Sensor Networks for Emergency Response: Challenges and Opportunities

Moulton (B.U), Lorincz et. al. (Harvard)

Ryan Seney
seneyr@wpi.edu

CS525M – Mobile & Ubiquitous Computing
3/28/2006

Overview

- Introduction
- CodeBlue Infrastructure
- Wireless Vital Sign Monitors
- Security Implications
- MoteTrack: RF-based Location Tracking

Introduction

- CodeBlue is a suite of applications
  - Wearable vital signs monitors
  - MoteTrack: personnel and patient tracking
- Tested by developing two monitors and PDA for triaging

CodeBlue Infrastructure

- **Discovery & Naming**
  - Device naming should be application centric
  - Decentralize discovery process to avoid single point of failure
- **Robust Routing**
  - Devices might need to communicate with others outside their immediate range
  - Ad hoc routing improves this through relaying
  - Vital sign sensors may need to send data to multiple devices

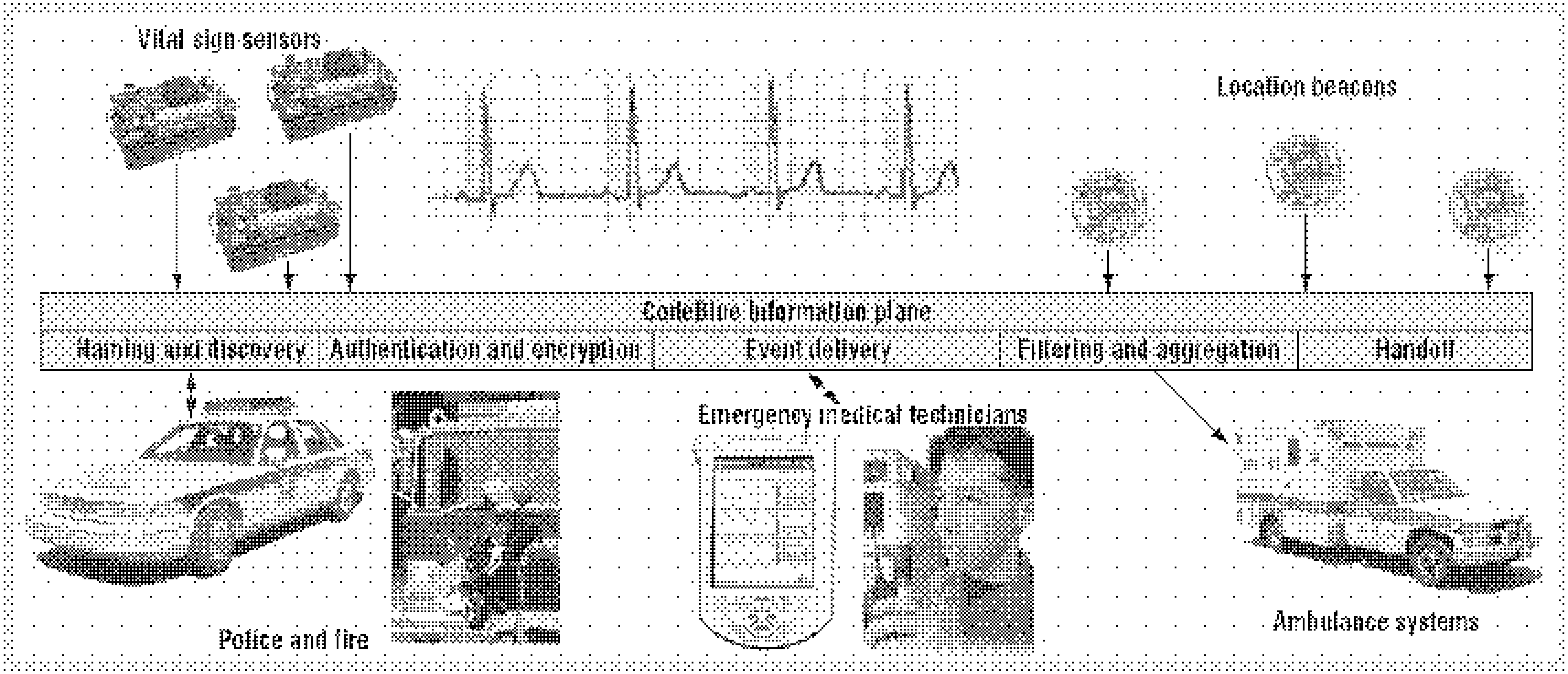
CodeBlue Infrastructure

- **Prioritization**
  - Very limited bandwidth in low-powered sensor radios
  - Critical data MUST get delivered
    - Vital signs on patient in cardiac arrest, SOS messages, etc take priority
- **Security**
  - Efficient establishment of security credentials
    - Fluctuating number of responders and patients
    - Pre-deployed public key should not be assumed
    - Most devices won't have processing power to handle strong cryptography protocols

CodeBlue Architecture

- CodeBlue is an “information plane” providing services
  - Flexible naming scheme
  - Publish and subscribe routing framework
  - Authentication and encryption
  - Credential establishment and handoff
  - Location tracking
  - In-network filtering and aggregation

CodeBlue Architecture



CodeBlue Architecture

- Previous similar systems
  - Patient Centric Network
    - Common architecture for sensors in hospital rooms
    - Not focused on low power sensors in emergency response
  - Agent Based Casualty Care
    - Developing wearable physiological sensors

Wireless Vital Sign Monitors

- Merger of motes with vital sign monitors
  - Mote: Low-power, low-capability device
- Used Mica2 developed at UC Berkely
  - 7.3 MHz Amtel ATmega128L running TinyOS
  - 4 Kbytes RAM, 128 Kbytes ROM
  - Chipcon CC1000 Radio
    - 76.8 kbps, 20-30 meters indoors range
  - 5.7 cm x 3.2 cm x 2.2 cm
  - AA Batteries for continuous power up to a week
    - Up to months or years with duty cycling

Wireless Vital Sign Monitors

- Limited bandwidth and computing power limits use of TCP/IP, DNS and ARP (Address Resolution Protocol)
- However, incredibly mobile and versatile
  - Other nodes exist integrating all Mica2 functions onto a 5 mm^2 chip

Wireless Vital Sign Monitors

- **Non-invasive monitors**
  - **Heart rate, oxygen saturation, end-tidal CO_2 and serum chemistries**
- **Similar wireless enabled monitors**
  - **Nonin and Numed: sensors with Bluetooth**
  - **Radianse: RF-based location tracking system for hospital use**
  - **Mobi-Health Project: Continuous monitoring of patients with 3G enabled "Body-Area Network"**

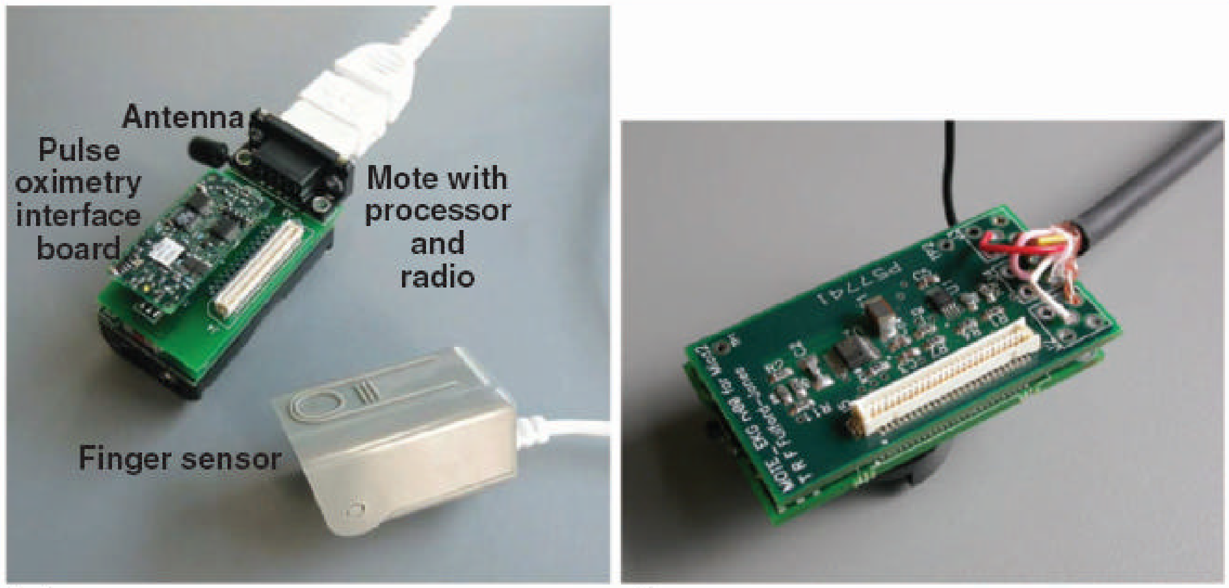
Wireless Vital Sign Monitors

- **Mote-based sensors**
  - Pulse Oximeter:
    - Used by EMTs to measure heart rate and blood oxygen saturation (SpO_2)
    - Measures amount of light transmitted through non-invasive sensor on patient's finger
    - Smith-BCI daughterboard attached to Mica2 mote
      - Transfers heart rate and SpO_2 about once a second

Wireless Vital Sign Monitors

- Mote-based sensors
  - Two-lead electrocardiogram (EKG)
    - Continually monitors heart's electrical activity through leads connected to patient's chest
    - Reports heart rate and rhythm
    - Custom built circuit board attached to Mica2 mote
      - Captures data at rate of 120 Hz
      - Compresses through differential encoding and transmits through Mica2 radio

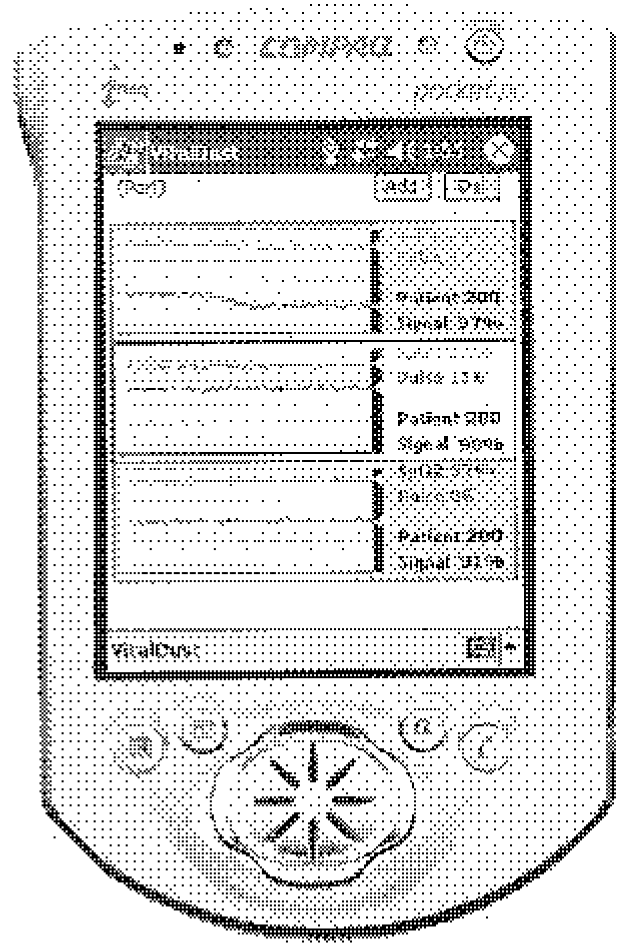
Wireless Vital Sign Monitors



(a) (b)

Wireless Vital Sign Monitors

- EMTs carry handheld computers (PDAs)
- Receive and visualize vitals from multiple patients
- Audible and visual alerts if vitals are outside specified range
- PDA data can be transferred to patient care record applications (iRevive)
  – Record patient history, identification and any intervention techniques



Security Implications

- **Security important since patient records are confidential**
- **HIPAA (1996) mandates all medical devices must ensure privacy of patients' medical data**
- **Defense against capturing data, spoofing and DOS attacks in the field**

Security Implications

- Should not assume that all organizations have exchanged security information (keys, certificates, etc.) ahead of time
- Personnel can't spend time typing passwords, logging into databases, etc. when arriving on the scene of an incident

Security Implications

- Ad hoc network security that self-organizes based on devices present
- Must cope with changing number of nodes
  - Emergency personnel arriving, patients transported away
- Seamless credential handoff
  - First responder gives access rights to another without preexisting relationships between the two

Security Implications

- Traditionally use trusted outside authority for maintaining current information about access rights
- Architecture for outside contact might not be available at disaster scene
- Best-effort security model might be appropriate
  - Strong guarantees when outside connection available, weaker guarantees with poor or no connectivity
- Public key crypto can solve most of the above
  - But limited resources on sensors make this hard
  - Eg. 4 Kbytes of memory in Mica2 limits number of keys to be stored

Security Implications

- Elliptic Curve Cryptography as alternative
  - 163 bit ECC key equivalent to 768-bit RSA
  - Implement with integer arithmetic
    - No hardware floating point support on sensors
- Key generated in 35 seconds
  - Good performance if not frequently performed
- Could be used for generating symmetric keys in TinySec

Security Implications – Future Work

- Take advantage of available computing power
  - PDAs and laptops generate keys
  - Not complete solution since sensor nodes still need to know which devices to trust in order to offload security computations

MoteTrack: RF-based Location Tracking

- Two applications
  - Patient locating
    - Monitoring various patients need to know where they are located in case they need attention
  - Tracking responders in buildings
    - Firefighters in building with poor visibility, monitoring safe exit routes, central command monitoring

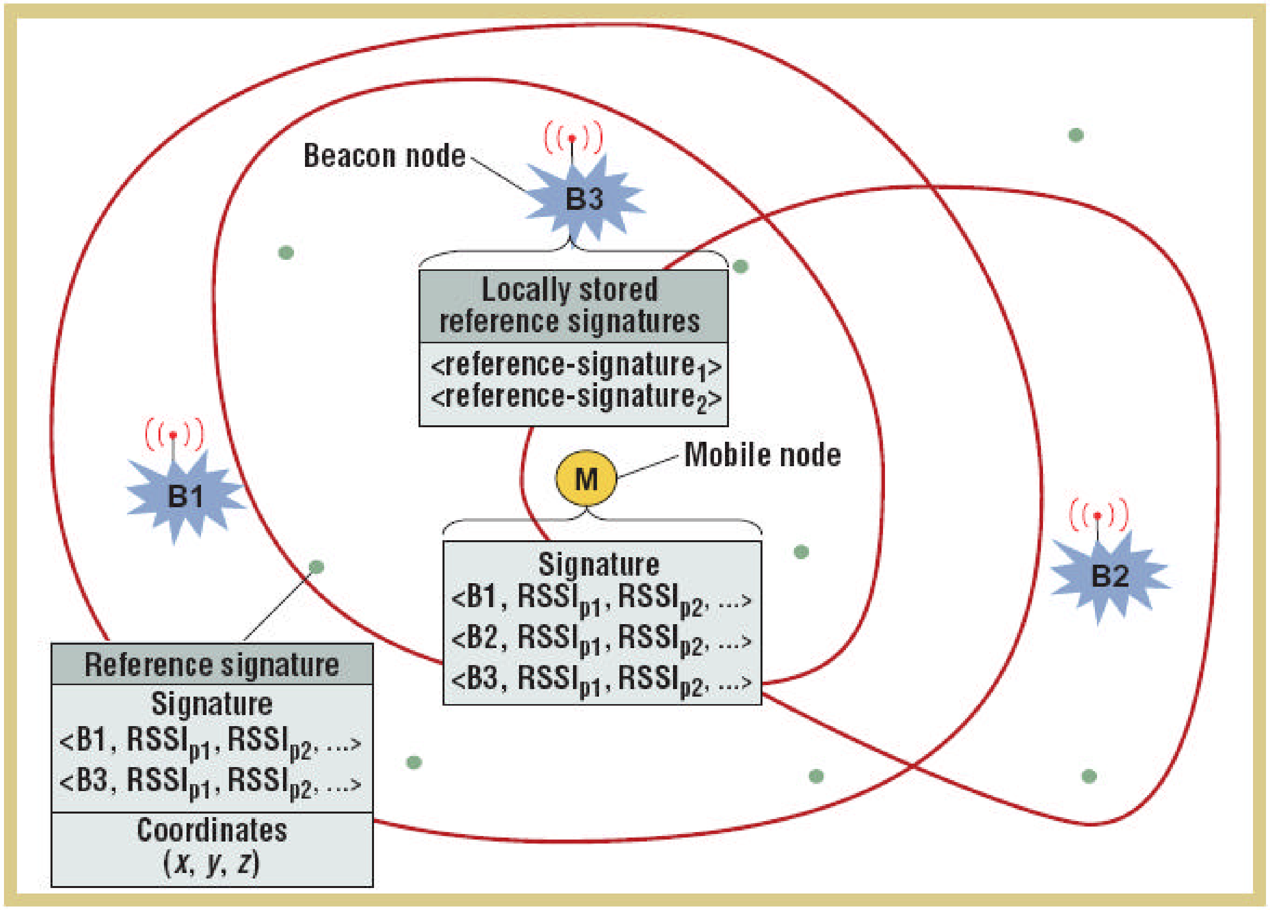
MoteTrack: RF-based Location Tracking

- Decentralized sensor network using low-power single-chip radio trancievers
- Provides good location accuracy even with partial failures of tracking infrastructure
- Populate area with battery operated beacon nodes
  - Replace existing smoke detectors with new detectors containing integrated beacon node

MoteTrack: RF-based Location Tracking

- Beacon nodes periodically broadcast beacon messages
  - Tuple containing {sourceID, powerLevel}
    - sourceID is unique identifier of the node
    - powerLevel is transmission power level used to broadcast message
- Mobile nodes listen for some time to acquire a signature
  - Beacon messages received over time interval, and received signal strength indication (RSSI) for each message

MoteTrack: RF-based Location Tracking



MoteTrack: RF-based Location Tracking

- **Reference signature is a signature plus a known 3D location**
- **Two phase process for estimating locations**
  - **Once beacons installed use a mobile node to acquire reference signatures at known, fixed locations throughout area**
  - **Later, mobile nodes can obtain a signature and send it to beacon node from which it received the strongest RSSI to estimate its current location**

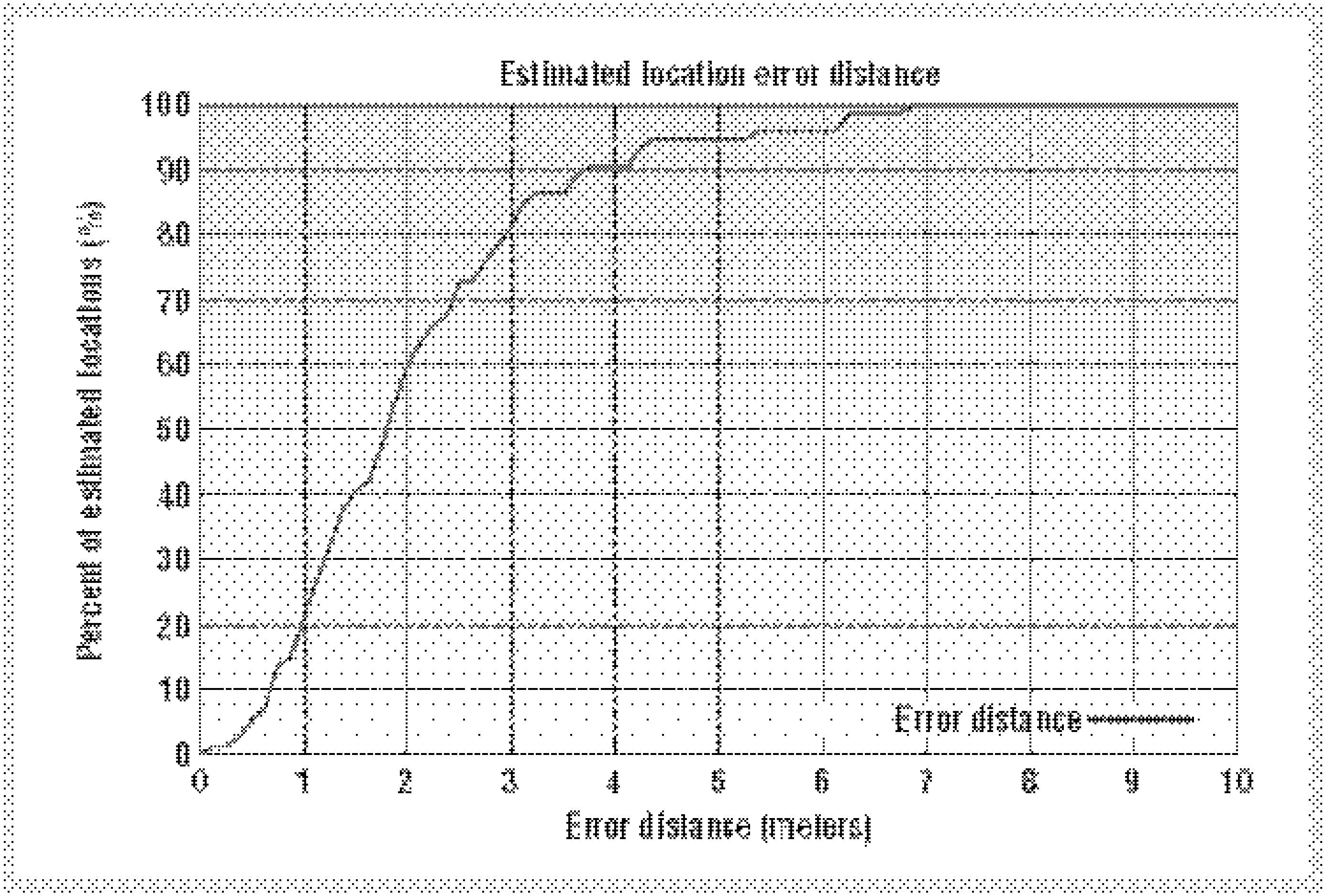
MoteTrack: RF-based Location Tracking

- System resembles RADAR, but:
  - MoteTrack is decentralized, no main back-end database involved
  - Replicates reference signatures set across beacon nodes so that each node stores only a subset of the reference signatures
  - Beacon nodes perform all data storage and computations using locally stored reference signatures

MoteTrack: RF-based Location Tracking

- MoteTrack tested on Harvard campus
- 20 beacon nodes distributed on one floor of CS building
- 1742m^2 area covered
- Achieved 80th percentile location accuracy of 3 meters over 74 separate location estimates
- Tolerate failure of up to 40 beacon nodes with negligible increase in error
- Accuracy is roughly the same as commercial 802.11 based location tracking systems
- Ultrasound based systems have higher accuracy
  - Denser beacon placement and directional beacons

MoteTrack: RF-based Location Tracking



Obligatory Questions Page

- Questions?