



# Wireless Sensor Networks An Overview

Pavlos Papageorgiou

# Overview

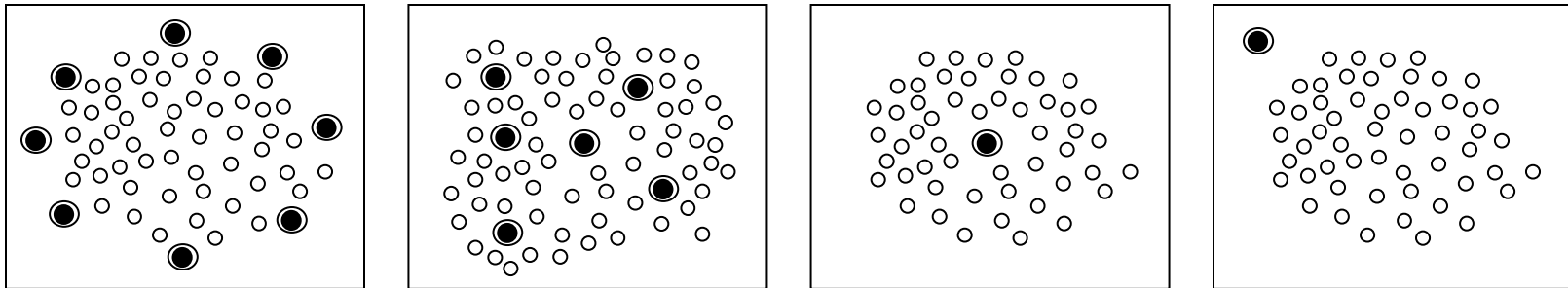


- 
- Definition of Wireless Sensor Network
  - Differences from other wireless networks
  - Design issues
  - Routing
  - Media Access Control
  - Security
  - Open Research Issues

# What is a Wireless Sensor Network (WSN)?



**Network of small wireless sensor devices, deployed in an ad-hoc fashion to cooperate on sensing a physical phenomenon**



- Collaborative network of large number of loosely connected nodes
- Wireless communication medium
- Deployed only once
- Distributed system tasked to sample environment for sensory information
- Combines and compresses small fragments of possibly inaccurate data
- Propagates data back to the user through gateways
- Traffic moves over several hops
- Various scenarios for gateway placement (multiple, on the edge, mobile)

# Sample application scenarios

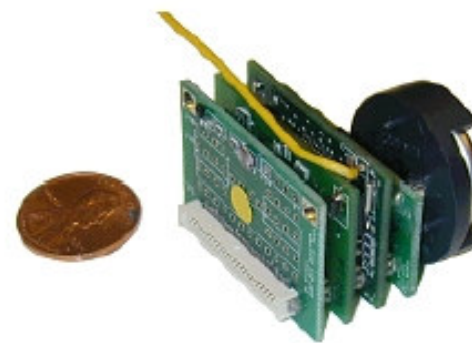


- Environmental monitoring of inhospitable areas
  - Chemical spills
  - Fire detection
  - Disaster recovery
  - Natural habitat monitoring
- Embedded in structures
  - Integrity checking of building, airplanes
  - Detection of life signs in case of building collapse
- Military applications
  - Surveillance
- Analyzing environmental phenomena
  - Tornados, tides
- Urban monitoring
  - Traffic congestion
  - Utility monitoring

# Sensor Node



- ATMEL 4MHz 8bit microcontroller
- 8 KB program memory
- 512 bytes data memory
- Single channel RF at 916MHz
- 10kbps transmit rate
- On-Off keying encoding
- Sensing transducers integrated
  - Light, temperature, humidity, pressure, magnetic field, etc.
- TinyOS real-time OS



Berkeley Mote  
[www.xbow.com](http://www.xbow.com)

# Observer's view



- Desired properties of WSN
  - Information retrieval on demand
  - Notifications about events of interest
  - Configurable sensing tasks / events of interest
  - Configurable latency
  - Information integrity and accuracy
  - High Availability even when failures occur
  - Deploy only once
  - Unattended operation
  - Low cost
  - Long system lifetime
  - Ability to reprogram sensor task after deployment

# Designer's view

---



## ■ Hardware Design

- Sensing range
- Communication range
- Communication method (RF, Infrared, Optical)
- Ultra low power paging mechanism
- Energy harvesting from the environment
- Aggressive energy management

## ■ Protocol Design

- Low overhead
- Resource adaptive
- Fault tolerant
- Prefer processing over communication
- Extremely scalable
- Cross-layer design
- Sleep most of the time
- Wake-up on demand
- Sensors not addressable

# Differences from ad-hoc wireless networks



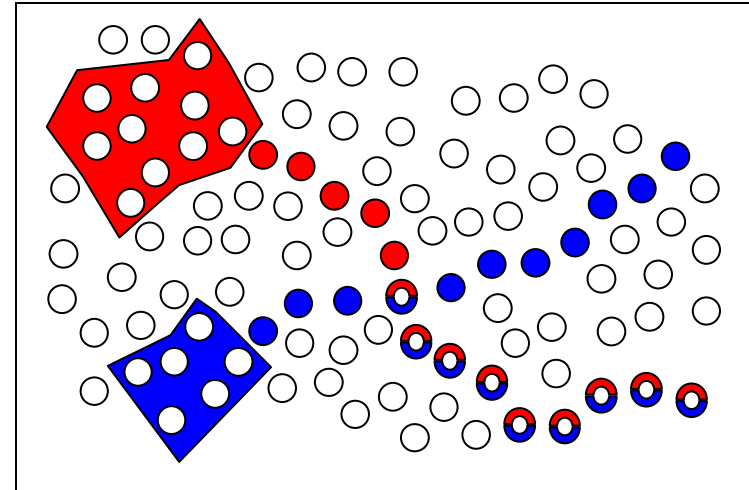
- Severe constraints
  - Available energy is hard constraint; not cost function
  - Processing power
  - Storage / Memory
  - Small size ( $<1\text{cm}^3$ )
  - Low cost ( $\ll \$1$ )
  - Transmission and reception consume the same energy
- Usage
  - Departure from 2-entity model; no notion of peers
  - Lack of global identification
  - Collaborative information gathering and propagation
- Traffic Characteristics:
  - Variable and highly correlated
  - Long periods of inactivity
  - Short periods of intense traffic
  - Periodic sampling yields correlated bursts
  - Data-centric
- Frequent topology changes
  - Node mobility
  - Node sleep patterns
  - Environmental interference
  - Node failures
  - Node battery depletion

# Rumor Routing



- Multiple paths to events
  - Paths may not be optimal
  - Query sent on random walk until it crosses path to event
  - Possible to never cross path
  - Revert to query flooding

D. Braginsky, D. Estrin WSNA 2002



- Setting up the paths
  - Event nodes generate agents that travel the network
  - Long lived agents create paths towards events they encounter
  - Paths created as state at nodes (event forwarding table)
  - Agent synchronizes event table with nodes as it travels
  - Agent uses straightening algorithm to determine next hop
  - Due to broadcast medium, agent leaves thick path

# LEACH: Hierarchical Routing



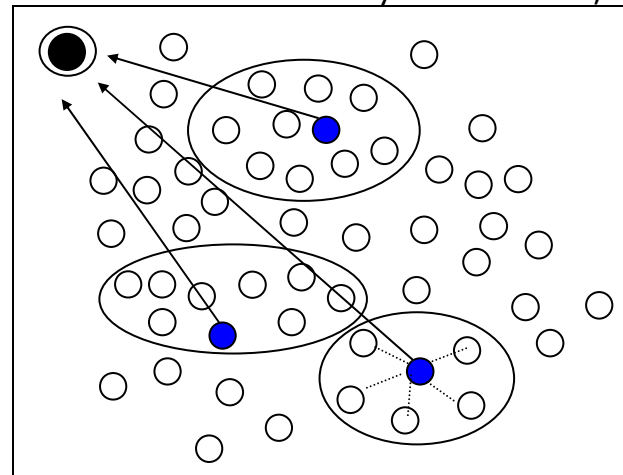
- 2-level hierarchical routing

- Minimize global energy
- Distribute energy consumption
- Form clusters with local coordination
- Rotate high-energy cluster heads
- Locally compress data
- Nodes always have data to send

- Operation

- In every round nodes self organize in clusters
- One node serves as cluster head
- Each node decides whether to become cluster head
- Non-cluster heads decide which cluster to join
- Cluster heads advertise TDMA schedule for members
- Members send to cluster head (low energy transmission)
- Cluster head sends to base station (high energy transmission)

Heinzelman, Chandrakasan, Balakrishnan  
Hawaii Intl Conference on System Sciences, 2000

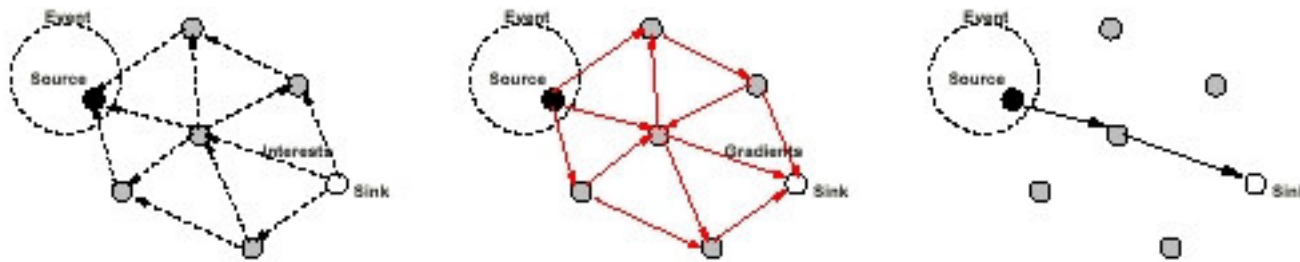


# Directed Diffusion



## Directed Diffusion: A Scalable and Robust Communication Paradigm

Intanagonwiwat, Govindan, Estrin  
USC/ISI



- Interest of the sink is diffused by name in the network
- Interest has specified attributes and rate
- Each node maintains interest cache of neighbors (not the originator)
- The node propagates the interest to its neighbors and “gradients” are formed towards the sink
- Identical interests from different neighbors are aggregated
- When event happens, source node propagates information along the gradient through a reinforced path

# Media Access Control



---

## A Transmission Control Scheme for Media Access in Sensor Networks

A. Woo and D. Culler

Berkeley

---

- Adapting CSMA based medium access for WSNs
  - Achieve fairness
  - Energy efficient
- Listening combined with backoff mechanism
  - Node introduces random delay before transmission
  - Constant listening period
  - If channel not free enter backoff and turn off radio
  - Backoff period is also applied as a application phase shift
- Contention control mechanism
  - Use minimum number of control packets RTS/CTS
- Rate control mechanism
  - MAC should control the rate of originating data to allow route-thru traffic. Achieves fair allocation of bandwidth.

# Security Issues



---

**Service available to legitimate users whenever they request it.**

---

- Availability
  - Service available to legitimate users whenever they request it
- Authenticity
  - To whom can a node talk?
- Integrity
  - Node has not been maliciously altered
    - Sensing subsystem vulnerable
    - Tamper resistance is costly
    - Core bootstrap portion must be protected
- Confidentiality
  - Once authenticity has been established, secrecy can be accomplished with secret session keys

# Security Issues : Availability



---

**Service available to legitimate users whenever they request it.**

---

- RF jamming attacks (for any wireless network)
  - Spread spectrum
  - Frequency hopping
- Power exhaustion attacks (specific to WSNs)
  - Active
    - Explicitly waking up sensors.
    - Inserting bogus network traffic to be routed
    - Can be minimized with proper network design
  - Passive
    - Creating bogus sensor stimuli to cause sleep deprivation
    - Exploit application so that continuous sensor traffic is generated
    - Very difficult to protect against (another form of DOS attacks)

# Security: Imprinting



---

## The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks

Frank Stajano and Ross Anderson  
AT&T Laboratories Cambridge

---

- Traditional authorization mechanisms
  - Access control lists
  - Signed certificates
  - Not applicable to WSNs
    - Absence of an online server
    - Severe computation and storage constraints
- Secure Transient Association
  - Device is imprinted with secret key shared with owner
  - The device has policy statements for each of the permissible actions or levels of access.
  - Policy is first specified by the owner
  - Other principals can access device services only if policy allows

# Security: Talking to Strangers



---

## Talking to Strangers: Authentication in Ad-Hoc Wireless Networks

Balfanz, Smetters, Stewart, Wong  
Xerox Palo Alto Research Center

---

- Location Limited Channel
  - Demonstrative identification
  - Authenticity
  - No need for secrecy
- Pre-authentication phase
  - Exchange public keys or their digests
- Main wireless link
  - Exchange full public keys
  - Use any public-key based key exchange protocol
  - Establish secure and authenticated session

# Open Research Issues

---



- Evaluation framework for WSN
- Collaborative Information Gathering Networks
- Routing Protocols
- Transport Protocols
- Media Access Protocols
- Security Model
- Cooperating clusters or layers of WSNs
- Localization protocols
- Time synchronization protocols

# Evaluation Framework



- Current state
  - Ad-hoc design and evaluation of new protocols
  - Each paper has a different model and assumptions
  - Need for integrated view
- Introduce a **point of reference** for the **design** and **evaluation** of communication protocols in WSNs
  - Define handful of models for classification of WSNs
  - Design factors influencing development
  - Define appropriate metrics
  - Provide baseline protocols for evaluation
    - Use idealized, global knowledge, simplistic protocols
    - The “goodness” of new protocols can be quantified by measuring how much better or worse they are from the baseline protocols.

# Collaborative Information Gathering Networks

---



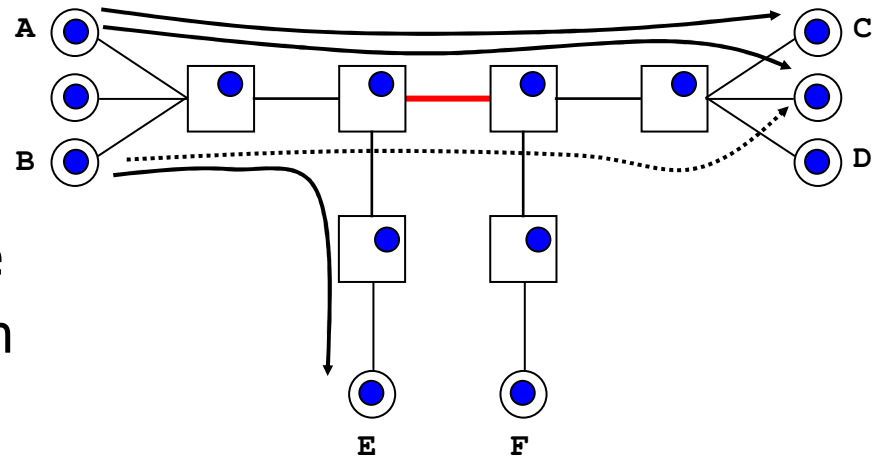
- Let us revisit the properties of WSNs
  - The Network as a whole propagates information
  - Severe constraints in energy, bandwidth, processing
  - Nodes cooperate to perform a sensing task
  - Nodes do not need to be individually addressable
  - User queries the network, the network responds
- WSN is an instantiation of Collaborative Information Gathering Networks
  - Implicit assumptions (wireless links, nature of nodes)
  - Can we derive a more general model and apply it to seemingly different problems?

# Example



## ■ Problem: Congestion Control in Packet Networks

- Extend notion of Congestion Manager
- Multiplex congestion information across multiple macroflows with cooperation from routers
- Can we view this as a sensor network?
  - Consider the process on the router as the sensor node
  - It has constraints on bandwidth, processing and storage
  - We are not interested on a specific node alone
  - The purpose of the network is to propagate information about **congestion events** in the network, so that endpoints can adjust



# Conclusions

---



- WSNs new class of wireless networks
- WSN propagates information
- Novel protocols need to be devised
- Need for evaluation framework
- Information paradigm of WSNs can be generalized and applied to different problems