Reading:

Wireless Sensor Networks (WSNs)

- Microsensors
  - Low power, cheap sensors
  - Sensor module (e.g., acoustic, seismic, image)
  - A digital processor for signal processing and network protocol functions
  - Radio for communication
  - Battery-operated

- Sensors monitor environment
  - Cameras, microphones, physiological sensors, etc.
  - Gather data for some purpose

- Hundreds or thousands of nodes scattered throughout an environment
- Each sensor can collect data
- Data routed via other sensors to a sink or base station node
WSNs (cont.)

- Sensor data limited in range and accuracy
  - Each node can only gather data from a limited physical area of the environment
  - Data may be noisy
  - Data aggregation enables higher quality (less noisy) data to be obtained that gives information about a larger physical area than any individual data signal

- Networking sensors enables
  - Extended range of sensing $\rightarrow$ improved quality
  - Fault tolerance due to redundancy in data from different sensors
  - Distributed processing of large amounts of sensor data
  - Scalability: quality can be traded for system lifetime
  - “Team-work”: nodes can help each perform a larger sensing task
WSN Applications

- New wireless networking paradigm
  - Requires autonomous operation
  - Highly dynamic environments
    - Sensor nodes added/fail
    - Events in the environment
  - Distributed computation and communication protocols required

- Applications
  - Home security
  - Machine failure diagnosis
  - Chemical/biological detection
  - Medical monitoring
  - Surveillance and reconnaissance
  - Animal/plant monitoring (e.g., for research)
Example Application: Environmental Monitoring

- Traffic patterns many-to-one
- Raw sensor data or high level descriptions about environmental phenomena

Example projects
- ZebraNet
- Ecology of rare plants in Hawaii
Example Application: Health Monitoring

- Sensors monitoring vital signs
  - Blood pressure, heart rate, EKG, blood O2
- One or more sensors indicate abnormality
  - Inform person
  - Take corrective measures
    - Control pacemaker functions
    - Automatically dispense medication
  - Alert emergency team
- Sensing, processing, understanding, feedback/control
- Requires protocols that are
  - Reliable
  - Flexible
  - Scalable
  - Secure
Sensor Platforms

- Example platforms
  - Smart Dust (UC Berkeley)
  - Berkeley Motes
  - Telos Motes (MoteIV)
  - iBadge (UCLA)
  - WINS (UCLA)
Sensor Platforms
WSN Limitations

- Sensor energy
  - Each sensor node has limited energy supply
  - Nodes may not be rechargeable
  - Eventually nodes may be self-powered
  - Energy consumption in sensing, data processing, and communication
    - Communication the most energy-intensive
    - Must use energy-conserving communication

![Power consumption of node subsystems](image)
WSN Limitations (cont.)

- Communication
  - The bandwidth is limited and must be shared among all the nodes in the sensor network
  - Spatial reuse essential
  - Efficient local use of bandwidth needed
## WSNs vs. MANETs

<table>
<thead>
<tr>
<th>General Ad Hoc Networks</th>
<th>Sensor Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unreliable communication</td>
<td>Unreliable communication</td>
</tr>
<tr>
<td>Require self-configuration</td>
<td>Require self-configuration</td>
</tr>
<tr>
<td>Constrained energy and bandwidth</td>
<td>Very constrained energy and bandwidth</td>
</tr>
<tr>
<td>Small-scale</td>
<td>Large-scale</td>
</tr>
<tr>
<td>Typically mobile</td>
<td>Typically immobile</td>
</tr>
<tr>
<td>Competitive</td>
<td>Cooperative</td>
</tr>
<tr>
<td>One-to-one traffic pattern</td>
<td>Many-to-one traffic pattern</td>
</tr>
<tr>
<td>Address-centric</td>
<td>Data-centric</td>
</tr>
<tr>
<td>QoS: delay, etc</td>
<td>Application-specific QoS</td>
</tr>
</tbody>
</table>
Design Factors

- What are the important features of WSNs?
- Fault tolerance/reliability
  - Network should be robust to individual node failures
  - Failures due to running out of energy, hardware failures, malicious intercept of sensor, etc.
- Scalability
  - Protocols must scale to thousands or millions of sensor nodes
  - Requires intelligent management of high density nodes
- Cost
  - Must have cheap sensors
Design Factors (cont.)

- **Topology**
  - Deployment: random or deliberate placement of nodes
  - Changes in topology during network operation
    - New nodes added to the system
    - Nodes failing
    - Environmental changes

- **Energy consumption**
  - Sensor functions: sensing, communication, data processing
  - All require energy
Evaluating WSNs

- What are the performance metrics for WSNs?
  - System lifetime
    - E.g., time until network partition
    - E.g., time until probability of missed detection exceeds a threshold
  - Quality of result of sensor network
    - Application-specific measure
    - Latency of data transfer
    - SNR of aggregate data signal
    - Probability of missed detection or false alarm
  - Tradeoffs can be made among network parameters
    - E.g., can reduce quality of result of sensor network to increase system lifetime
Taxonomy of WSN Architectures

- In what ways do sensor networks for various applications differ?
- Data sink(s)
  - Embedded within network
  - Network edges
  - Mobile access point
  - One or several
- Sensor mobility
  - Typically stationary sensors
  - Some projects use mobile sensors
    - ZebraNet
    - Military operations
    - Self-propelled sensors
    - Robots
Taxonomy (cont.)

- Sensor resources
  - Memory
  - Processing
  - Transmit power (fixed vs. variable)
  - Locations/density

- Traffic patterns
  - Event-driven applications
  - Continuous data generation
  - Query-driven applications
Design Issues

- New protocols needed
- MAC
  - Cooperative nature of sensor networks (fairness not an issue)
  - Exploit traffic patterns
  - Energy efficiency extremely important
    - Reduce idle listening
    - Reduce unnecessary reception
- Routing
  - Different traffic models
  - Data dissemination rather than point-to-point routing
  - Data-centric rather than address-centric
  - Location-aware sensors
  - Resource-aware routing needed
  - Exploit local aggregation
Design Issues (cont.)

- Topology control
  - Reduce idle power consumption → nodes sleep
  - Create fully-connected dominating set from active routers

- Transmission power control
  - How to avoid “hot spot” problem?
  - Provide connected network

- QoS Management
  - QoS determined by content of data rather than amount
  - Transport layer
    - Intelligent congestion management
    - Throttle back irrelevant data rather than each node’s sending rate
  - Coverage
    - Ensure enough sensors provide data
    - K-coverage: each location monitored by at least K sensors
Design Issues (cont.)

- Time synchronization
  - Very important in sensor networks
  - Needed to determine if event sensed by two sensors is in fact the same event
  - Needed to determine object speed
- Approaches
  - GPS – expensive, not energy-efficient
  - NTP (used in computer networks) – not enough precision
  - Newer approaches being researched
    - Romer’s Algorithm
    - Reference-Broadcast Synchronization (RBS)
Design Issues (cont.)

- Localization
  - Important for same reasons as time synchronization
  - Often times, only relative position is necessary
    - GPS is overkill and unattractive for energy reasons
    - RSSI used to infer distances
    - Time of Arrival (ToA)
    - Time Difference of Arrival (TDoA)
    - Angle of Arrival (AoA)
  - Sensor can find its own location using received beacons
  - Sensor can have other nodes measure its location
    - Sensor sends beacon message and neighbors use trilateration based on signal strength measurements
  - Problem – small scale fading
Research Issues (1)

- Appropriate QoS model
  - Traditional networks: delay, packet delivery ratio, jitter
  - Sensor networks: probability of missed detection of an event, signal-to-noise ratio and network sensing coverage
  - Difficult to translate these data-specific QoS parameters into meaningful protocol parameters

- Cross-layer Architectures
  - Entire protocol stack tailored to specific needs of WSN application
  - Protocols should be integrated with hardware
  - Trade-off: generality and ease of network design to achieve lifetime increases
Research Issues (2)

- Reliability
  - Links and sensors may fail, temporarily or permanently
  - Must design protocols to provide reliable service with these failures
- Heterogeneous Applications
  - Sensor nodes may be shared by multiple applications with differing goals
  - Protocols must efficiently serve multiple applications simultaneously
- Heterogeneous Sensors
  - How to make best use of resources in heterogeneous sensor networks
Research Issues (3)

- **Security**
  - How much and what type of security is really needed?
  - How can data be authenticated?
  - How can misbehaving nodes be prevented from providing false data?
  - Can energy and security be traded-off such that the level of network security can be easily adapted?

- **Actuation**
  - Eventually sensor networks will “close the loop”
  - Data do not need to reach base station
  - Current models for sensor networks may not be valid
Research Issues (4)

- Distributed and Collaborative Data Processing
  - How to best process heterogeneous data?
  - How much data and what type of data should be processed to meet application QoS goals while minimizing energy drain?

- Integration with Other Networks
  - Sensor networks may interface with other networks, such as a WiFi network, a cellular network, or the Internet
  - What is the best way to interface these networks?
  - Should the sensor network protocols support (or at least not compete with) the protocols of the other networks?
  - Or should the sensors have dual network interface capabilities?
Discussion