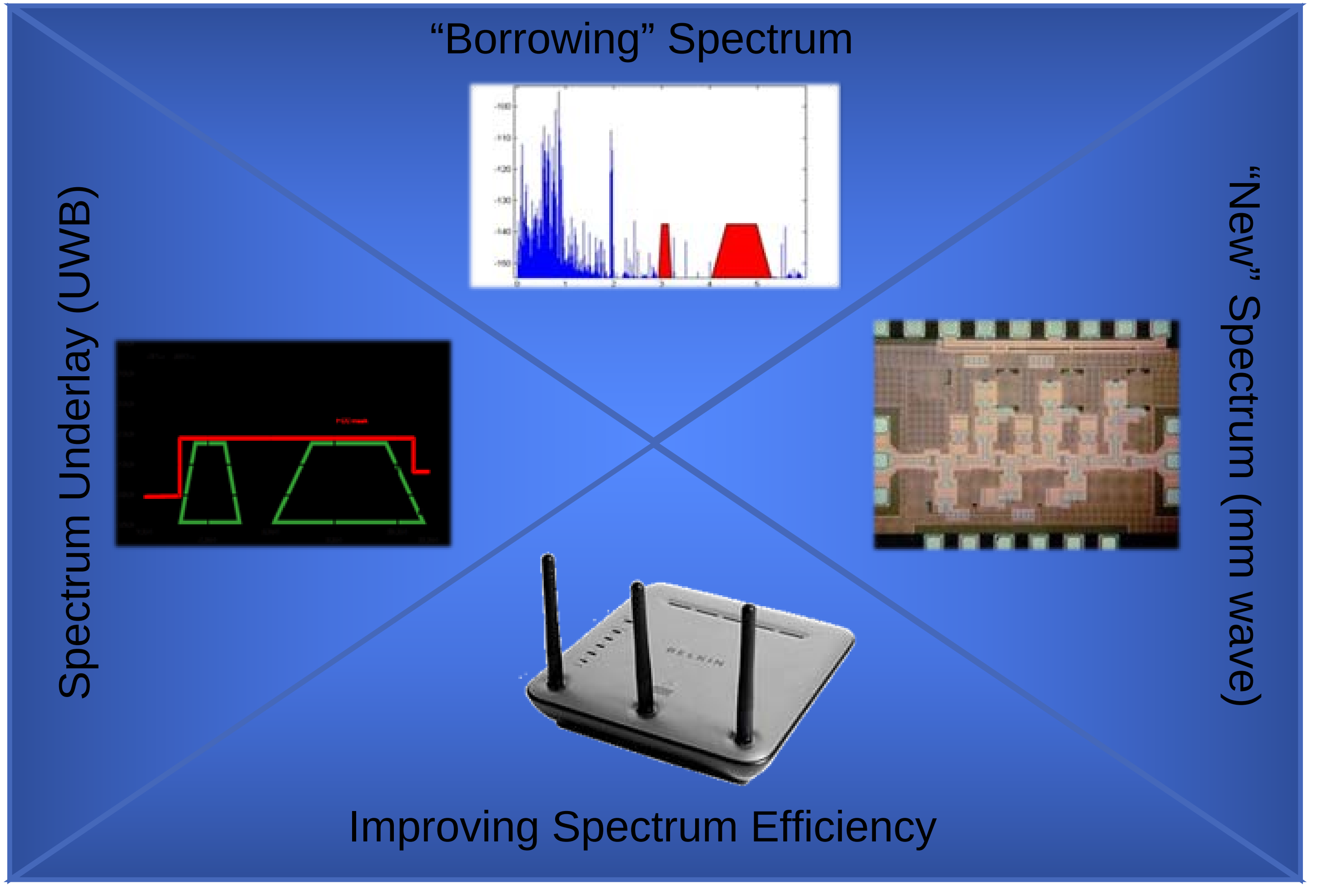
Updated Mon, 14 Jan 2008 01:03:01 PM EST

CE's wireless Babel: Connectivity strategies are all over the map

Now that consumer electronics companies are delivering a full suite of product to the digital living room, they are working out how to connect them.

EE Times, Jan. 14 2008

A World with Unlimited Wireless Bandwidth and Always-On Coverage?



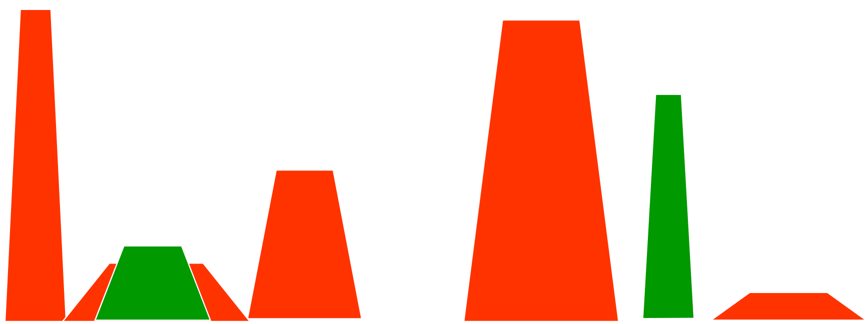
Some exciting technology developments

A World with Unlimited Wireless Bandwidth and Always-On Coverage?

- **Cognitive capabilities of terminals offer prospect of dramatic increase in attainable wireless data-rates**
  - **Spectrum becomes a dynamic commodity**
- **Collaboration among terminals and infrastructure essential to accomplish cognitive promises, while providing reliability**
  - **Enables multi-modal operation (e.g. in emergencies)**
  - **Opens door for collaboration between heterogeneous services or standards**
- **Connectivity Brokerage as the new operational (as well as business) paradigm**

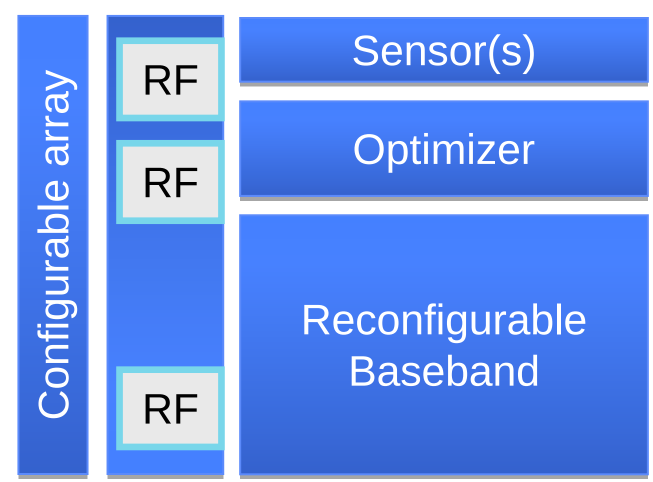
A Fundamentally Disruptive Technology

Cognitive Radio to Enable Dynamic Spectrum Allocation



First Experiment in Cognitive:
TV Bands @ 700 MHz
(IEEE 802.22)

- Sense **the spectral environment over a wide bandwidth**
- **Reliably** detect **presence/absence of primary users and/or interferers**
- Rules **of sharing the available resources (time, frequency, space)**
- Flexibility **to adjust to changing circumstances (power, freq. band)**



Cognitive terminal

The Power of Collaboration

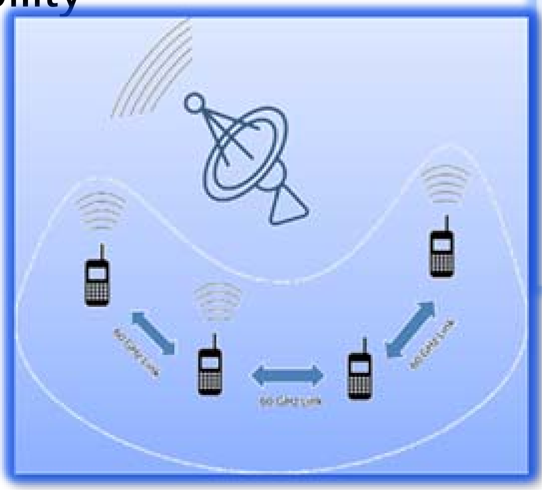
Conventional wireless mindset**:**

- **Services compete!**
  - » **Example: Bluetooth, WIFI and Zigbee**
- **Adding terminals degrades user capacity**

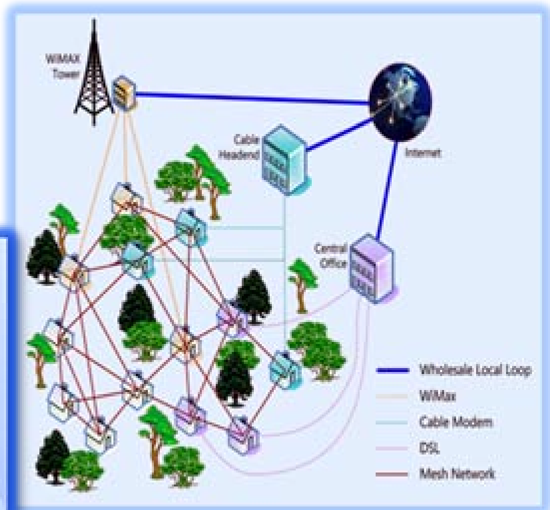
Collaboration as a means to improve spectrum utilization!

A single terminal or base-station has only limited perspective

- Working together leads to better capacity, coverage and/or reliability
- Examples: multi-hop, collaborative diversity



[Ref: Ozgur/Leveque/Tse'07]



[Ref: Gupta/Kumar'00]

Cognitive-Collaborative Networks: The Challenges

- **How to manage degrees of freedom?**
  - **Frequency/spatial utilization, collaboration, topology**
- **So that some global and user goals are met**
  - **Cost, User experience, Life time**
- **While …**
  - **Providing absolute reliability**
  - **Hiding complexity**
  - **Providing security and access control**
  - **Dealing with legacy systems**

A Societal IT System on Its Own!

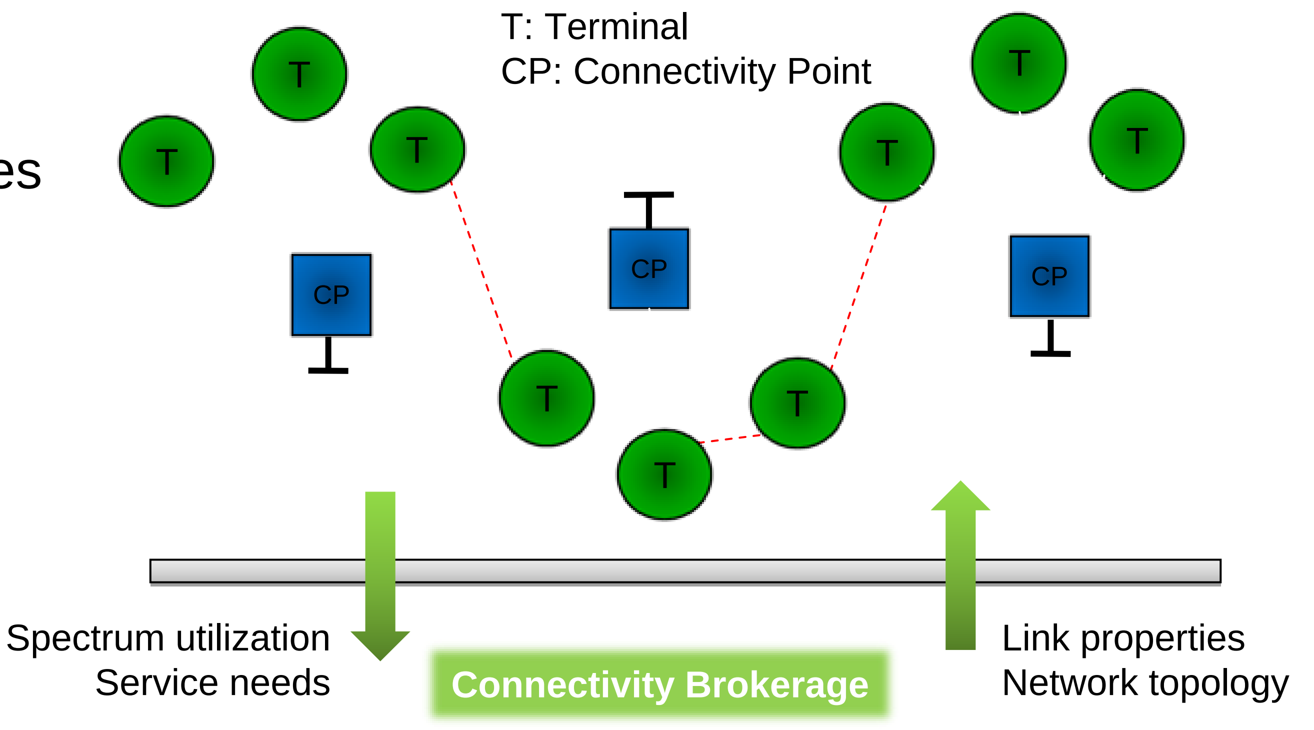
Making Cognitive/Collaborative Work

Connectivity Brokerage (*) as a Distributed OS

Functional entity that enables collection of terminals to transparently connect to backbone network or each other to perform set of services

While optimizing utilization of spectrum under policy rules, rules of engagement and security constraints.

(*) Term first coined by Adam Wolisz (TU Berlin)



A Technical as well as Economic Proposition

Closing the Loop Around Sensor Networks

Cyber Physical Computing

Next Generation SCADA/DCS Systems

- IEEE definition for a SCADA System:
  - All control, indication, and associated telemetering equipment at the master station, and all of the complementary devices at the RTU(s). (C37.1-1994)
- DCS: Digital Control Systems
  - The overall collection of control systems that measure and change the infrastructure state to facilitate delivery of the commodity (electricity, water, gas, & oil)
- Wireless Sensor Networks; next Generation SCADA

~2 Square Miles, 1400 Employees, 40 years old

Infrastructure $ 10 B, Budget $200M+/year

Primary products: Chlorine, Silica, Caustics

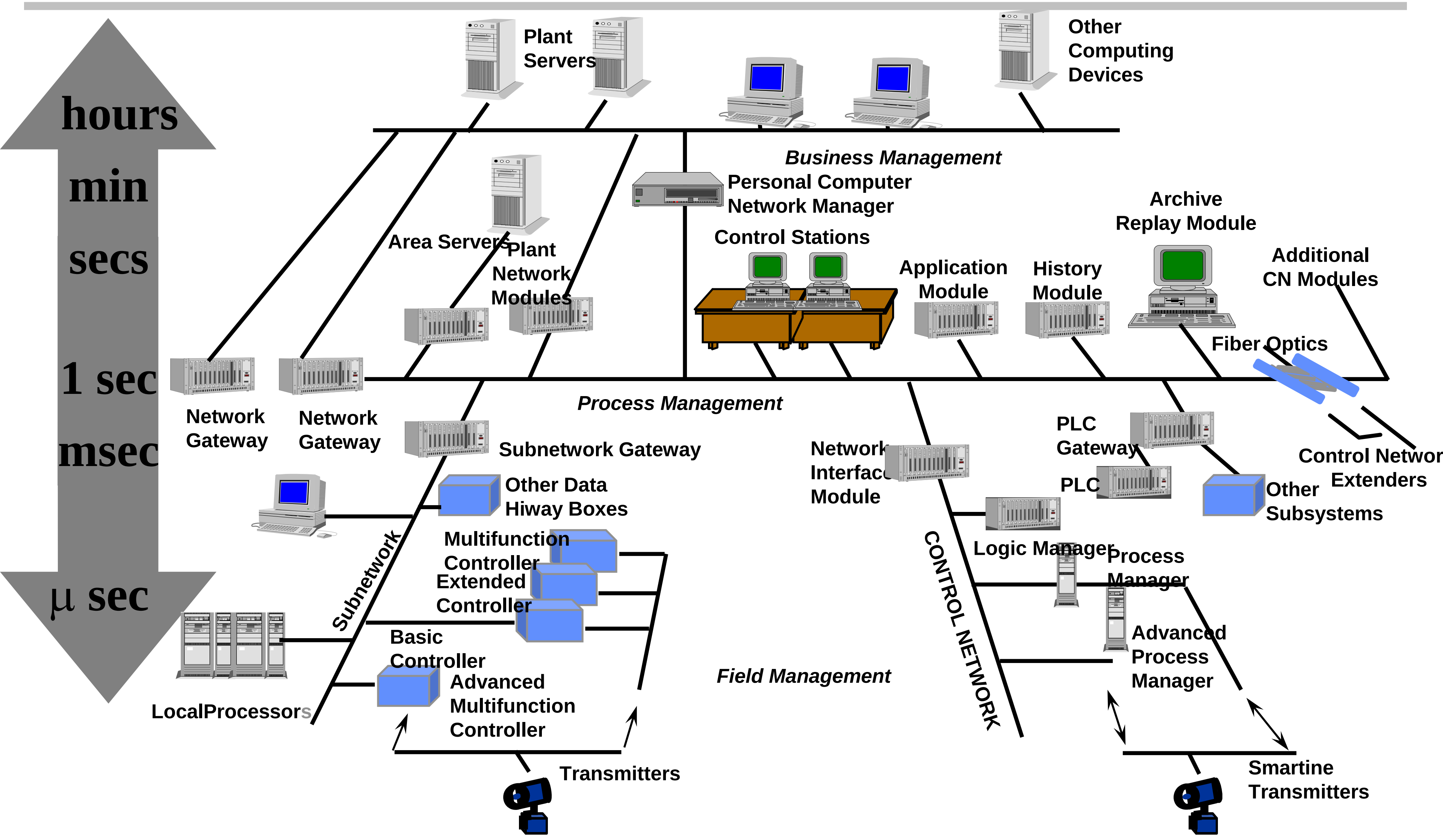
Highly profitable facility

DHS, OSHA, EPA compliance

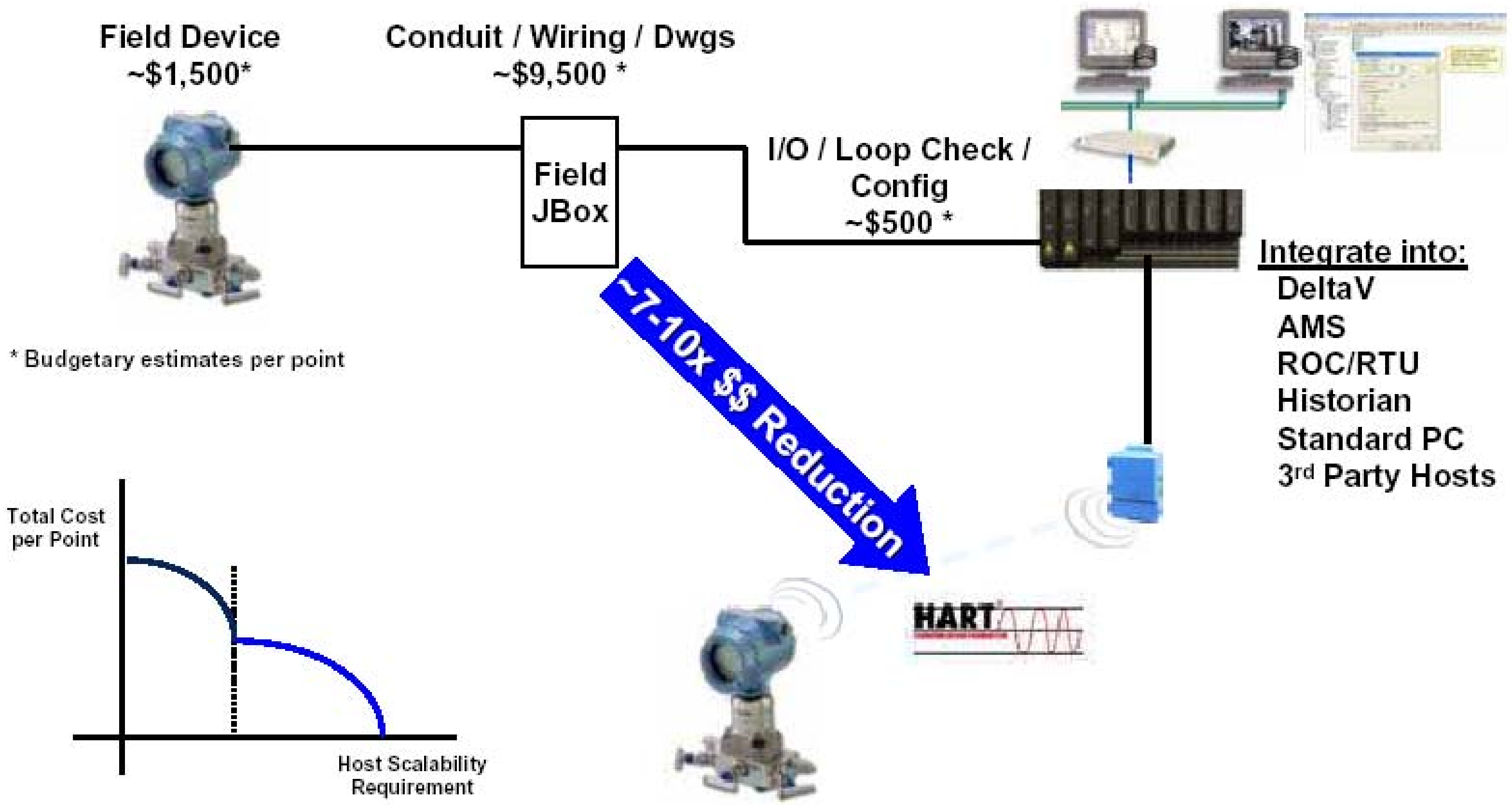
Industrial Automation

- **Motivation: Cost reduction**
  - More than 85% reduction in cost compared to wired systems (case study by Emerson)
  - SCADA (Supervisory Control And Data Acquisition)
- **Reliability is the number one issue**
  - Robust estimation: Estimation of parameters of interest from noisy measurements with high fidelity in the presence of unreliable communication
  - Real-time control: A must for mission-critical systems

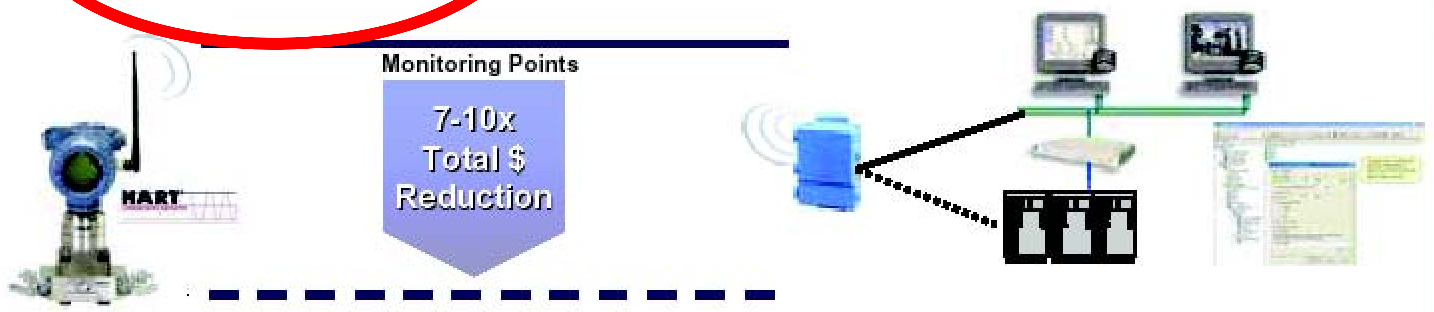
The Plant: A Complex Environment



A Shift In Total Data Acquisition Cost Will Drive A New Asset Management Paradigm



Therefore, Self Org Nets Are Proving to be More Reliable, Easier to Use, & Cost Effective



Wireless HART (Self Organizing Networks)

Measurement 100% * Communication 99.99% * Data Management 100% = 99.99%

Traditional Point-to-Point Wireless (Proprietary)

Measurement ~90% * Communication ~70% * Data Management ~99% = ~64%

The overall system can only be as strong as the weakest link

Emerson Global Users Exchange

Installation

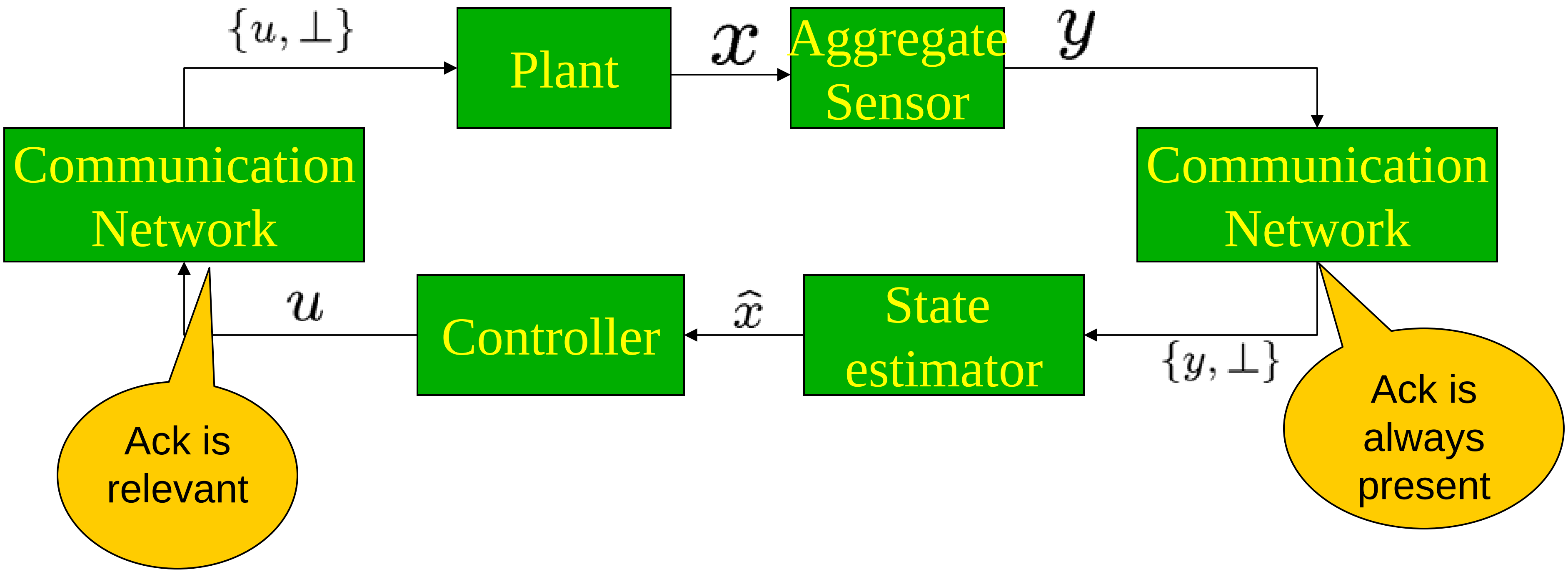
- No site Survey
- Installed Like a Wired Device
- Commissioned like a Wired Device
- Operates Like a Wired Device

Comments from Marty Geering, BP Wireless Engineer, Cherry Hill, New Jersey

Challenges

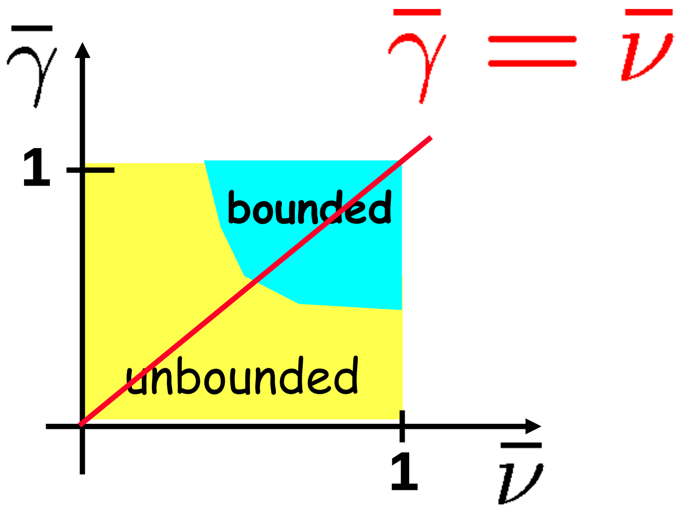
- Challenges faced with this type of device
  - Trying to find a location that would not work
  - The electricians did not like the ease of installation(sp)
    - Less work
    - Less wire
    - Less conduit….
- It just worked!

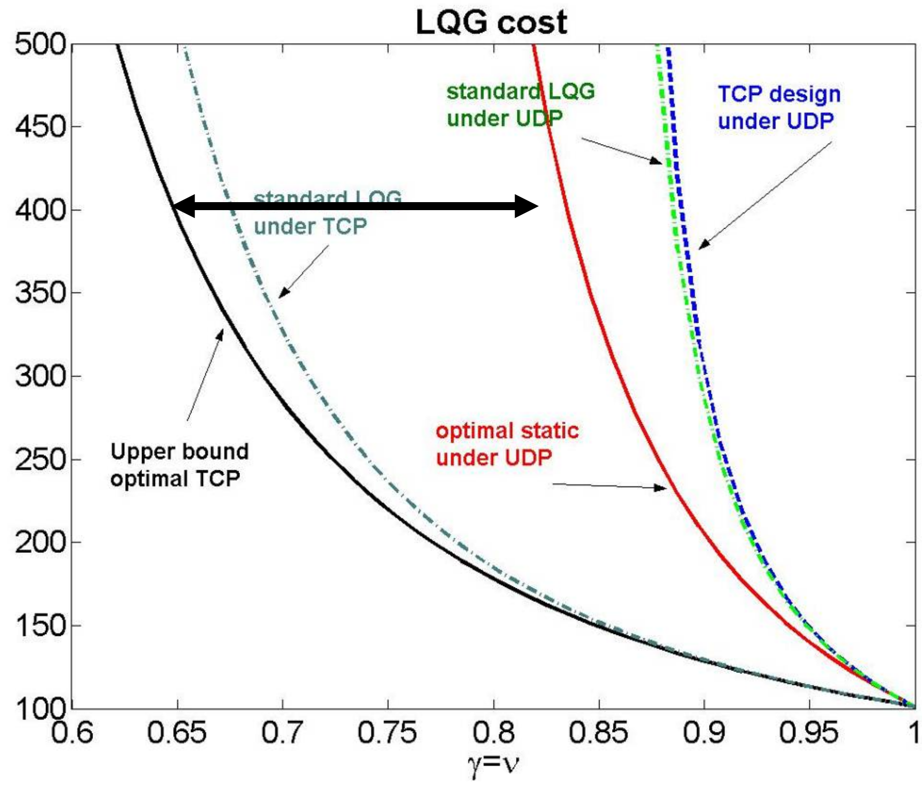
LQG control with intermittent observations and control



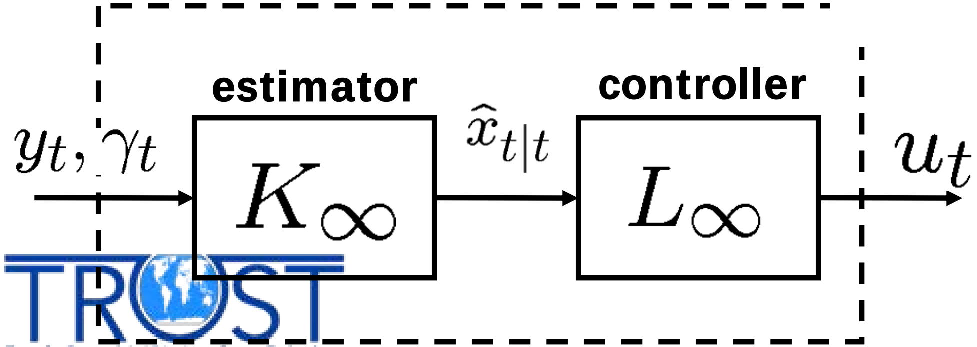
We'll group all communication protocols in two classes:
TCP-like (acknowledgement is available)
UDP-like (acknowledgement is absent)

UDP-like and TCP-like optimal static LQG design





OPTIMAL LQG CONTROL
w/ CONSTANT GAINS



Much better performance of TCP compared to UDP

Taxonomy of Security Attacks in Sensor Networks

Threat Model

- **Mote-class Attacker**
  - Controls a few ordinary sensor nodes
  - The 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
- **Outsider Attacks**
  - Passive eavesdropping: listening to the ongoing communication
  - Denial of service attacks: any type of attack that can cause a degradation in the performance of the network
  - Replay attacks: the adversary captures some of the messages, and plays them back at a later time which cause the network to operate on stale information
- **Insider Attacks: compromised node**
  - Node runs malicious code
  - The node has access to the secret keys and can participate in the authenticated communication.

Basic Security Requirements

- Confidentiality
- Authentication
- Integrity
- Freshness
- Secure Group Management
- Availability
- Graceful degradation
- Design time security

Limitations of Sensor Networks

- **Deployed in Hostile Environments**
  - **Vulnerability to physical capture**
- **Random Topology**
  - **No prior knowledge of post-deployment topology**
- **Limited Resources**
  - **Energy Restrictions**
  - **Limited Communication and Computational Power (10 KB RAM, 250 kbps data rate, for example)**
  - **Storage Restrictions**

TRUST
Team for Research in Ubiquitous Secure Technology

Attack and Countermeasures

- Secure communication
  - SPINS: Security Protocols for Sensor Networks (Perrig et. al)
  - TinySec: Link Layer encryption for tiny devices (Karlof et. al)
- Robust aggregation:
  - Given the redundancy of the data gathered by the sensor nodes, in-network processing is an essential task in sensor networks
  - Data aggregation is extremely prone to insider attacks who inject faulty data into the network
  - SIA: Secure Information Aggregation for Sensor Networks (Przydatek et. al)
  - Resilient Aggregation in Sensor Networks (Wagner)
- Sybil Attack:
  - In this attack a node pretends to have multiple identities, or the adversary creates node identities that do not exist in the network
  - Countermeasures for Sybil attack (Perrig et. al)

Other Attacks and Countermeasures

- **Secure location verification:**
  - The goal is to validate the claims of nodes
  - Verification of Location Claims (N. Sastry, et. al)
- **Robust localization:**
  - localization is used to find the position of the nodes
  - Statistical Methods for Robust Localization (Z. Li, et. al)
  - SeRLoc (Lazos, et. al)
- **Key distribution protocols:**
  - Used for distributing the cryptographic keys in the network after deployment
  - Random Key Distribution Protocol (Perrig et. al, Eschenauer et. al)

Vulnerabilities of SCADA systems

Experimental cyber-attack caused generator to self-destruct.

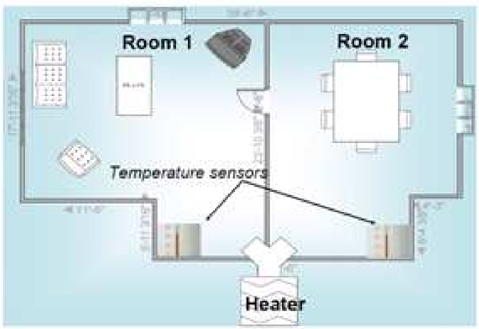
Polish teen hacks city's tram system with homemade transmitter to derail four trams

Sewage control system exploited by insider to cause sewage to flood the surroundings.

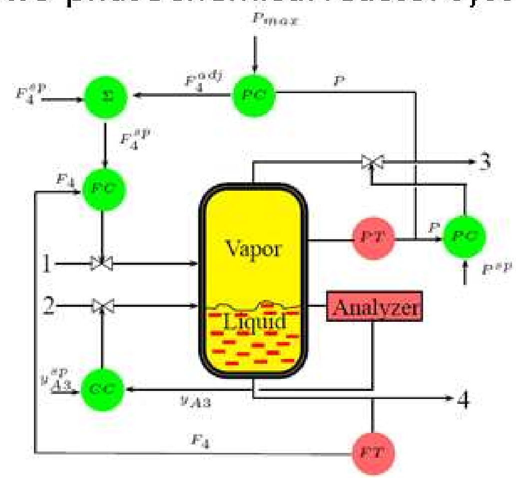
LA' traffic engineers hack computer system that controls traffic lights.

Sample Systems for study

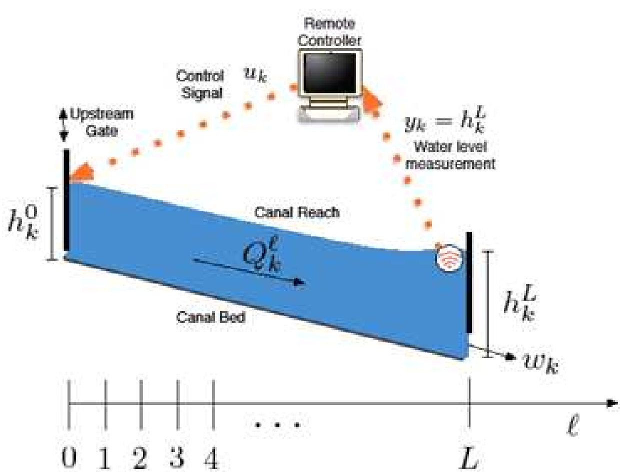
Room temperature control system



Two-phase chemical reactor system



Water canal control system



Traffic estimation system based on GPS phones

Small Technology, Broad Agenda, Unique Confluence

- **Societal Scale Systems**
  - security, privacy, usability, information sharing
- **Applications**
  - long lived, self-maintaining, dense instrumentation of previously unobservable phenomena
  - interacting with a computational environment: closing the loop
- **Programming the Ensemble**
  - describe global behavior
  - synthesis local rules that have correct, predictable global behavior
- **Distributed services**
  - localization, time synchronization, resilient aggregation
- **Networking**
  - self-organizing multihop, resilient, energy efficient routing
  - despite limited storage and tremendous noise
- **Operating system**
  - extensive resource-constrained concurrency, modularity
  - framework for defining boundaries
- **Architecture**
  - rich interfaces and simple primitives allowing cross-layer optimization
  - low-power processor, ADC, radio, communication, encryption

Where to go for more?

- http://webs.cs.berkeley.edu
- http://www.tinyos.net
- http://www.citris-uc.org
- http://chess.eecs.berkeley.edu
- http://trust.eecs.berkeley.edu
- http://robotics.eecs.berkeley.edu/~sastry
- http://trust.eecs.berkeley.edu/hsn/
- http://coe.berkeley.edu

Thanks! Questions ?