Wireless Network Embedded Systems: Sensor Nets and Beyond

Edited and Presented by

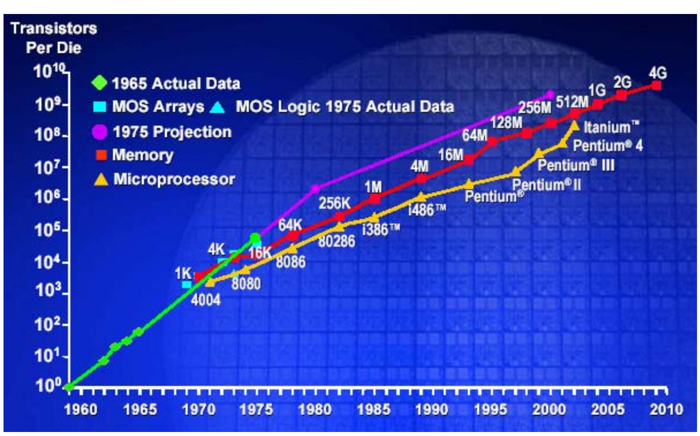
Shankar Sastry

Dept of EECS,

UC Berkeley

Chess Review
May 11, 2005
Berkeley, CA

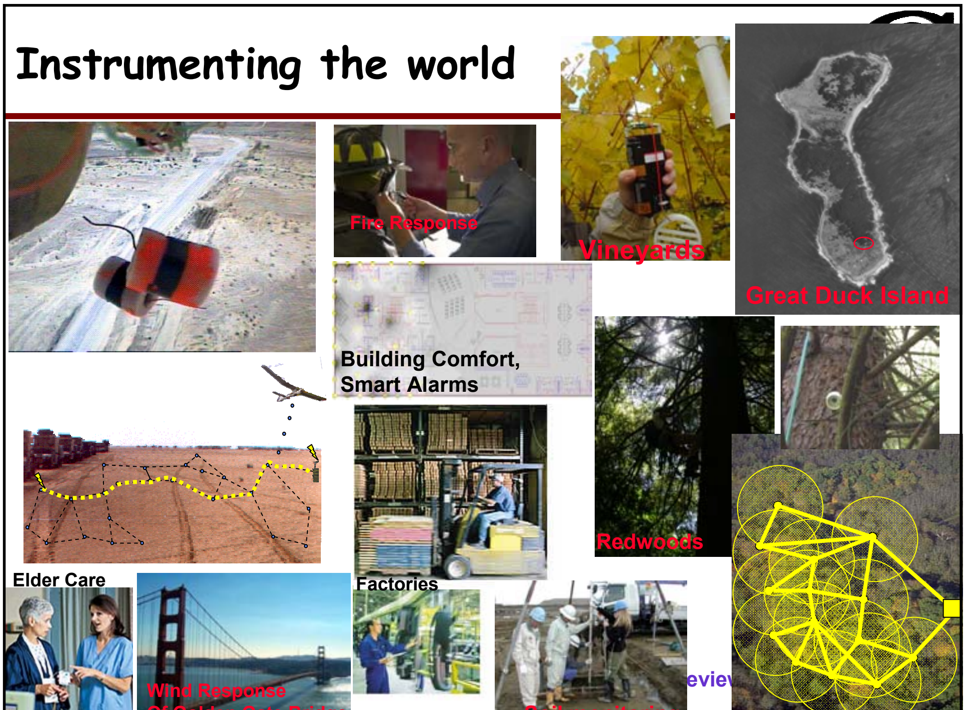
Moore's Law – 2x stuff per 1-2 yr



Bell's Law – new computer class per 10 years

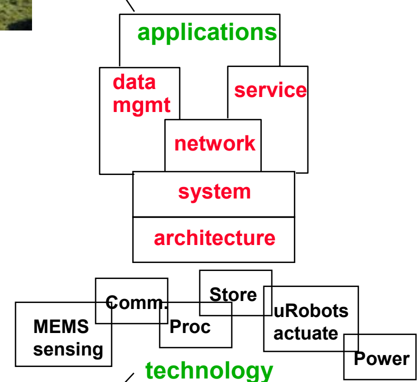
- Enabled by technological opportunities
- Smaller, more numerous and more intimately connected
- Ushers in a new kind of application
- Ultimately used in many ways not previously imagined

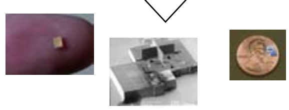
Instrumenting the world



The Sensor Network Challenge

Monitoring & Managing Spaces and Things

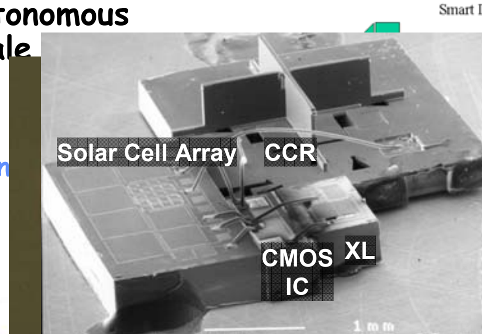


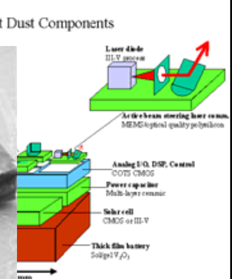


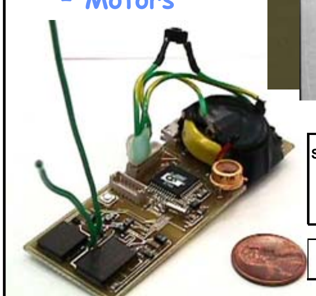
Miniature, low-power connections to the physical world

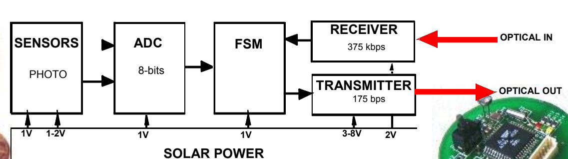
Miniaturization - Pister (SmartDust)

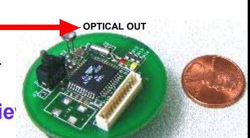
- The Goal: Autonomous millimeter-scale
  - Sensing
  - Computation
  - Communication
  - Power
  - Motors







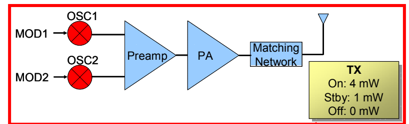


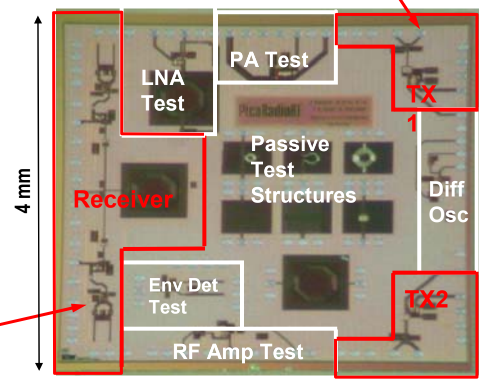


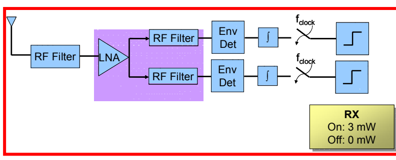
Low Power RF – Rabaey (PicoRadio)

- CMOS
  - Cheap, Integrated
- mW -> sub mW
- Simple
- Advantage in Numbers

BWRC







System/Networking/Prog. – Culler (TinyOS)

Services

Networking

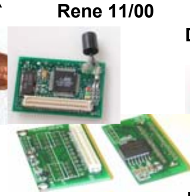
TinyOS www.tinyos.net

WeC 99 "Smart Rock"

Rene 11/00

Dot 9/01

Mica 1/02



Small microcontroller

- 8 kb code,
- 512 B data

Simple, low-power radio

- 10 kb

EEPROM (32 KB)

Simple sensors

Designed for experimentation

-sensor boards

-power boards

DARPA SENSIT, Expeditions

- Intel

Crossbow

Demonstrate scale

NEST open exp. platform

128 KB code, 4 KB data

50 KB radio

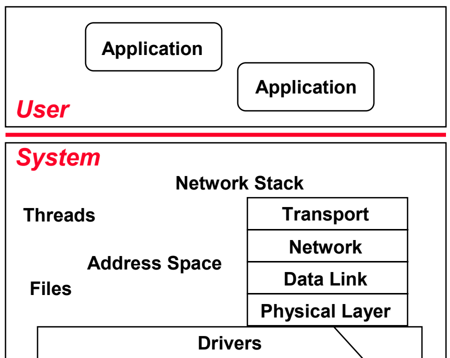
512 KB Flash

comm accelerators

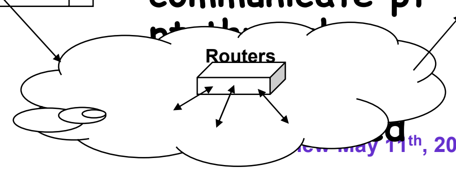
- DARPA NEST

Review Ma

Traditional Systems



- Well established layers of abstractions
- Strict boundaries
- Ample resources
- Independent Applications at endpoints communicate pt-



by comparison ...

- Highly Constrained resources
  - processing, storage, bandwidth, power
- Applications spread over many small nodes
  - self-organizing Collectives
  - highly integrated with changing environment and network
  - communication is fundamental
- Concurrency intensive in bursts
  - streams of sensor data and network traffic
- Robust
  - inaccessible, critical operation
- Unclear where the boundaries belong
  - even HW/SW will move

=> Provide a framework for:

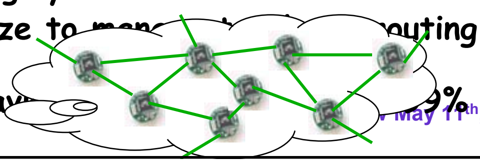
- Resource-constrained concurrency
- Defining boundaries
- Appl'n-specific processing and power management

allow abstractions to emerge

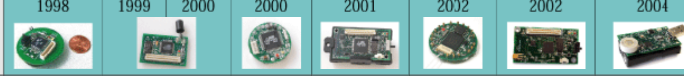
Vast Networks of Tiny Devices

- Past 25 years of internet technology built up around powerful dedicated devices that are carefully configured and very stable
  - local high-power wireless subnets at the
  - 1-1 communication between named compu
- Here, ...

- every little node is potentially a router
- work together in application specific ways
- collections of data defined by attributes
- connectivity is highly variable
- must self-organize to mana … uting, etc
- and for power sa … 9% of the time



Mote Evolution



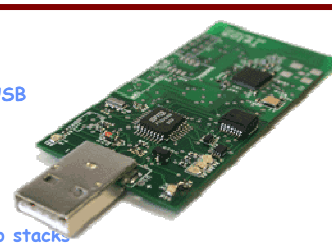
Mote Type / Year	*WeC* 1998	*René* 1999	*René 2* 2000	*Dot* 2000	*Mica* 2001	*Mica2Dot* 2002	*Mica 2* 2002	*Telos* 2004
Microcontroller								
Type	AT90LS8535		ATmega163		ATmega128			TI MSP430
Program memory (KB)	8		16		128			48
RAM (KB)	0.5		1		4			10
Active Power (mW)	15		15		15		60	0.5
Sleep Power (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 Key Areas of Progress

- OEP3 Hardware
  - Telos 802.25.4 mote (& MicaZ)
  - Mica2 testbed
- TinyOS Advances
  - Cross-platform 802.15.4 support
  - EXScal XSM support
  - Structured Release
  - BMAC
  - Large Scale Simulation
- Embedded Networking
  - Reliable, low-power data collection
  - Dissemination: trickle and drip
  - Reliable Bulk Communication
  - Scheduled Communication
- Network Programming
  - Deluge (really works at Scale)
  - Towards a tight lower bound
  - Incremental Updates
- MacroProgramming
  - Mate II application specific VM
- Security
  - 802.15.4
- Localization
  - Robust methodology - ultrasound
  - Making RSSI actually work
- Long Lived Applications
  - Analysis of GDI
  - Calibration in the redwoods
- Capstone Demo
  - Management infrastructure
  - Telos/XSM integration
  - Complete Simulation
  - Multiobject Tracking

OEP3 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
- 97% Yield on first 200
  - Remaining reparable

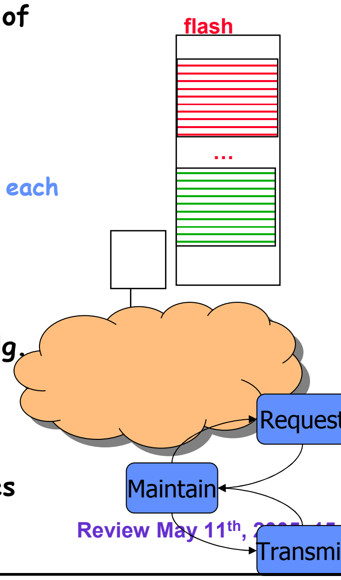


UCB Telos

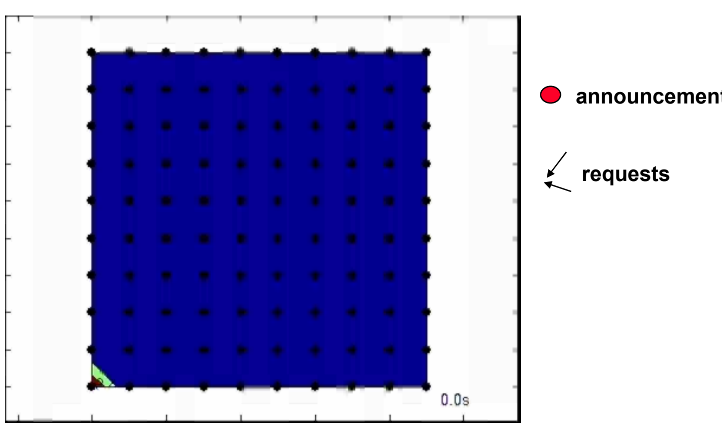
Xbow MicaZ

Deluge Network Programming

- Reliable Pipelined Epidemic Distribution of series of pages
  - Constrained storage hierarchy
  - Robust to lossy or asymmetric links
  - Very low maintenance bandwidth
- Page Advertise, Request/Fix, Xfer
  - Density-aware suppression and snoop on each
- Packet CRC + Page CRC
- 159 Byte memory footprint
- Packed image (no 64k xnp limit)
- Multiple Program images
- Extensive simulation of dissemination Alg. and many variants
- Tested extensively on 77 nodes
- Simulated on >1,000 nodes in EXSCAL configuration with multiple sources
- 4 mins for 1-hop 33k image to 33 nodes
- Command line host tools

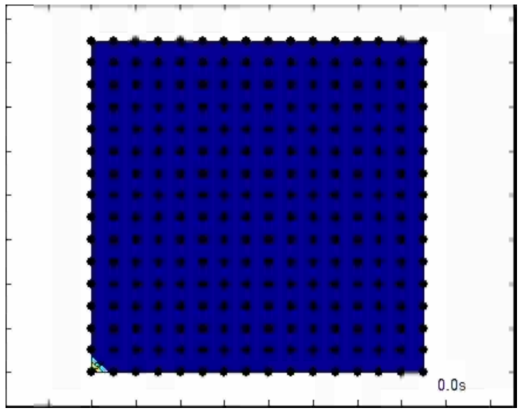


Simulated Dissemination (10x10)



- Smooth pipelined wavefront of multiple pages

Simulation at Larger Scale (16x16)

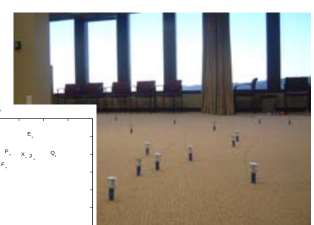


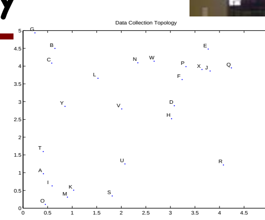
Wavefront propagates more rapidly along the edges due to lower density

- long linear structures are fast

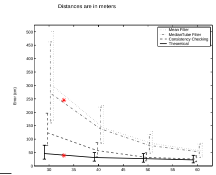
Behavior exacerbated by conservative interference model in TOSsim

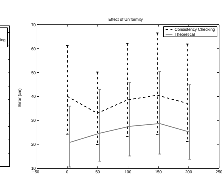
Localization Methodology

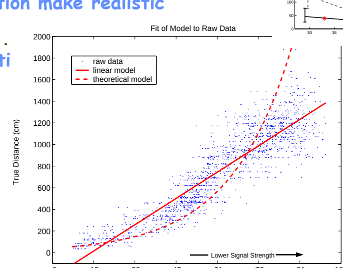


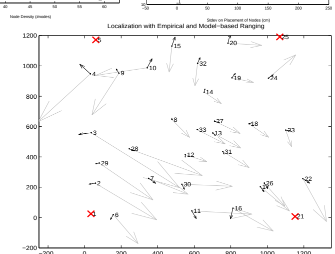


1. Environmental characterization
   - Measure accuracy and loss rate of many pairs and range of distances (pseudo-random pattern)
   - 45 environments empirically characterized
   - 660 empirical measurements taken within .3m of every distance between 0-30 m
2. System design
   - Design filters, schedule, model, localization alg. against observed error and loss distribution
   - Select simplest that works
3. Pre-deployment analysis
   - Determine a adequate system to deploy
   - Trace-based simulation make realistic predictions
     - Use data from 1.
   - Model-based simulati predictions

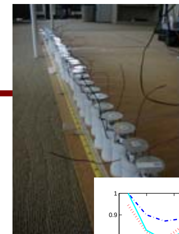




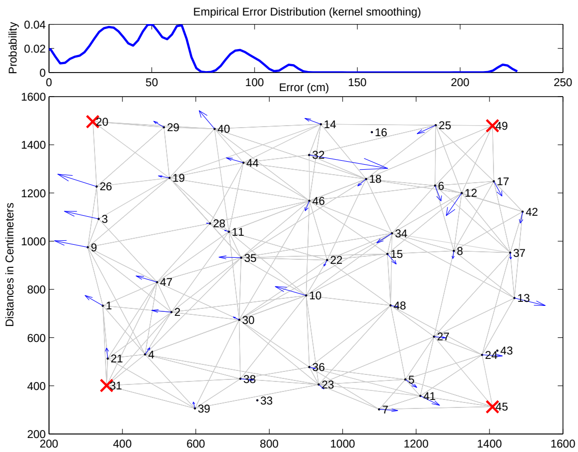


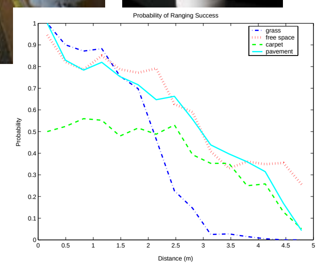


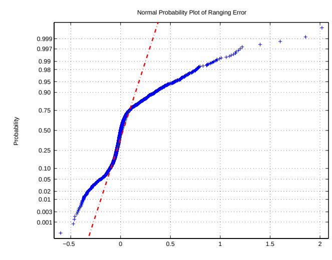
Ultrasound Results



- Non-gaussian error
- Probabilistic loss
- 50cm median error in deployment, as predicted



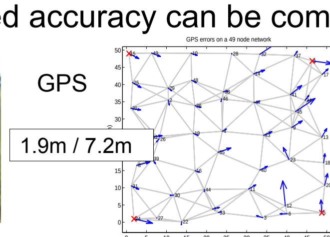




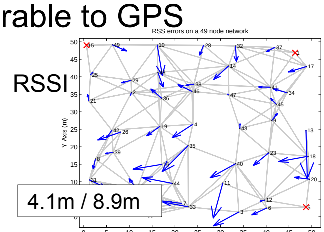
Signal Strength Results

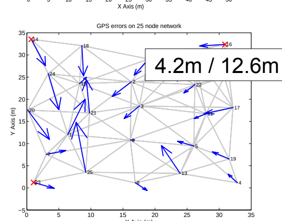
- Results vary greatly with each environment
- Pre-deployment analysis accurately predicted effects of environment, topology, and algorithmic parameters
- RSSI-based accuracy can be comparable to GPS

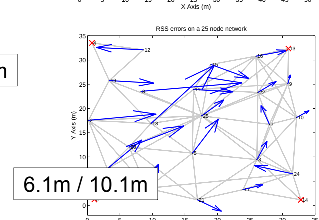
GPS



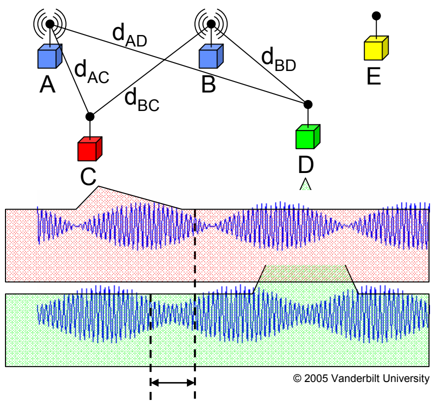
RSSI







Vanderbilt Radio Interferometric Ranging Champion to Date



relative phase offset of beat frequency
$= (d_{AD}-d_{BD}+d_{BC}-d_{AC})$ modulo λ
where $65cm < \lambda < 75cm$

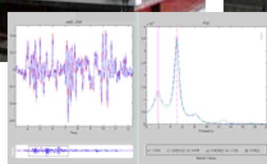
- COTS radio chip (CC1000 on MICA2)
  - transmit frequency: 400-460 MHz
  - wave length: 65 cm < λ < 75 cm
  - adjustable in 64 Hz steps
- Two senders (A and B) transmit simultaneously
  - frequency separation: 100-800 Hz
  - duration of transmission: 32 ms
- Several receivers (C, D and E) measure interference
  - sample radio signal strength at 8.9 kHz
  - beat frequency: 100-800 Hz
  - samples per beat: 10-80
  - beats per transmission: 3-25
  - use time synchronization with 1 μs precision to correlate phase offsets
  - result is $(d_{AD}-d_{BD}+d_{BC}-d_{AC})$ modulo λ
    - » d_{XY} is distance between X and Y
    - » λ is wave length of carrier frequency
  - expected error is less than 5 cm
- Perform multiple measurements with different frequencies to obtain $d_{AD}-d_{BD}+d_{BC}-d_{AC}$

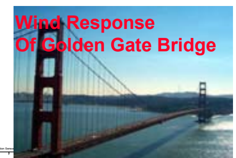
Akos Ledeczi, Miklos Maroti, et al

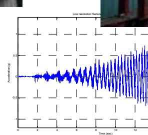
Technology Push matched by Application Pull

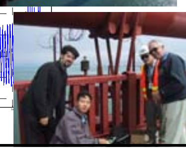
Structural Monitoring – Glaser, Fenves

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







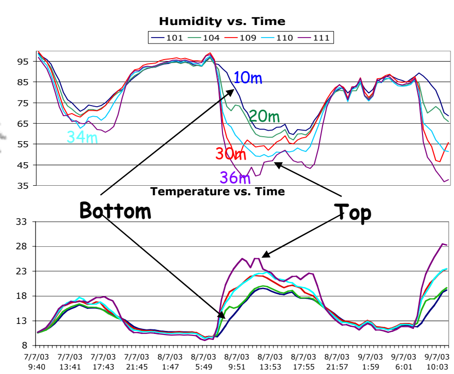


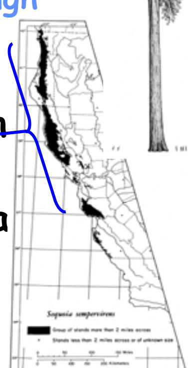
Forest Ecophysiology - Dawson

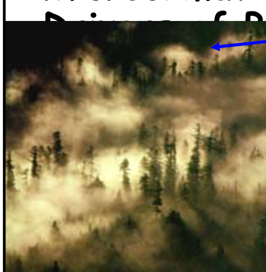
- TREES shape the hydrological cycle?
  - 2/3 of fresh H2O recycled through forests
- Microclimatic

lan

ma



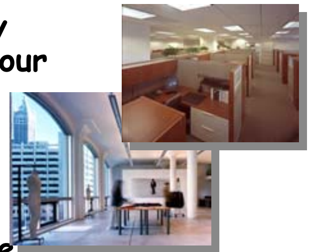


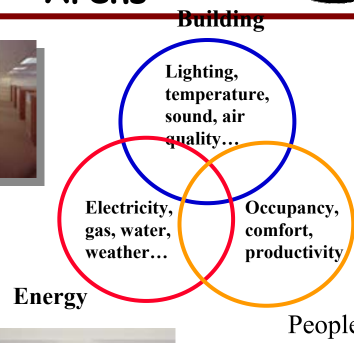


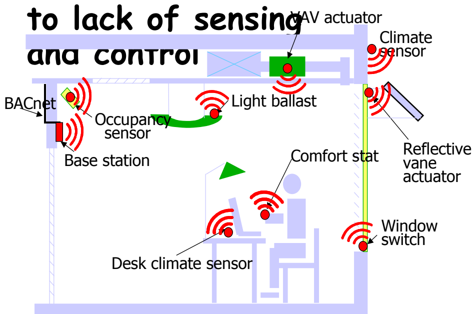
May 11th, 2003, unpublished

Built Environments - Arens

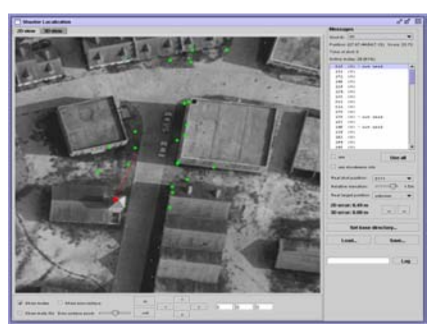
- 2/3 of US energy used to maintain our bldg environment
  - 40% lighting
- Inefficient, unhealthy, uncomfortable due to lack of sensing and control







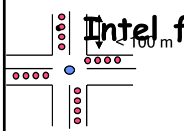
Shooter Localization Using SensorWebs



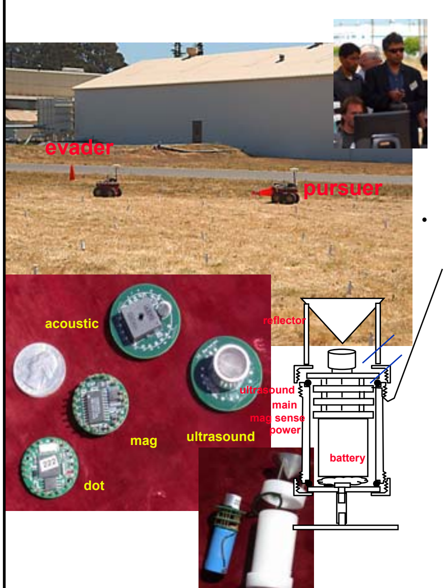
Berkeley motes and Vanderbilt algorithm

And many more

- Sitar - Firebug
- Agogino - Occupancy
- Varaiya - Traffic
- Wright – emergency personnel
- Brewer – ITC4B
- Student solar car
- Habitat Monitorin
- Intel f



Protection – Sastry, Culler, Brewer, Wagner



Detect vehicle entering sensitive area, track using magnetics, pursue and capture by UGV.

Components
- 10x10 array of robust wireless, self-localizing sensors over 400 m^2 area
- Low cost, robust 'mote' device
- Evader: human controlled Rover
- Pursuer: autonomous rover with mote, embedded PC, GPS

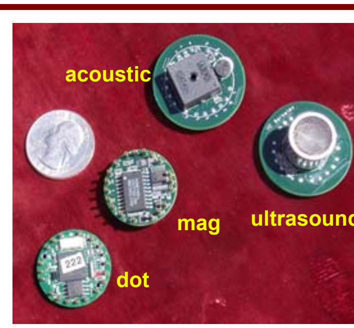
- Operation
  - Nodes inter-range (Ultrasonic) and self localize from few anchors, correct for earth mag, go into low-power 'sentry' state
  - Detect entry and track evader
    - » Local mag signal processing determines event and announces to neighbors
    - » Neighborhood aggregates and estimates position
    - » Network routes estimate from leader to tracker (multihop)
  - Pursuer enters and navigates to intercede
    - » Motes detect and estimate multiple events
    - » Route to mobile Pursuer node
    - » Disambiguates events to form map
    - » Closed inner-loop navigation control
    - » Closed information-driven pursuit control
    - » Capture when within one meter

Overall Demo Operation (2): Object Detection

- Evader enters field
- Pursuers enter field
- Each detecting mote announces its readings
- All readings in a neighborhood are aggregated
- Aggregate packet is routed through the root mote

OEP2 Hardware Platform

- Main board: Mica2 dot
  - ATmega microcontroller, Flash, clock
  - CC1000 frequency agile FSK radio
  - Small form-factor
  - Xbow based on Mica
- Sensor Board: magnetometer
  - Honeywell mag with 2-stage amplification
  - Set/reset circuit (5v)
  - 4-port digital Pot for biasing and filtering
- Ranging boards
  - Ultrasound
  - Acoustic
- Enclosure



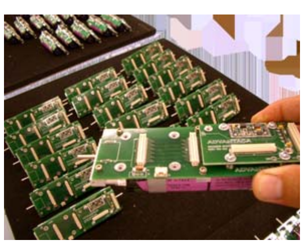
PEG Software Overview

- New routing protocol to relax dependency on localization service
- Remote configuration interface
  - Solution to a problem, not an original goal
- Network reprogramming
- System layer for remotely invoking disparate services
- Standard services
  - Sleep, ping, RF power, blink, network reprogram
- MATLAB command-line interface to network
- Strong decoupling between sensor networks and clients

PEG Demo from July 03

Mote Drop Experiences: Last 2 of 6 motes are dropped from MAV 29 Palms March 2001

Bald Camel Drop: China Lake 02/19/04



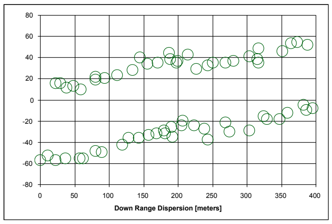
MIR integrated with Mica-2

Packaging to allow antennas to land pointing up

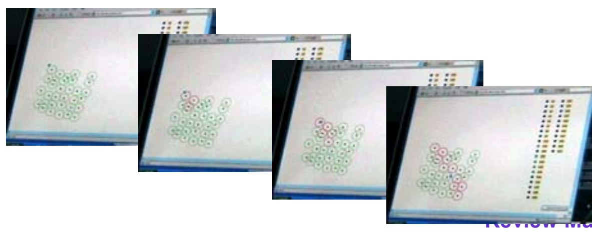
Explosive Dispenser

Aerial Drop from 500 ft.

Bald Camel Drop Feb 2004



Clockwise from top left: Actual Sensor Lay Down Pattern, Phoebus Chen walking through sensor field, Tracking of Phoebus through sensor field

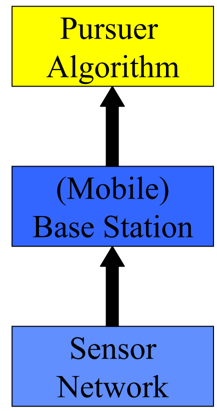


Big July 2005 Demo Philosophy

- **Midterm demos focused on *building* real applications**
  - "Will this work at all?"
- **ExScal focuses on *scaling* real applications**
  - "How big can it get?"
- **Capstone will focus on *evaluating* real applications**
  - "Can we describe, characterize, and predict how well it works?" Metrics, Metrics, Metrics
  - This is our opportunity and need to leverage experience toward good science
  - Deployment over a period of time (2-3 weeks) at Richmond Field Station not just in field but spread out over the station

Capstone Goals

- Establish metrics to evaluate PEG
  - Metrics vary at each abstraction level
  - Pursuer Algorithm cares about:
    - » Sensor Accuracy, Latency, Missing Data, False Alarm Rate, etc.
  - "Quality" of data stream from the Base Station depends on:
    - » Network Congestion, Node Density, Power Consumption Constraints, Physical Distance, etc.
- Simulations
- Experiments
- Characterize and predict



Towards Final Demo

- Redeployed substantial sensor field to collection data and develop metrics
- Worked with EXSCAL design to ensure can reuse XSM as sensor platform for final demo
  - Attach Telos as standalone or as bridge
- Replace/ augment acoustic localization with RSSI
- Airborne pursuer, airborne drop simulated
- Multiple evaders
- Focus on middleware architecture, science, measurement, ease of deployment, and reliability
  - Developed a baseline management architecture

Script for Final Demo: Aug 2005

- 1000+ XSM + Telos motes spread out over urban area (Richmond Field Station: area approximately 3 sq. km. Including several buildings, varying topography, trees, …). Experiment will be up and running for 2 weeks: fully instrumented.
- Base line demo components developed by UCB team. Technology Developers can swap in their components: localization, time synchronization, tracking, network management, network programming.
- Scenario: Evaders are humans/robots. Pursuers are humans/robots: some aerial and some ground robots. Distinguish between red forces, blue forces and green forces in tracking algorithms to minimize capture time or localization
- UAVs with motes used to localize sensor field
- Sensor fields to cue higher bandwidth sensors (cameras)
- Metrics: time to capture, energy expenditure, ease of re-programmability

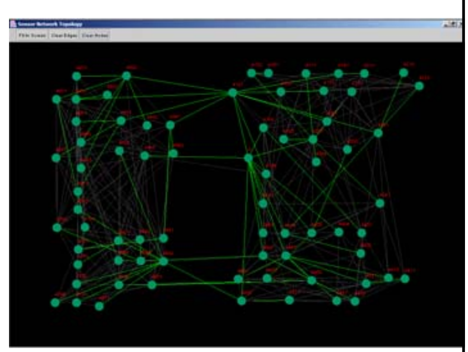
Features of Final Demo

- Pursuit evasion games with red, blue and green forces, a combination of pre-deployed sensor webs, MAV dropped sensor webs, MAV/UGV camera platforms and other higher bandwidth assets
- Persistence/Reprogrammability
- Network Management
- MOBILE Sensor Webs
- Determination of Pursuit and Evasion policies and tactics

Implementation in an Instrumented Testbed

- 9 x 5 grid of 45 motes
- 10 ft by 20 ft area, 2.5 ft spacing
- Ethernet backend for monitoring/data collection
- Multiple robots running underneath mesh of sensors
- Camera for "ground truth" position of robots

Soda Hall Routing Environment



Conceptual Issues

- Given a certain WSN, can we successfully design a particular application?
- How does the application impose constraints on the network?
- Can we derive important metrics from those constraints?
- How do we measure network parameters?

We need analytical tools and experimental data

What can you do with a sensor network?

- Literature provides key asymptotic results
- We are interested in answer different semantic questions, e.g.:
- At the algorithmic level:
  - How much packet loss can a tracking algorithm tolerate?
- At the network level:
  - How many objects can a particular sensor network reliably track?

Expanding the Vision

Legal / Privacy – Samuelson, Mulligan

- TOWARD A LEGAL FRAMEWORK FOR SENSOR NETWORKS
  - existing laws?
  - new laws or regulations
- Modes of Regulation and Policy
- Evolving notions of Privacy
- FAIR INFORMATION PRACTICES
  - Limitations on collection of data
  - specific purpose
  - Notice and choice
  - Verifiability
  - Accuracy, Security
  - Accountability

Small Technology, Broad Agenda, Unique Confluence

- Social factors
  - security, privacy, information sharing
- Applications
  - long lived, self-maintaining, dense instrumentation of previously unobservable phenomena
  - interacting with a computational environment
- 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

Secure SCADA and beyond

We think that there is a great deal to be done in terms of operationalizing secure versions of SCADA (Supervisory Control And Data Acquisition) and DCS (Digital Control Systems) for the infrastructures considered, especially power, natural gas, chemical and process control, etc. However, the sense was that this infrastructure was going to be gradually replaced by networked embedded devices (possibly wireless) as computing and communication devices become more ubiquitous and prevalent. Thus, the major research recommendations were for an area that we named Secure Networked Embedded Systems (SENSE).

SCADA of the Future

- Current SCADA
  - Closed systems, limited coordination, unprotected cyber-infrastructure
  - Local, limited adaptation (parametric), manual control
  - Static, centralized structure
- Future requirements
  - Decentralized, secure open systems (peer-to-peer, mutable hierarchies of operation)
  - Direct support for coordinated control, authority restriction
  - Trusted, automated reconfiguration
    - » Isolate drop-outs, limit cascading failure, manage regions under attack
    - » Enable re-entry upon recovery to normal operation
    - » Coordinate degraded, recovery modes

Secure Network Embedded Systems

Embedded Software prevalent in all critical infrastructures. Critical to high confidence embedded software are open source techniques for

- Automated Design, Verification and Validation
  - Verified design in a formal, mathematical sense
  - Validated design in an engineering sense
  - Certifiable design to allow for regulatory and certification input
- High Confidence Systems
  - Narrow waisted middleware
    - » Trusted abstractions, limited interfaces
    - » Algorithms and protocols for secure, distributed coordination and control
  - Security and composable operating systems
  - Tamper Proof Software
- Generative Programming
- Intelligent Microsystems: infrastructure of the future with security codesign with hardware and software.

Adaptive Networked Infrastructure

Core partners: Berkeley (lead), Cornell, Vanderbilt

Outreach partners: San Jose State, Smith, Tennessee Tech, UC Davis, UC Merced.

Principal investigator: Edward A. Lee, Professor, EECS, UC Berkeley, eal@eecs.berkeley.edu

•***Enabling technologies***: wireless networked embedded systems with sensors and actuators

•*Approach*: Engineering methods for integrating computer-controlled, networked sensors and actuators in societal-scale infrastructure systems.

•***Resource management test beds***:
- electric power
- transportation
- water

The ANI ERC

- ***Deliverables***: Engineering Methods, Models, and Toolkits for:
- design and analysis of systems with embedded computing
- computation integrated with the physical world
- analysis of control dynamics with software and network behavior
- programming the ensemble, not the computer

Strategic Framework