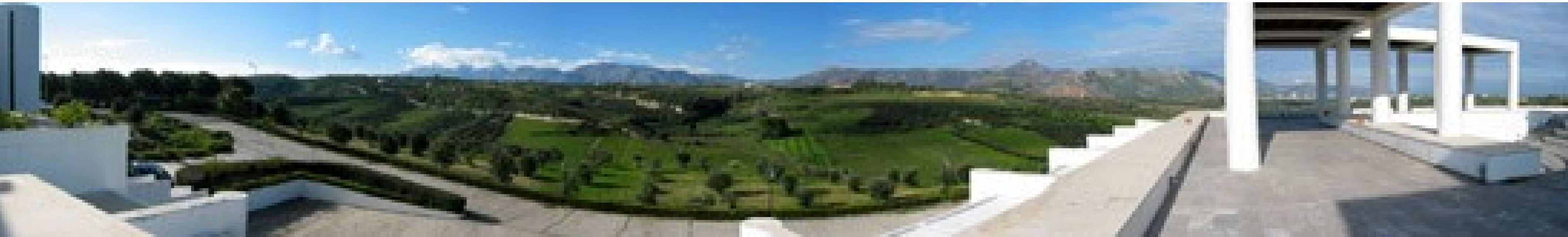
Introduction on Sensor Networks

CS 439 & 539

Prof. Maria Papadopouli
University of Crete
ICS-FORTH
http://www.ics.forth.gr/mobile



Introduction to Wireless Sensor Networks

Wireless sensor networks (WSNs)

- What is a Wireless Sensor Network ?
- What is the typical node architecture ?
- How is a network organized ?
- What are the relevant aspects of networking protocols ?
- How to design protocols for control and automation ?

Sensor

- A transducer
- Measures a physical phenomenon e.g. heat, light, motion, vibration, and sound and transmits it

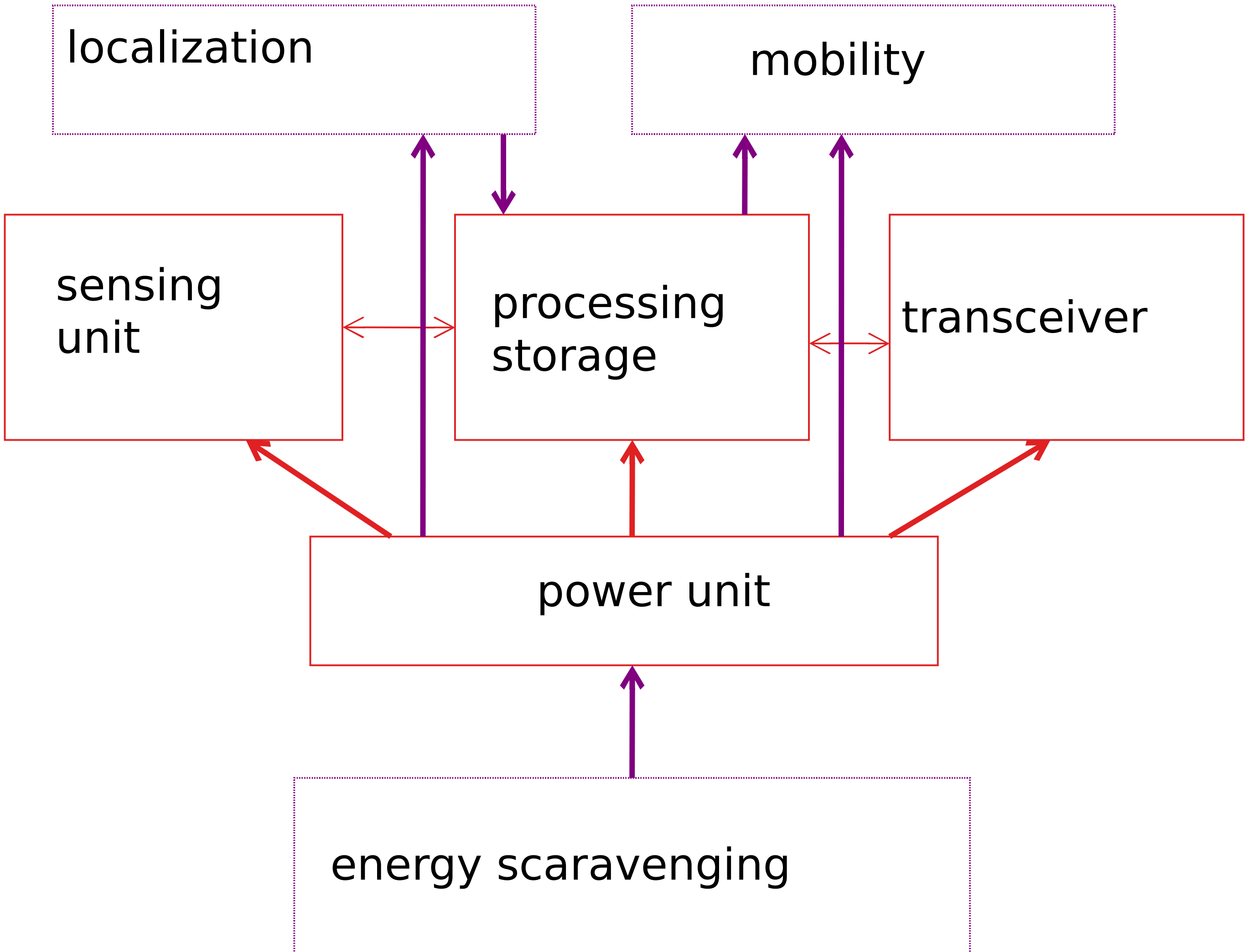
Sensor node

- Basic unit in sensor network
- Contains on-board sensors, processor, memory, transceiver, and power supply

Sensor network

- Consists of a large number of sensor nodes
- Nodes deployed either inside or close to the phenomenon/parameter being sensed

Sensor node


localization
mobility
sensing
unit
processing
storage
transceiver
power unit
energy scaravenging

Typical sensor characteristics

- Consume low power
- Autonomous
- Operate in high volumetric densities
- Adaptive to environment
- Cheap
- Limited resources & capabilities (e.g., memory, processing, battery)

- Wireless sensor and actuator networks (WNSs) make Internet of Things possible
- Computing, transmitting and receiving nodes, wirelessly networked for communication, control, sensing and actuation purposes

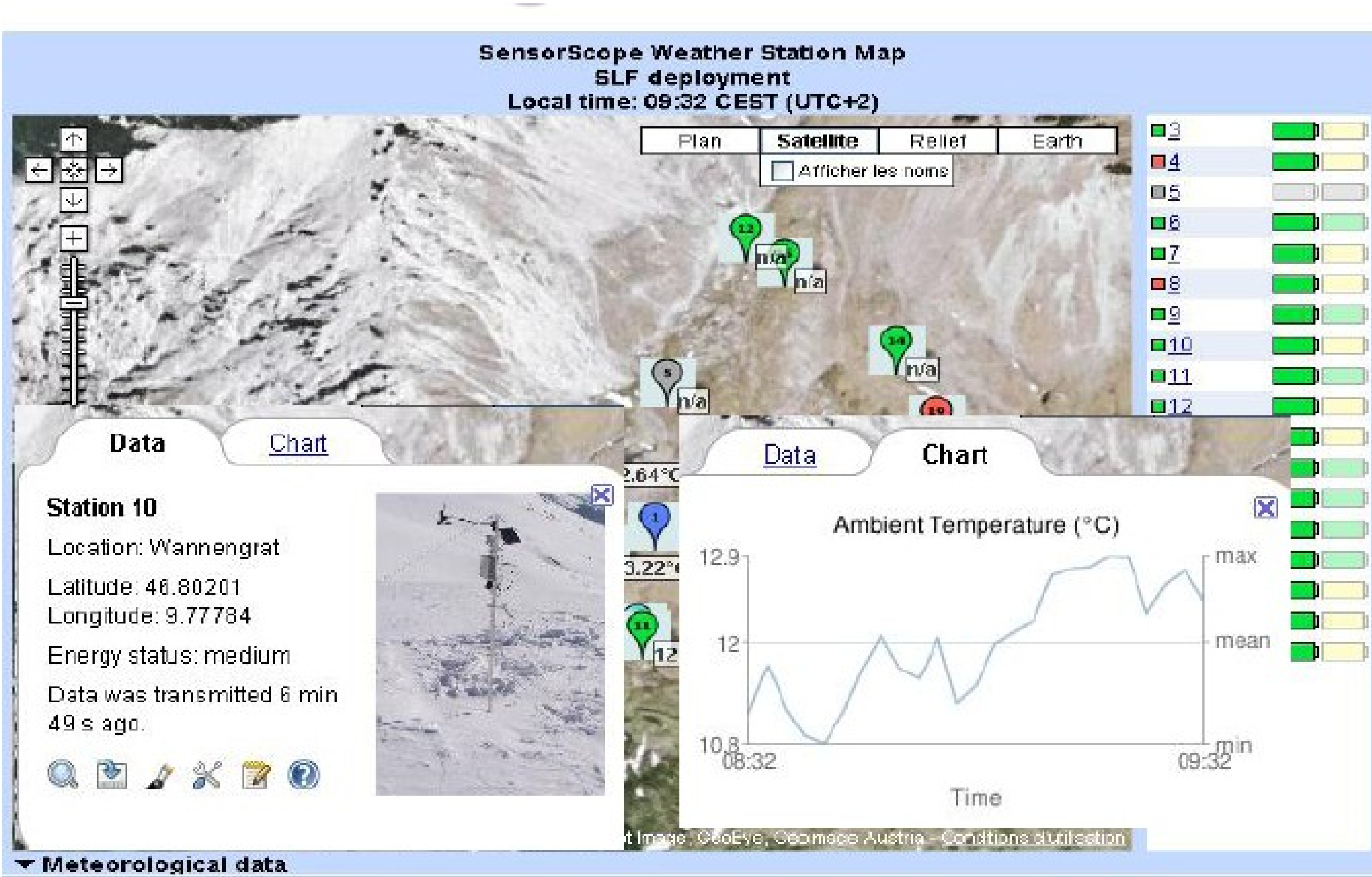
Characteristics of WNSs

- Battery-operated nodes
- Limited wireless communication
- Reduced coordination
- Mobility of nodes

Environmental Applications

- Forest fire detection
- Bio-complexity mapping of environment
- Flood detection
- Precision Agriculture
- Air and water pollution
- Surveillance & monitoring

Environmental Monitoring



Source: Joao Da Silva's talk at Enisa, July 20th, 2008

Goals

- Understanding better the overall behavior of migratory Wrynecks (endangered species) and therefore actively intervene for improving his survivability
- Monitoring nest passages, hunting movements, environmental cues (e.g., temperature inside and outside the nest)
- No networking

App#3:Ecosystem Monitoring

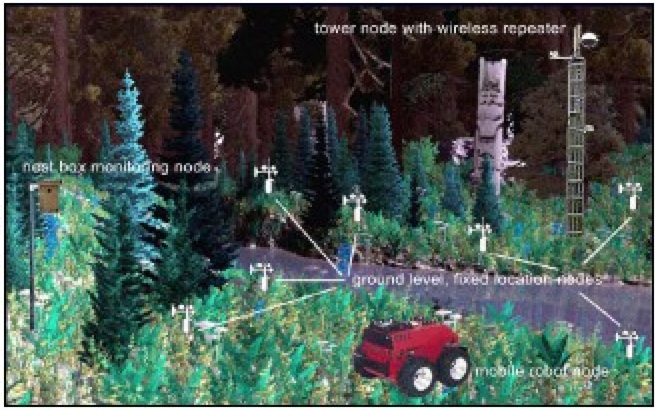
SWIS

Science

- Understand response of wild populations (plants and animals) to habitats over time.
- Develop in situ observation of species and ecosystem dynamics.

Techniques

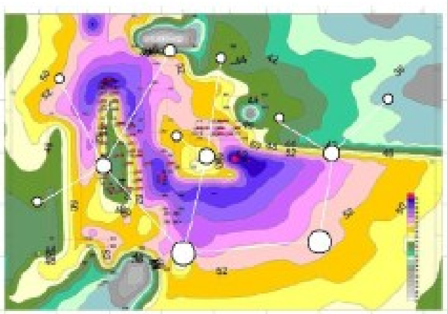
- **Data acquisition of physical and chemical properties, at various spatial and temporal scales, appropriate to the ecosystem, species and habitat.**
- Automatic identification of organisms (current techniques involve close-range human observation).
- Measurements over long period of time, taken *in-situ*.
- Harsh environments with extremes in temperature, moisture, obstructions, ...



Source: D. Estrin, UCLA

Monitoring the Terroir [ESA]

- MACRO: satellite
- MICRO: WSN



Noise Pollution
[ETHZ]

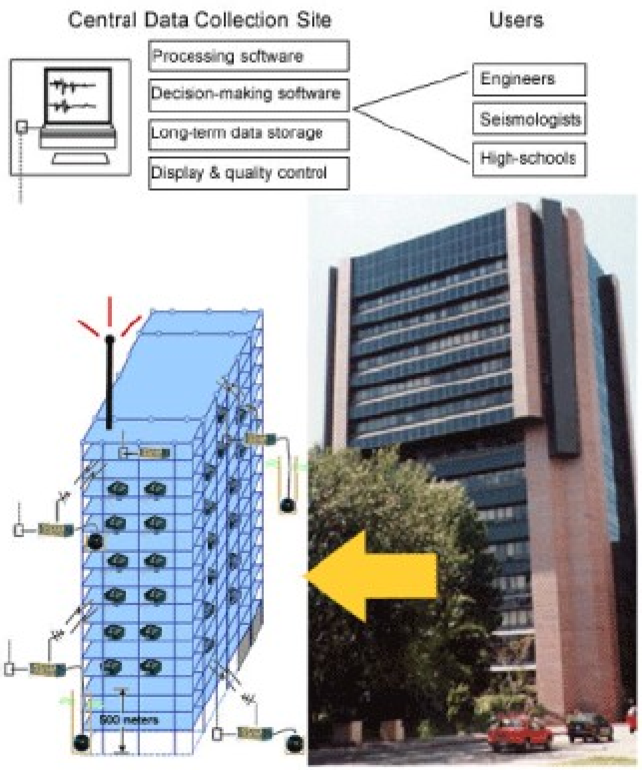
Monitoring the archeological site at DIS
[Soprintendenza Archeologica di Roma
Barrano, Leoni]

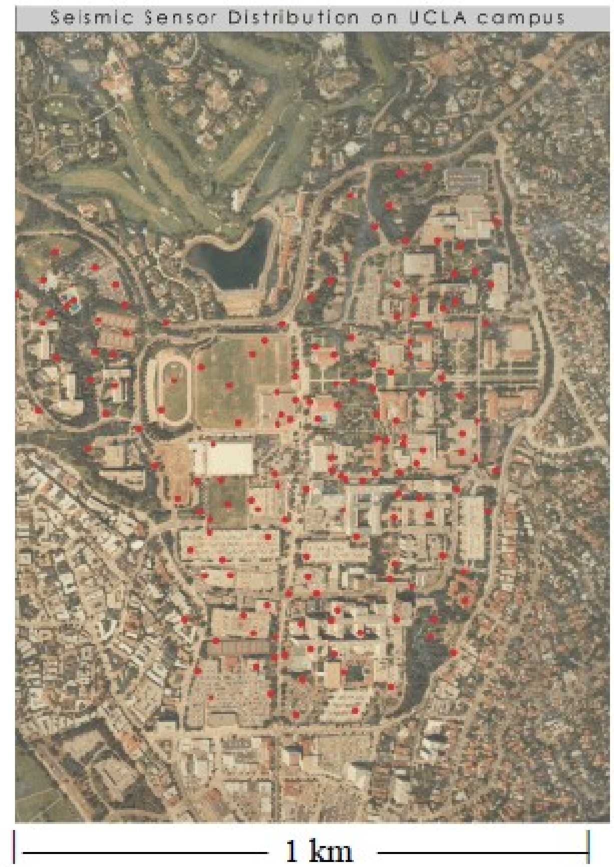
App#1: Seismic

- Interaction between ground motions and structure/foundation response not well understood.
  - **Current seismic networks not spatially dense enough** to monitor structure deformation in response to ground motion, to sample wavefield without spatial aliasing.
- Science
  - Understand response of buildings and underlying soil to ground shaking
  - Develop models to predict structure response for earthquake scenarios.
- Technology/Applications
  - Identification of seismic events that cause significant structure shaking.
  - Local, at-node processing of waveforms.
  - Dense structure monitoring systems.
- ENS will provide field data at sufficient densities to develop predictive models of structure, foundation, soil response.

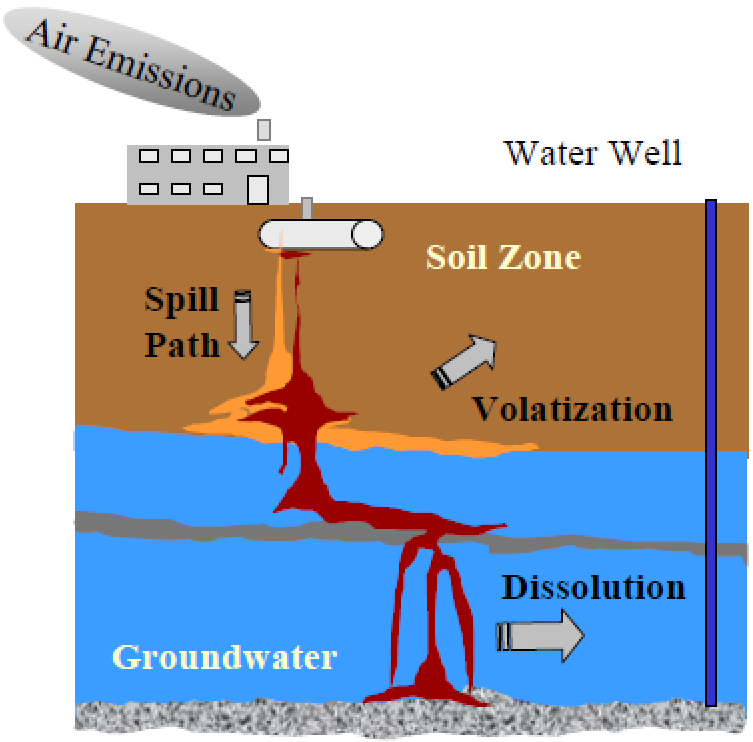
Source: D. Estrin, UCLA

- 38 strong-motion seismometers in 17-story steel-frame Factor Building.
- 100 free-field seismometers in UCLA campus ground at 100-m spacing



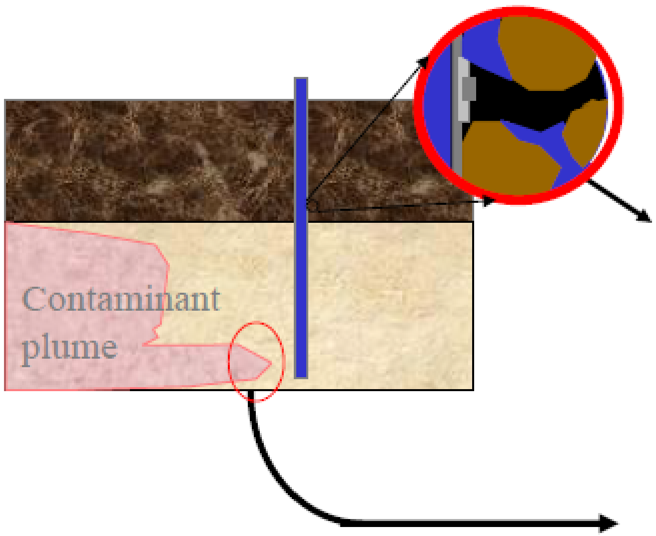


Source: D. Estrin, UCLA



Source: D. Estrin, UCLA

- Science
  - Understand intermedia contaminant transport and fate in real systems.
  - Identify risky situations before they become exposures. Subterranean deployment.
- Multiple modalities (e.g., pH, redox conditions, etc.)
- Micro sizes for some applications (e.g., pesticide transport in plant roots).
- Tracking contaminant "fronts".
- At-node interpretation of potential for risk (in field deployment).



- Environmental Micro-Sensors
  - Sensors capable of recognizing phases in air/water/soil mixtures.
  - Sensors that withstand physically and chemically harsh conditions.
  - Microsensors.
- Signal Processing
  - Nodes capable of real-time analysis of signals.
  - **Collaborative signal processing to expend energy only where there is risk.**

Source: D. Estrin, UCLA

Military Applications

- Monitoring friendly forces, equipment, and ammunition
- Battlefield surveillance
- Reconnaissance of opposing forces and terrain
- Targeting
- Battle damage assessment
- Nuclear, biological, and chemical attack detection

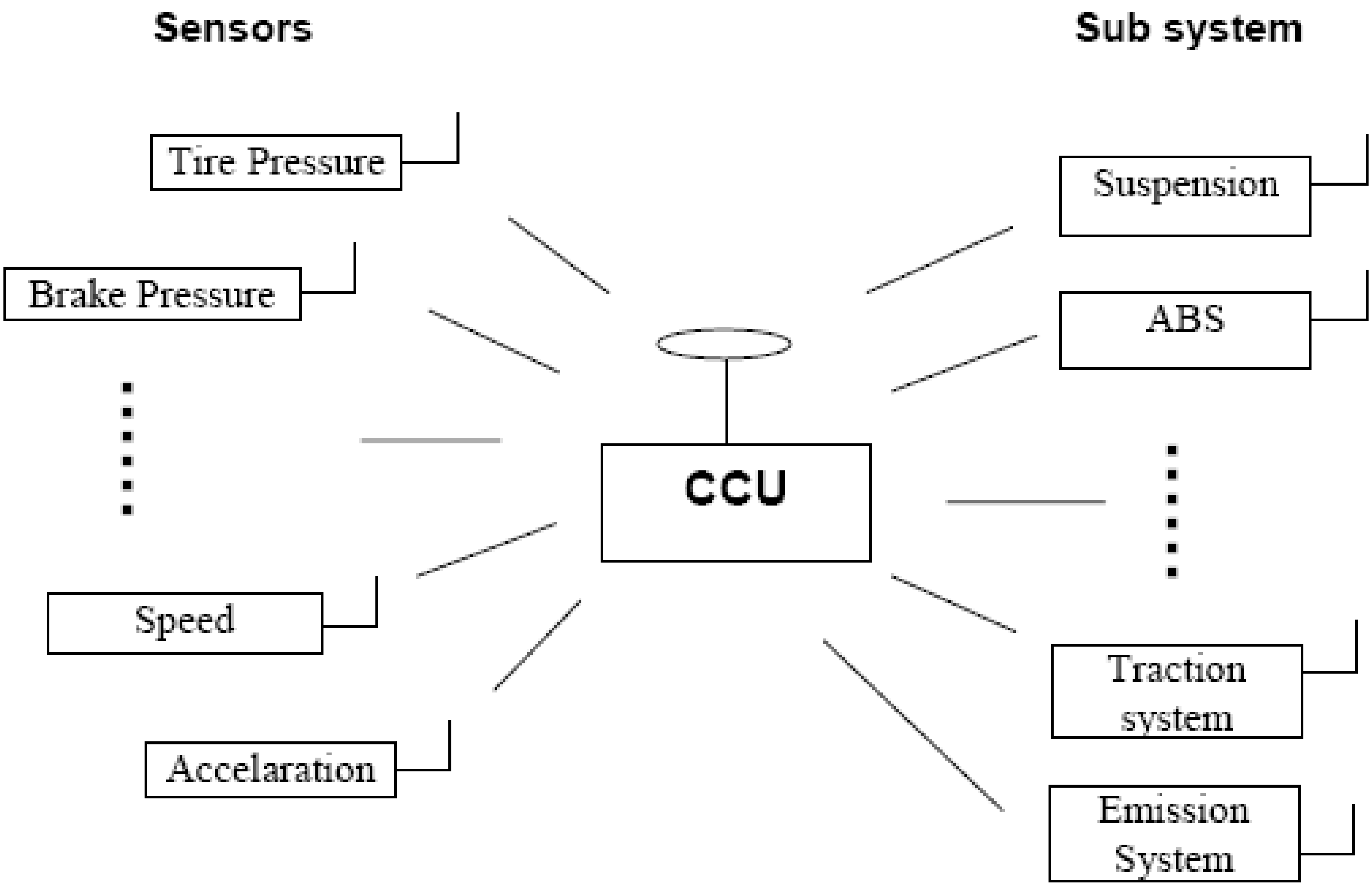
Health Applications

- Telemonitoring of human physiological data
- Tracking and monitoring doctors and patients inside a hospital
- Drug administration in hospitals

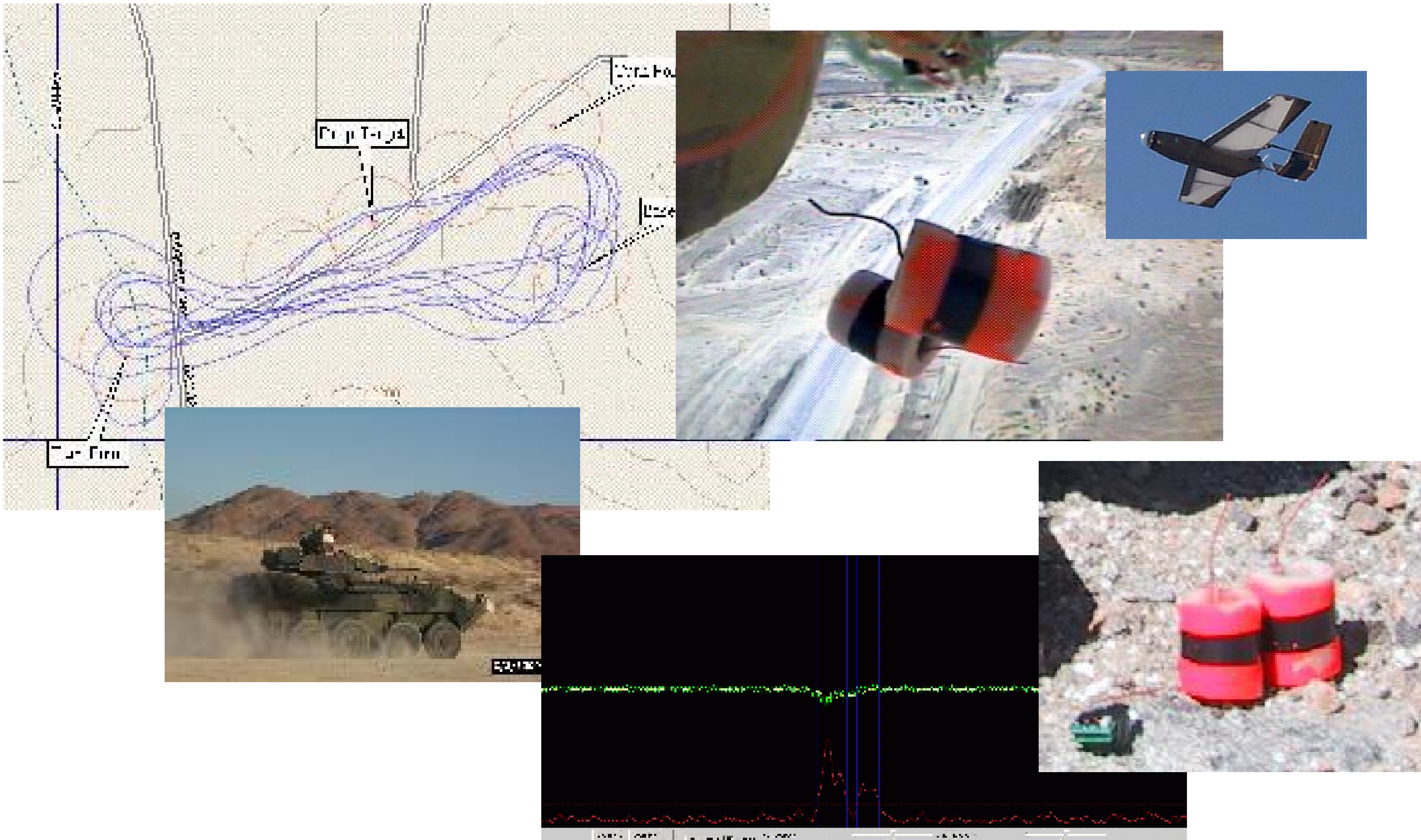
Automotive Applications

- Reduces wiring effects
- Measurements in chambers and rotating parts
- Remote technical inspections
- Conditions monitoring e.g. at a bearing

Automotive Application

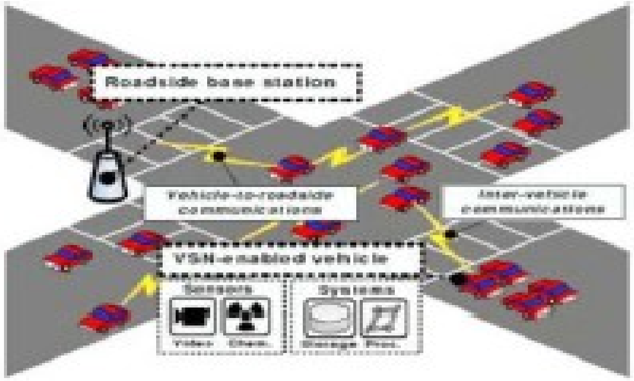


Vehicle Tracking

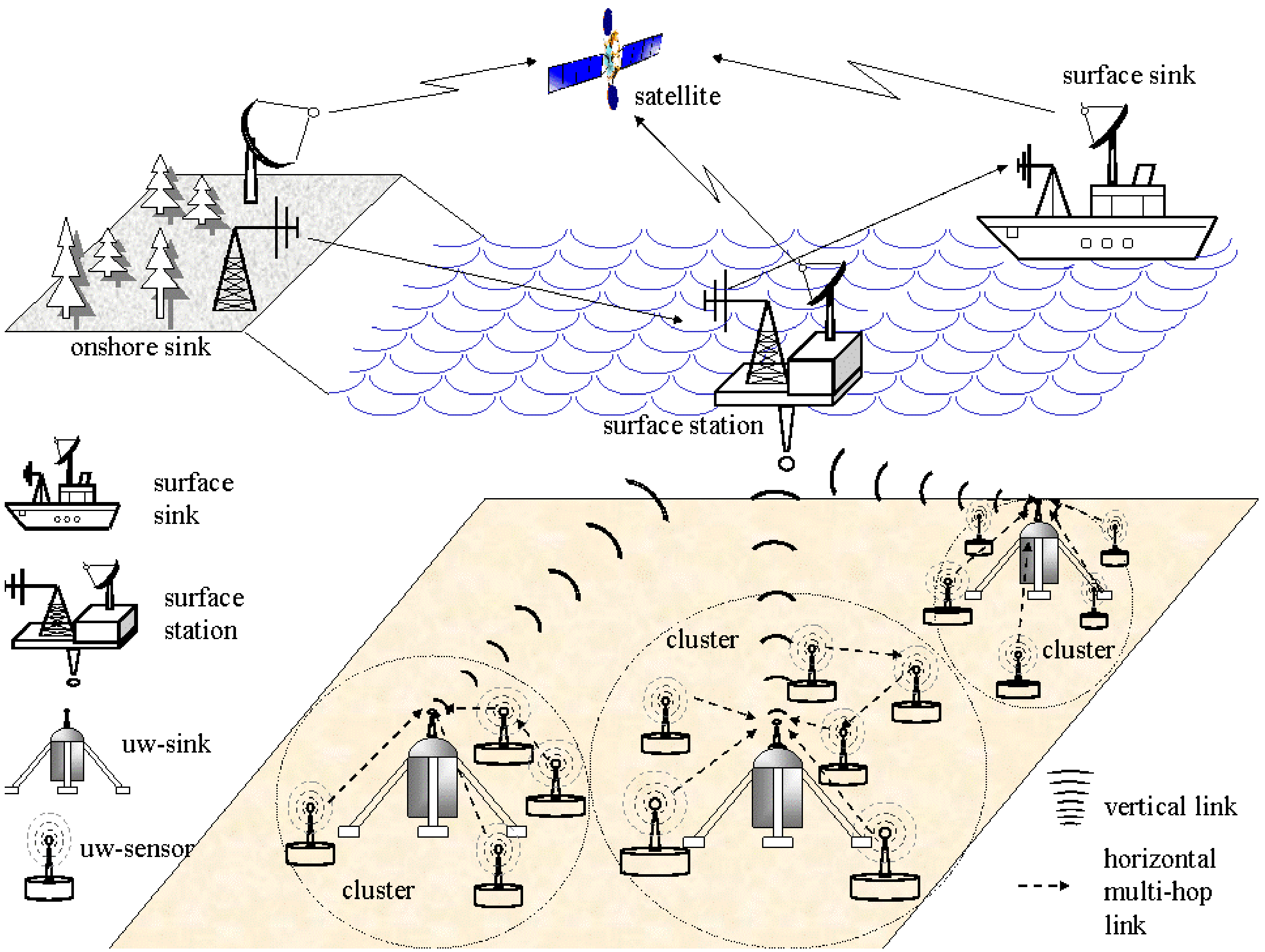


ess Sensor Networks in Intelligent Transportation System

The wirelless systems are everywhere even in the places that we never thought,one of the its uses is to traffic lights and signs.

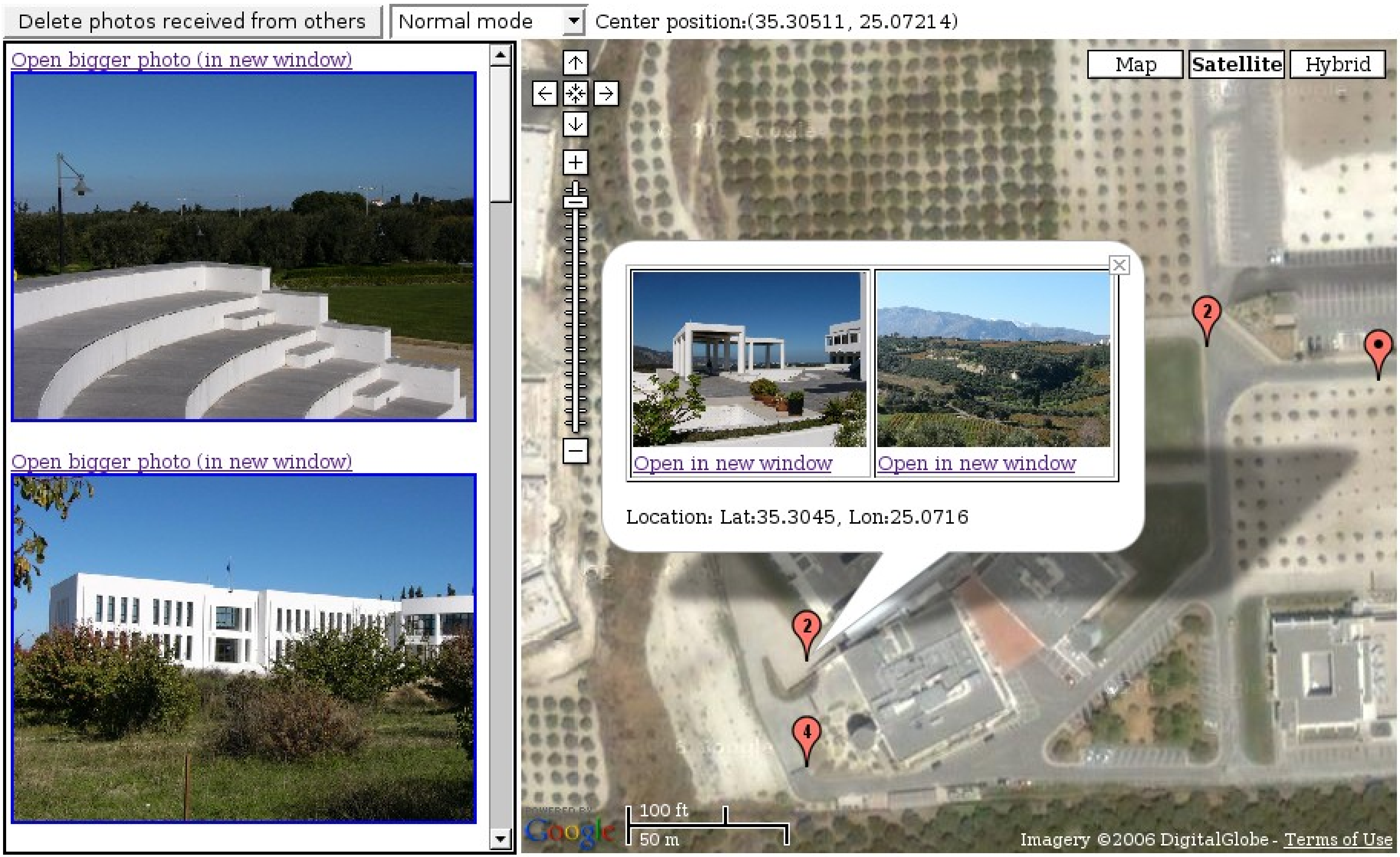


Underwater Acoustic Sensor Networks

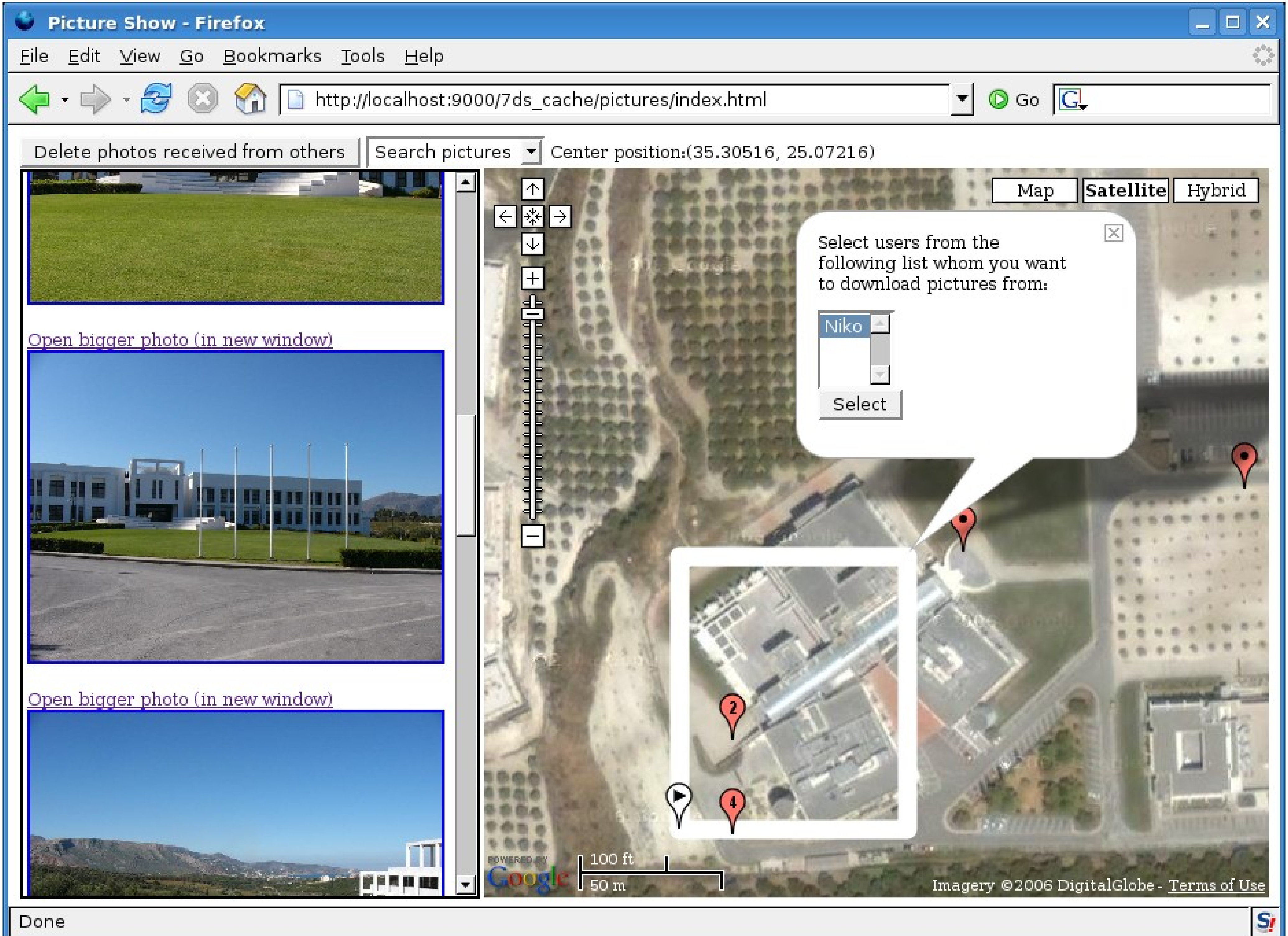


Other Commercial Applications

- Environmental control in office buildings (estimated energy savings $55 billion per year!)
- Interactive museums
- Detecting and monitoring car thefts
- Managing inventory control
- Vehicle tracking and detection



Delete photos received from others
Normal mode
Center position:(35.30511, 25.07214)
Open bigger photo (in new window)
Open bigger photo (in new window)
Map
Satellite
Hybrid
Open in new window
Open in new window
Location: Lat:35.3045, Lon:25.0716
2
2
4
100 ft
50 m
Imagery ©2006 DigitalGlobe - Terms of Use


Picture Show - Firefox
File Edit View Go Bookmarks Tools Help
http://localhost:9000/7ds_cache/pictures/index.html
Go
Delete photos received from others
Search pictures
Center position:(35.30516, 25.07216)
Open bigger photo (in new window)
Open bigger photo (in new window)
Map
Satellite
Hybrid
Select users from the following list whom you want to download pictures from:
Niko
Select
2
4
100 ft
50 m
POWERED BY Google
Imagery ©2006 DigitalGlobe - Terms of Use
Done

Tagged products

Source: Joao Da Silva’s talk at Enisa, July 20th, 2008

Factors Influencing WSN Design

- Fault tolerance
- Scalability
- Production costs
- Hardware constraints
- Sensor network topology
- Environment
- Transmission media
- Power Consumption
  - Sensing
  - Communication
  - Data processing
- Clock skew
- Radio turn-on time

Key Software Requirements

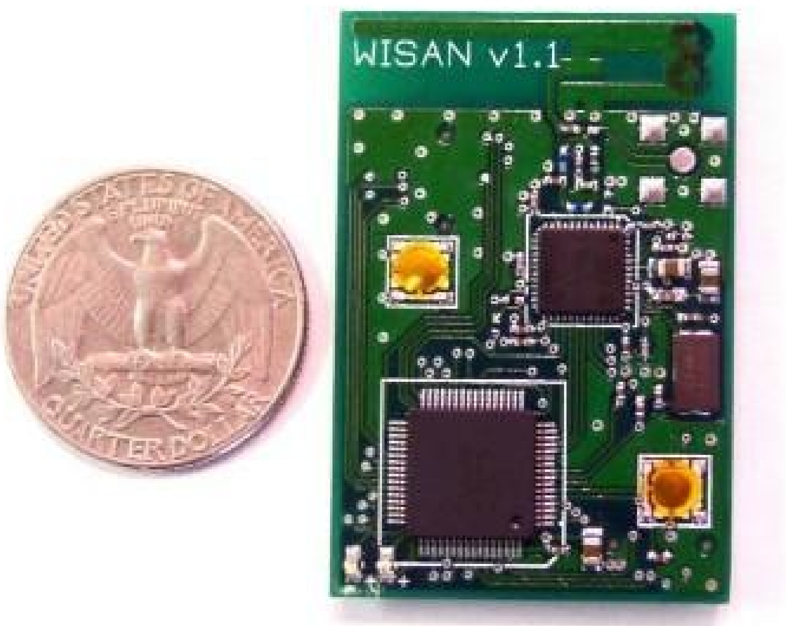
- Capable of fine grained concurrency
- Small physical size
- Efficient Resource Utilization
- Highly Modular
- Self Configuring

WSN Requirements for Habitat/Ecophysiology Applications

- Diverse sensor sizes (1-10 cm), spatial sampling intervals (1 cm - 100 m), and temporal sampling intervals (1 ms - days), depending on habitats and organisms.
- Naive approach → Too many sensors →Too many data.
  - In-network, distributed information processing
- Wireless communication due to climate, terrain, thick vegetation.
- Adaptive Self-Organization to achieve reliable, long-lived, operation in dynamic, resource-limited, harsh environment.
- Mobility for deploying scarce resources (e.g., high resolution sensors).

Source: D. Estrin, UCLA

Worldsens Inc. Sensor Node



Crossbow Sensor Node

xample of sensor: camera

Camera networks:

- Cameras provide rich information
- Have wider and longer sensing range

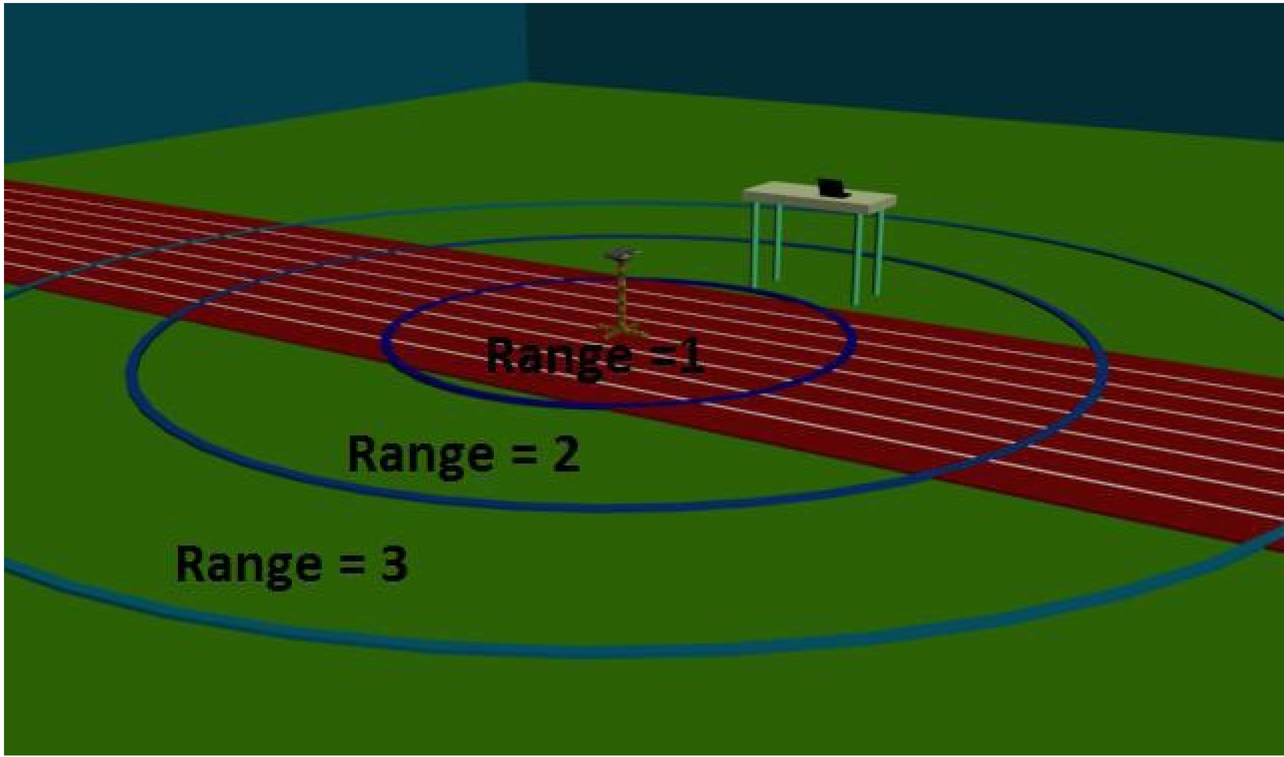
But

- Consume more power
- Increased memory/storage requirements

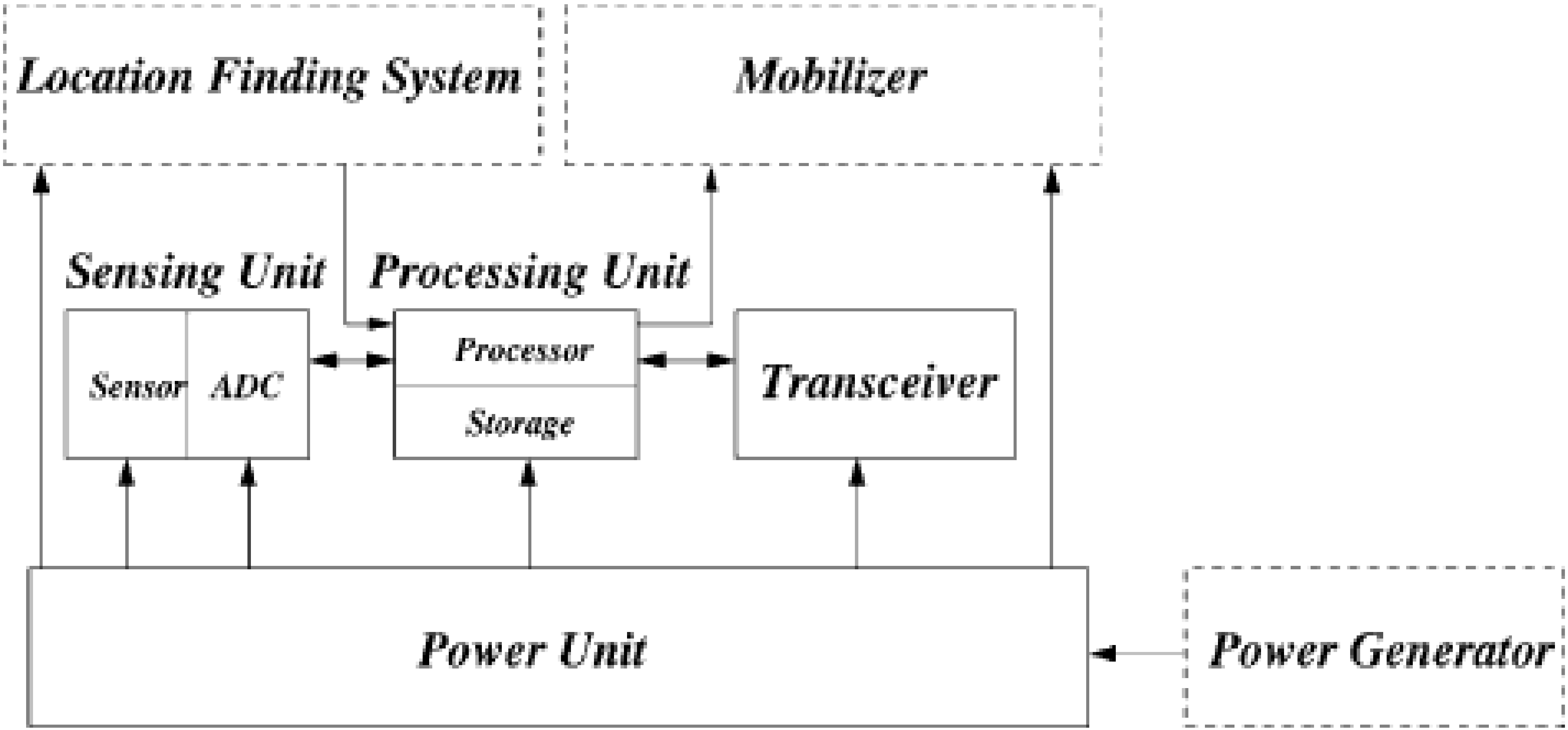
mple of sensors: RF reader & RFID tag

at the size of a modem with 2 Omni-directional Antennas on it.
The M200 reader provides an RS-232 port and an Ethernet RJ-45 port to communicate with a PC.

- Managing inventory control
- Vehicle tracking and detection



Sensor node components

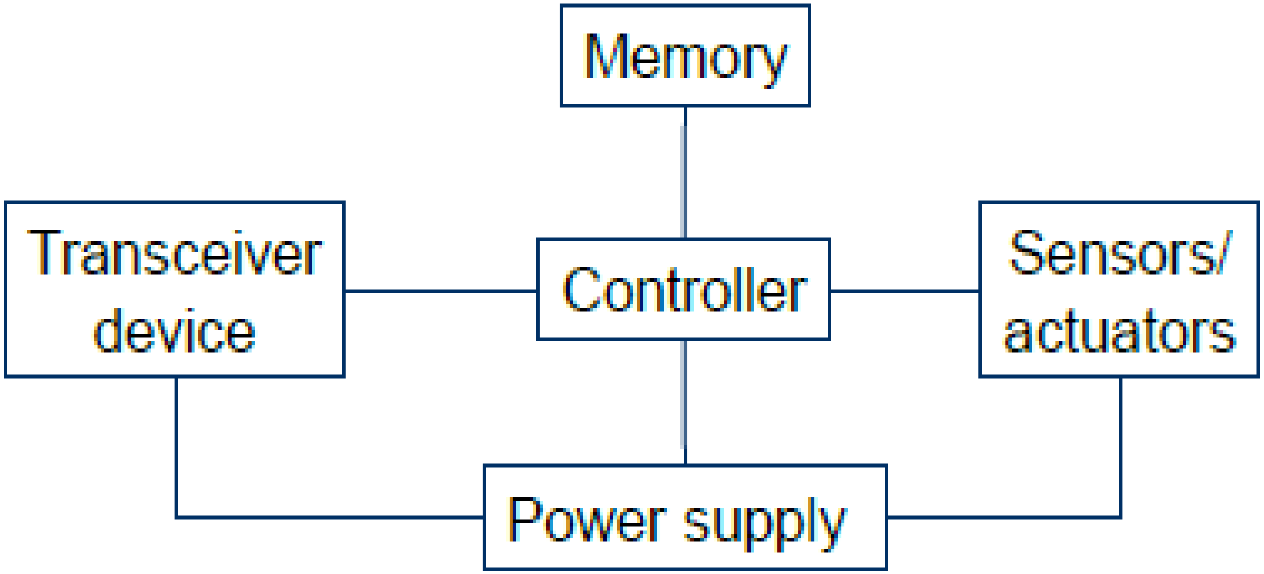


Sensor Node Components

- Sensing Unit
- Processing Unit
- Transceiver Unit
- Power Unit
- Location Finding System (optional)
- Power Generator (optional)
- Mobilizer (optional)

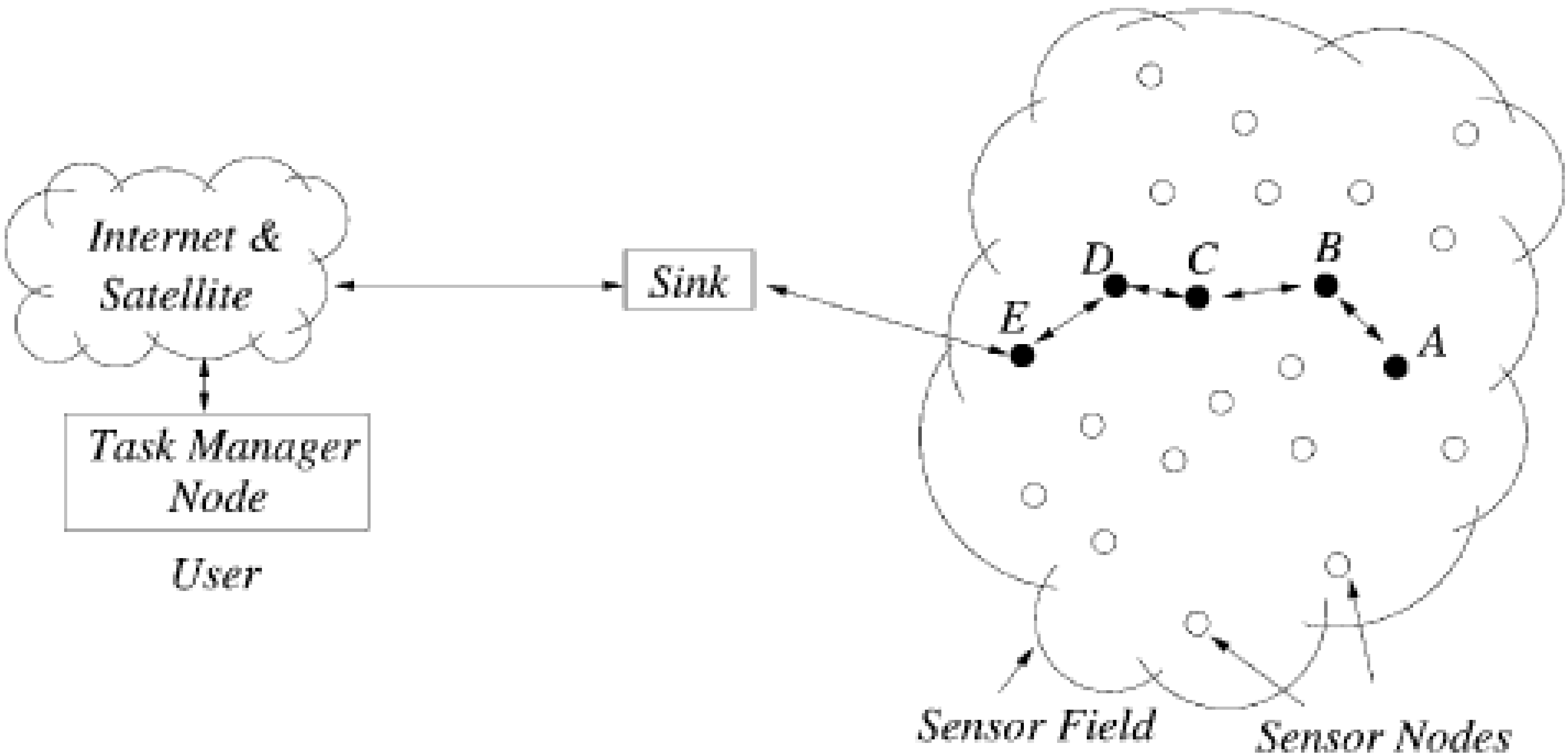
Sensor Node Requirements

- Low power
- Support multi-hop wireless communication
- Self-configuring
- Small physical size
- Reprogrammable over network
- Meets research goals
  - Operating system exploration
  - Enables exploration of algorithm space
  - Instrumentation

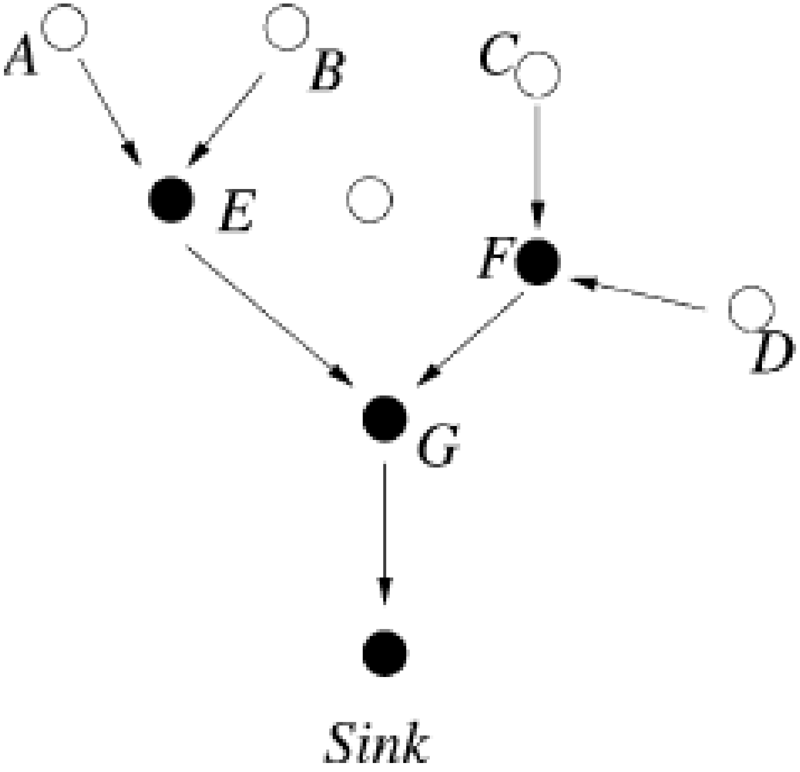


Memory
Transceiver device
Controller
Sensors/ actuators
Power supply

WSN Communication Architecture



Data measured at different sensor nodes measuring the same parameter/attribute are aggregated

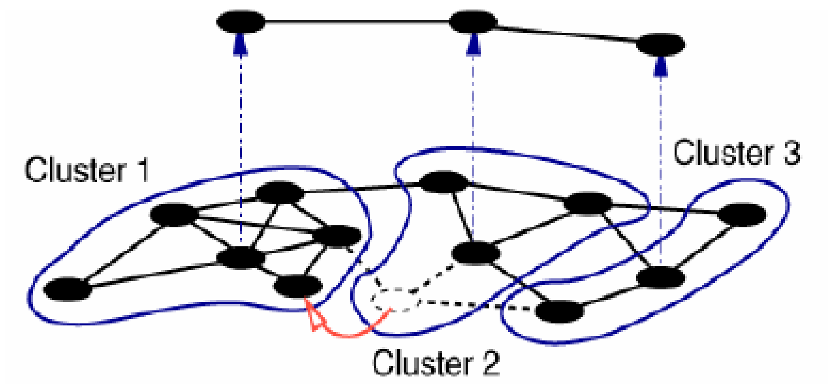


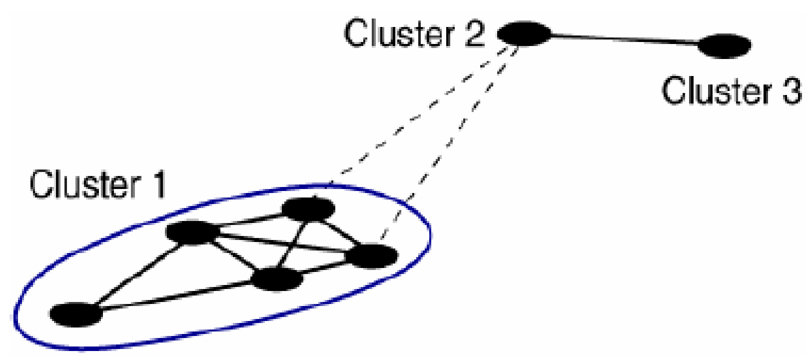
Data aggregation architectures

- Cluster heads collect and process data, then they transmit the data to a gateway/server/controller
- Gateway collects all data or samples and performs the aggregation, then they send the data to server/controller
- Gossiping algorithms or routing algorithms across the WSN
- Specific node(s) route data to the gateway

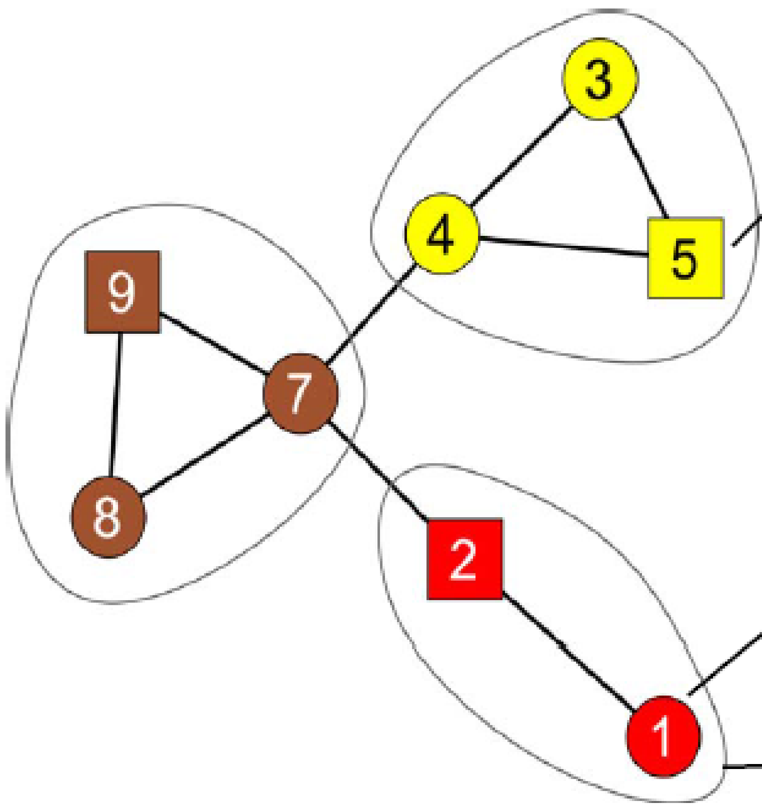
Clustering

- Creates hierarchy
- Useful for:
  - Hierarchical routing
  - Address assignment
  - Radio resource allocation
- In ad hoc networks:
  - Distributed algorithm
  - Online algorithms
  - Adaptive to mobility





Makes dynamic networks look less dynamic.



Clusterhead <weight>

- Has largest weight in its neighborhood
- Two clusterheads can not be neighbors

Ordinary node <weight>

- Joins the neighboring clusterhead with the largest weight.

Cluster

- two hop size

What is a „good" clustering algorithm?

- Load on clusterheads (traffic and processing): bottlenecks?
- Message complexity: Number of messages after a change in the topology until a valid cluster structure is re-achieved.
- Convergence time complexity: Number of time steps after a change in the topology until a valid cluster structure is re-achieved.

- Routing table size and routing optimality (hierarchy)
- Decision speed (required neighbor knowledge)
- Level of adaptability (which parameters are adaptive?)
- Asynchronous operation
- Cluster stability

Sensor Network Algorithms

- Directed Diffusion – Data centric routing (Estrin, UCLA)
- Sensor Network Query Processing (Madden, UCB)
- Distributed Data Aggregation
- Localization in sensor networks (UCLA, UW, USC, UCB)
- Multi-object tracking/Pursuer Evader (UCB, NEST)
- Security

Controller

- Microcontroller-general purpose processor, optimized for embedded applications, low power consumption
- DSPs-optimized for signal processing tasks, not suitable for WSNs
- FPGAs-may be good for testing
- ASICs-only when peak performance is needed 7,no flexibility
- Example microcontrollers
  - Exas Instuments MSP430
    - 16-bit RISC core,up to 4MHz,versions with 2-10 kbytes RAM, several DACs, RT clock, prices start at 0,49$
    - Fully operational 1.2 mW
    - Deepest sleep mode 0.3µW-only woken up by external interrupts
- Atmel ATMega
  - 8-bit controller, larger memory than MSP430,slower
  - Operational mode:15mW active,6 mW idle
  - Sleep mode :75µW

WSN Operating Systems

- TinyOS
- Contiki
- MANTIS
- BTnut
- SOS
- Nano-RK

Από τεχνολογικής πλευράς το κυριότερο πρότυπο που χρησιμοποιείται σήμερα είναι το IEEE 802.15.4.
Το μεγαλύτερο πλεονέκτημά του είναι ότι προσφέρει ικανοποιητική ποιότητα υπηρεσίας με την χαμηλότερη δυνατή κατανάλωση ενέργειας.
Πάνω σε αυτό έχει στηριχθεί το πρωτόκολλο Zigbee το οποίο χρησιμοποιείται κατά κόρον από τα Δίκτυα Αισθητήρων σήμερα.

Τα τελευταία χρόνια όμως έχουν κάνει την εμφάνισή τους και λειτουργικά συστήματα για αισθητήρες ανοιχτού κώδικα, με κυριότερα τα TinyOS και Contiki.
Επειδή ακριβώς είναι ανοιχτού κώδικα λογισμικά, έχουν αρχίσει να χρησιμοποιούνται κατά κόρον για ερευνητικούς σκοπούς, με αποτέλεσμα ολοένα και περισσότεροι κατασκευαστές αισθητήρων να τα υποστηρίζουν στα προϊόντα τους.

Cooja & Contiki

Advantages:

- Open source
- Low learning curve
- Full IP networking
- Power awareness
- Support for IPv6, RPL, threads, Cooja network simulator
- Support a variety of hardware platforms (Tsky, MicaZ, Avr-raven, Z1)

Disadvantages:

- Lack of detailed documentation
- Performance scalability issues when the number of motes is large

Cooja & Contiki

Advantages:

Open source

Low learning curve

Allows direct code loading from Cooja to real motes- > deployment time minimization Support for:

- Different type of radio propagation models
- IEEE 802.15.4, ContikiMAC
- IPv4, IPv6, 6LoWPAN
- RPL, AODV
- TCP/UDP/ICMP
- different types of motes (Z1, Tsky, TelosB, etc)

Disadvantages:

Lack of detailed documentation

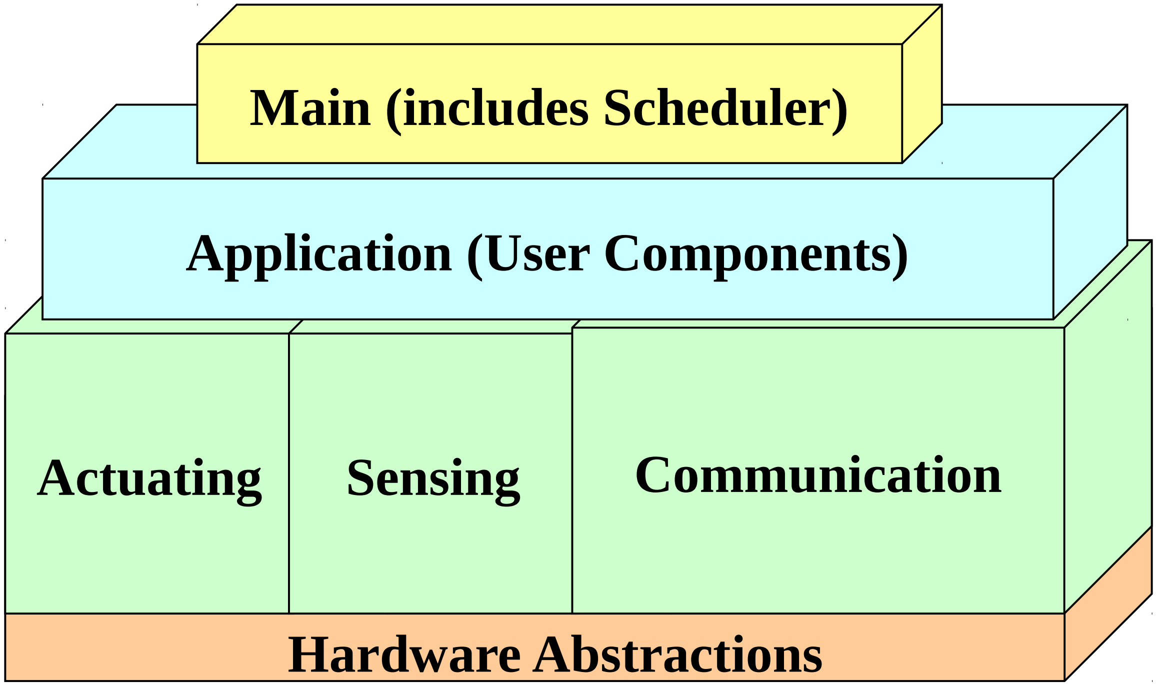
Performance scalability issues when the number of motes is large

TinyOS

- OS/Runtime model designed to manage the high levels of concurrency required
- Gives up IP, sockets, threads
- Uses state-machine based programming concepts to allow for fine grained concurrency
- Provides the primitive of low-level message delivery and dispatching as building block for all distributed algorithms

TinyOS

- Event-driven programming model instead of multithreading
- TinyOS and its programs written in nesC



TinyOS Characteristics

Small memory footprint

- non-premptable FIFO task scheduling

Power Efficient

- Puts microcontroller to sleep
- Puts radio to sleep

Concurrency-Intensive Operations

- Event-driven architecture
- Efficient Interrupts and event handling

No Real-time guarantees

Tiny OS Concepts

Scheduler + Graph of Components

- constrained two-level scheduling model: threads + events

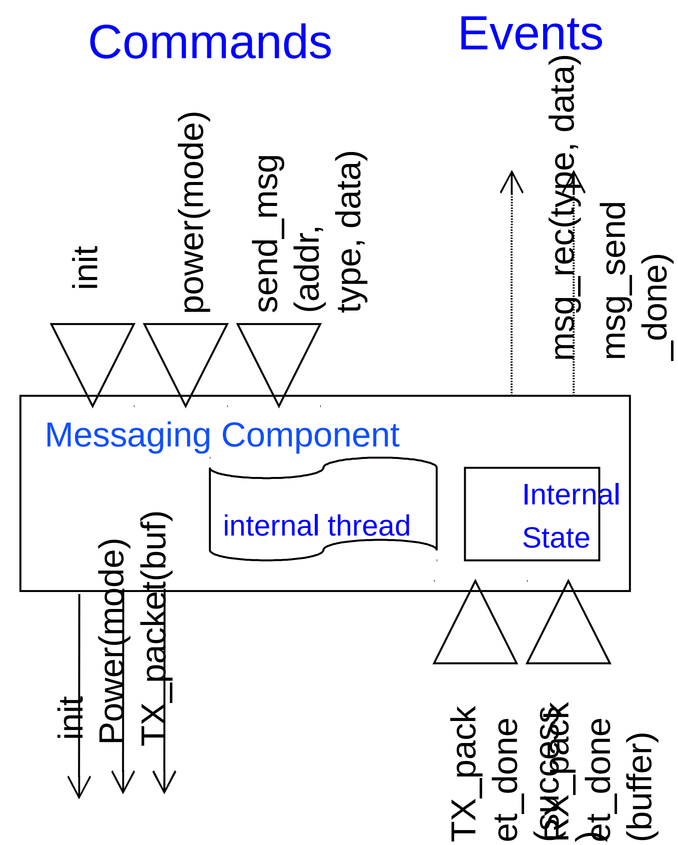
Component:

- Commands,
- Event Handlers
- Frame (storage)
- Tasks (concurrency)

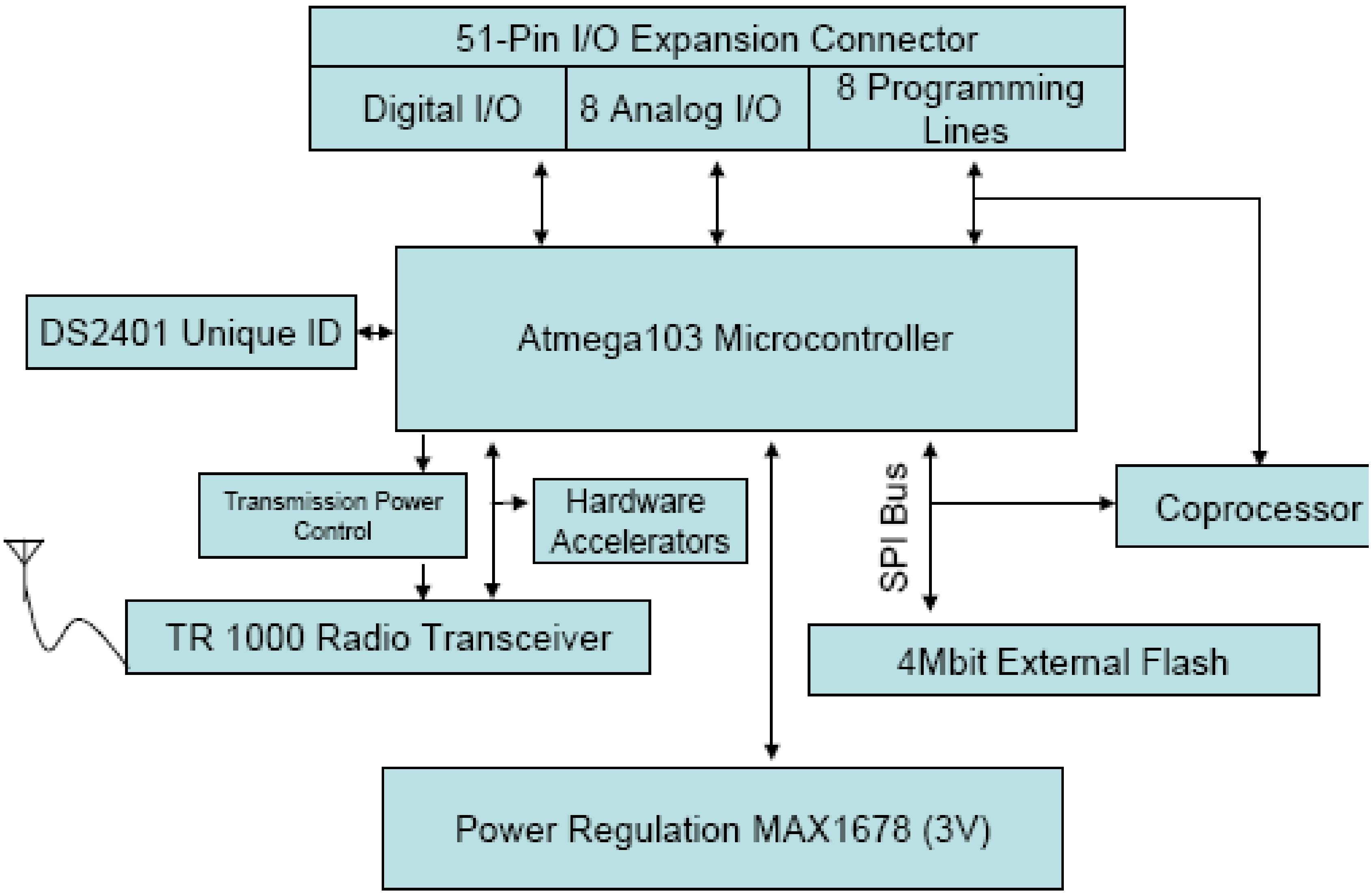
Constrained Storage Model

- frame per component, shared stack, no heap

Very lean multithreading



MICA Sensor Mote



WSN Development Platforms

- Crossbow
- Dust Networks
- Sensoria Corporation
- Ember Corporation
- Worldsens

WSN Simulators

- NS-2
- GloMoSim
- OPNET
- SensorSim
- J-Sim
- OMNeT++
- Sidh
- SENS

Conclusion

- WSNs possible today due to technological advancement in various domains
- Envisioned to become an essential part of our lives
- Design Constraints need to be satisfied for realization of sensor networks
- Tremendous research efforts being made in different layers of WSNs protocol stack

References

- Dr. Chenyang Lu Slides on “Berkeley Motes and TinyOS”, Washington University in St. Louis, USA
- J. Hill and D. Culler, “A Wireless Embedded Sensor Architecture for System-Level Optimization”, Technical Report, U.C. Berkeley, 2001.
- X. Su, B.S. Prabhu, and R. Gadh, “RFID based General Wireless Sensor Interface”, Technical Report, UCLA, 2003.

Examples of radio transceivers

RFM TR1000 family

- 916 or 868 Mhz
- 400kHz bandwidth
- Up to 115,2 kbps
- On/off keying or ASK
- Dynamically tunable output power
- Maximum power about 1.4 mW
- Low power consumption

Chipcon CC1000

- Range 300 to1000 Mhz, programmable in 250 Hz steps
- PSK modulation
- Provides RSSi

Chipcon CC2400

- Implements 802.15.4
- 2.4 Ghz DSSS modem
- 250kbps
- Higher power consumption than above transceivers

Infineon TDA 525x family

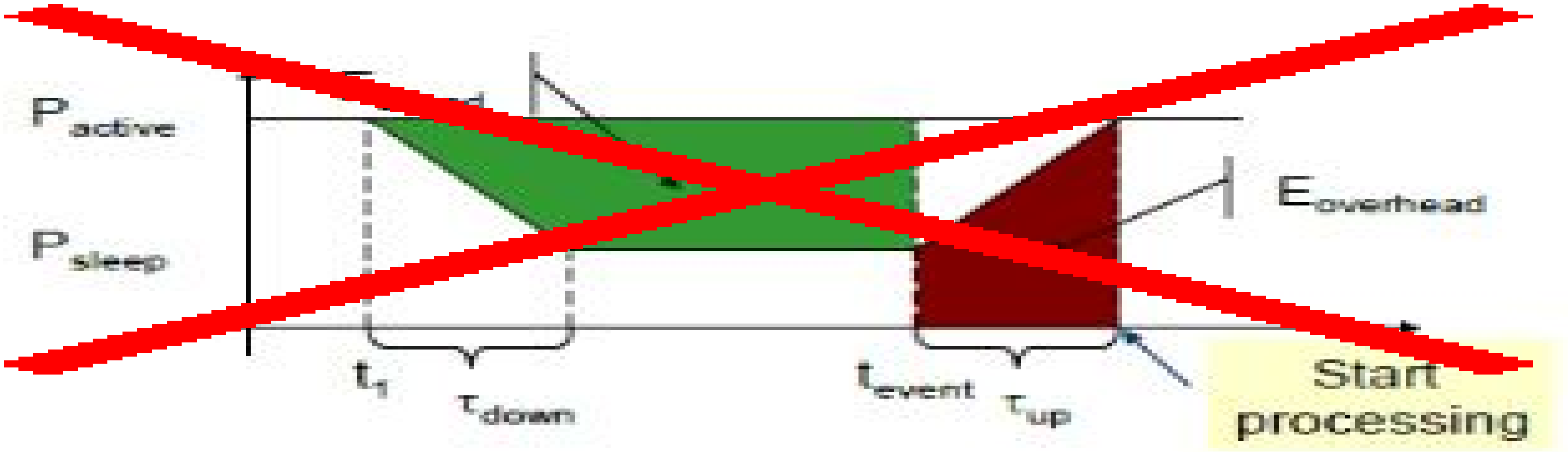
- E.g., 5250:868MHz
- ASK or FSK modulation
- RSSS, highly efficient power amplifier
- Intelligent power down,'' self-polling'' mechanism
- Excellent blocking performance

How to recharge a battery?

Try to scavenger energy from environment

Ambient energy sources

- Light, solar cells-between 10 $\mu W/cm^2$ and 15mW/cm^2
- Temperature gradinets - 80 $\mu W/cm^2$
- Vibrations – between 0.1 and 10000 $\mu W/cm^3$
- Pressure varation (piezo-electric), e.g., 330 $\mu W/cm^2$ from the heel of a shoe
- Air/linquid flow(MEMS gas turbines)



Do not run node at full operation all the time

- If nothing to do, switch to **power safe mode**
- Question: When to throttle down? How to wake up again?

Typically models

- Controller: Active, idle, sleep
- Radio mode: Turn on/off transmitter/reciever, both

IEEE 802.15.4 is the de-facto reference standard for low data rate and low power WNSs

Characteristics:

- **Low data rate** for ad hoc self-organizing network of inexpensive fixed, portable and moving devices
- High network flexibility
- **Very low power consumption**
- **Low cost**

IEEE 802.15.4 specifies two layers:

- Physical layer
- 2.4GHz global, 250Kbps
- 915MHz America,40Kbps
- 868MHz Europe,20Kbps
- Medium Acces Control (MAC) layer

IEEE 802.15.5 *does not specify the routing*

IEEE 802.15.4 Physical Layer

Frequency bands:

- 2.4-2.4835 Ghz,global,16 channels,250 Kbps
- 902.0-928.0MHz,America,10 channels,40 Kbps
- 868-868.6 Mhz,Europe,1 channel,20 Kbps

Features of PHY layer

- Activation and deactivation of the radio transceiver
- Energy detection(ED)
- Link quality indication(LQI)
- Clear channel assessment (CCA)
- Transmitting and receiving packet across the wireless channel
- Dynamic channel selection by a scanning a list of

IEEE 802.15.4 standard

Properties	2450 MHz	915 MHz	868 MHz
Bit rate	250 kbps	40 kbps	20 kbps
Number of channels	16	10	1
Modulation	O-QPSK	BPSK	BPSK
Pseudo noise chip sequence	32	15	15
Bits per symbol	4	4	1
Symbol period	16 μs	24 μs	49 μs
Latency	>15 ms	>15 ms	>15 ms
Transmission range	10-20 m	10-20 m	10-20 m

IEEE 802.15.4 standard

Supports two **network topologies**:

- **Star**: a node takes the role of the coordinator and all other nodes send traffic through it (like the role of an AP in IEEE 802.11)
- **peer-to-peer**: a multi-hop network is formed

Supports two **medium access modes**:

- **non-beacon-enabled mode:** nodes contend through a CSMA/CA mechanism, and
- **beacon-enabled mode:** a **PAN coordinator** activates a superframe through a beacon.

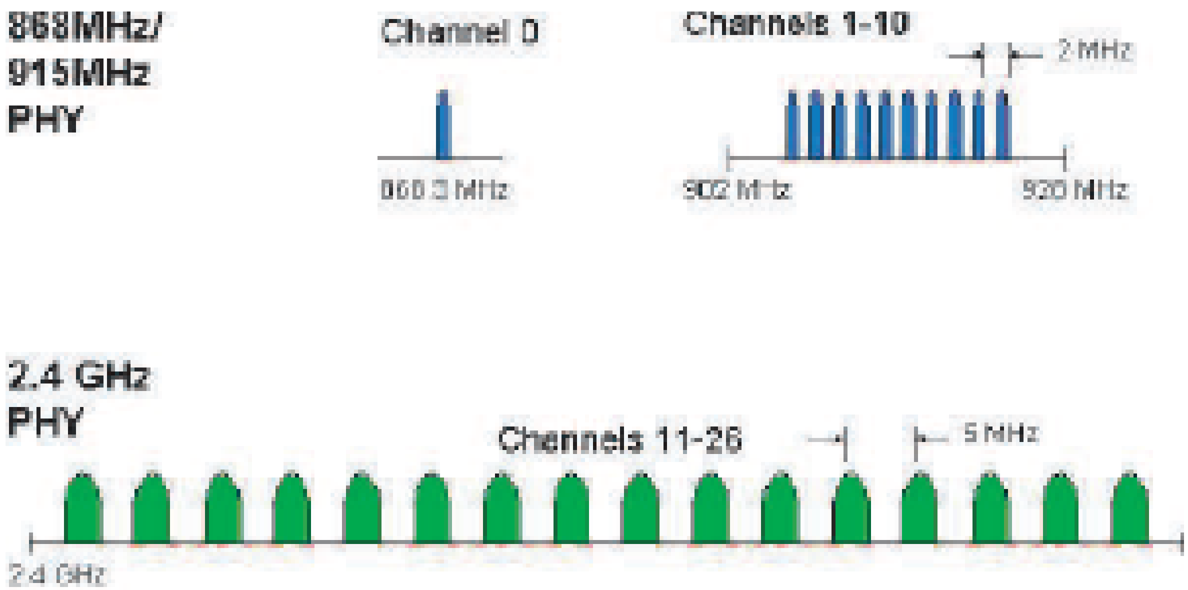
This superframe has an active and an inactive period, with a total duration of BI (beacon interval). BI and the active period of the superframe are determined by two parameters, BO and SO, respectively. IEEE 802.15.4 does not specify the optimum values for BO and SO

Zigbee

A low-cost, low-power, wireless mesh network standard based on IEEE 802.15.4

four main components: network layer, application layer, *ZigBee device objects* (ZDOs) and manufacturer-defined application objects which allow for customization and favor total integration

its specification is free for use for non-commercial purposes

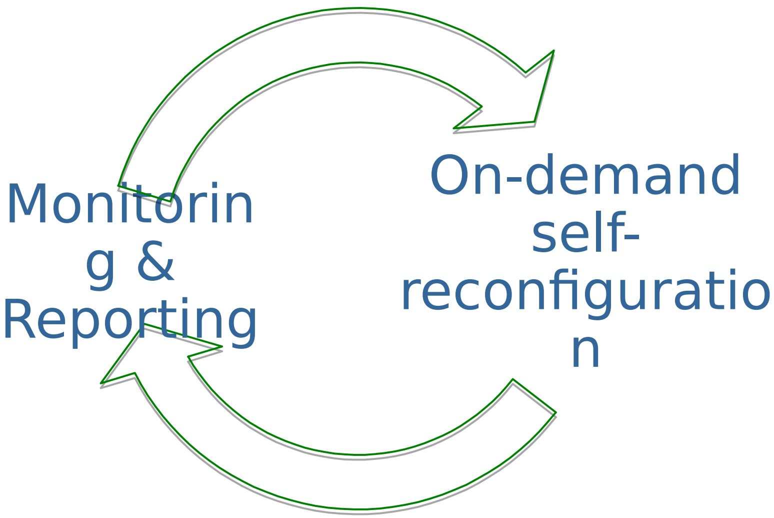


PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
868/915 (optional)	868–868.6	400	ASK	250	12.5	20-bit PSSS
	902–928	1600	ASK	250	50	5-bit PSSS
868/915 (optional)	868–868.6	400	O-QPSK	100	25	16-ary Orthogonal
	902–928	1000	O-QPSK	250	62.5	16-ary Orthogonal
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

Self-organized communications for WBN

WBN Evaluation Framework

- Impact of the environment on the network performance
- Impact of co-existing & co-operating clusters of WBN



Communication-specific parameters (e.g. operational channel, transmission power)

Additionally can be used for:

- Realization of the benchmark scenarios
- Evaluation of selected protocol stacks and the resutling on-node and cooperative network performance (e.g. lifetime, goodput, latency etc).
- Ease the structural design of end-to-end communication between WBN nodes and visualization and control system & the on-the-fly nodes reprogramming

Self-organized communications for WBN

Design and Development of WBN Evaluation Framework

Simulation-based framework

Small-scale experimental testbed

Contiki /Cooja simulation-based

- Flexibility in terms of network scalability
- Allows rapid code development on embedded devices

IEEE 802.15.4 / 2.4GHz –based

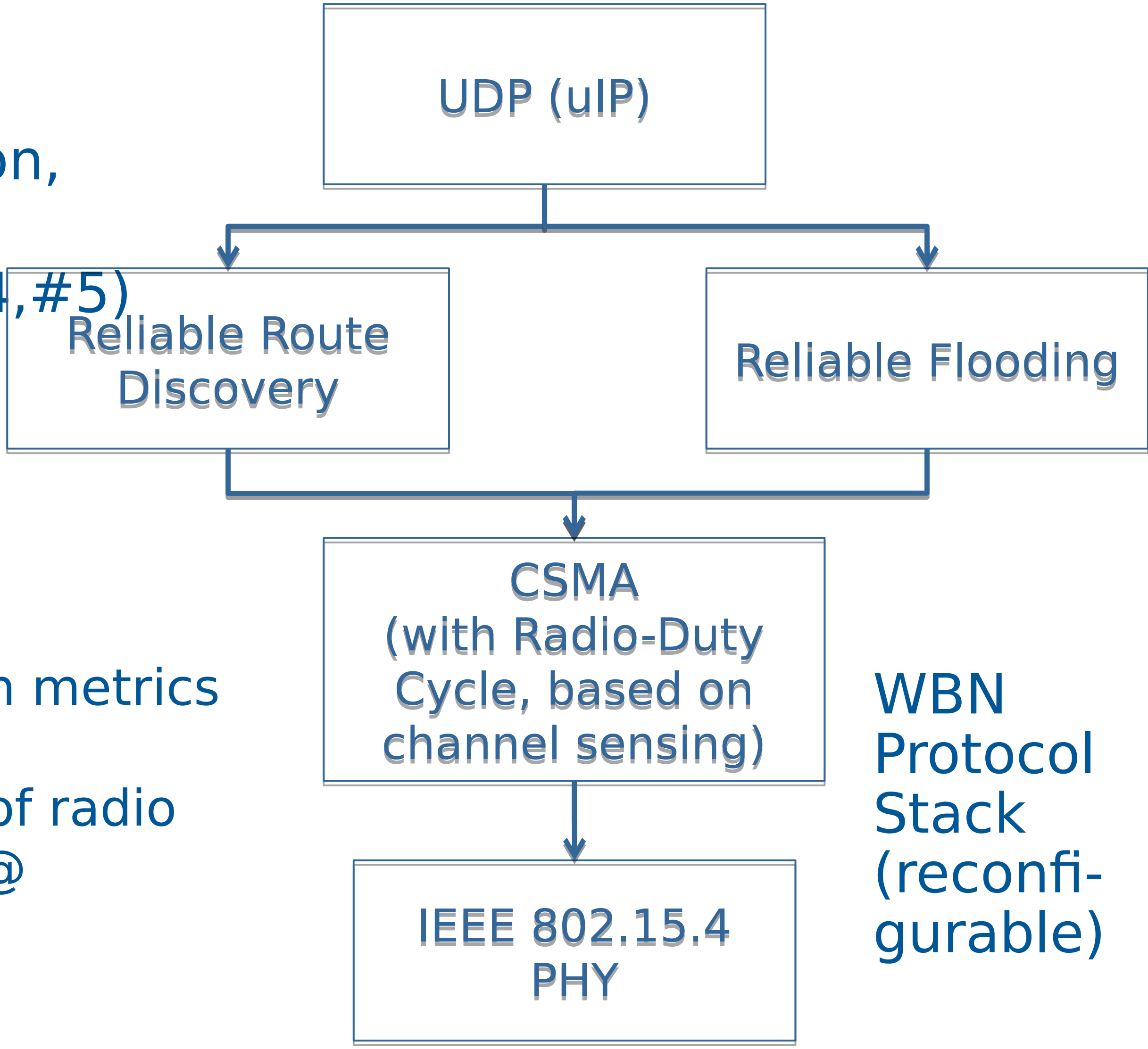
- Complementary to simulation-based
- Tier-1 & tier-2 of network architecture
- In 100% hardware compatibility to MKFF's testbed

WP4. Self-organized communications for WBN

Simulation-based WBN Evaluation Framework

- Multiple sources-1 sink architecture
- Event-driven communication, initiated from WBN nodes

(compatible to Scenario#1,#4,#5)



Currently looking into:

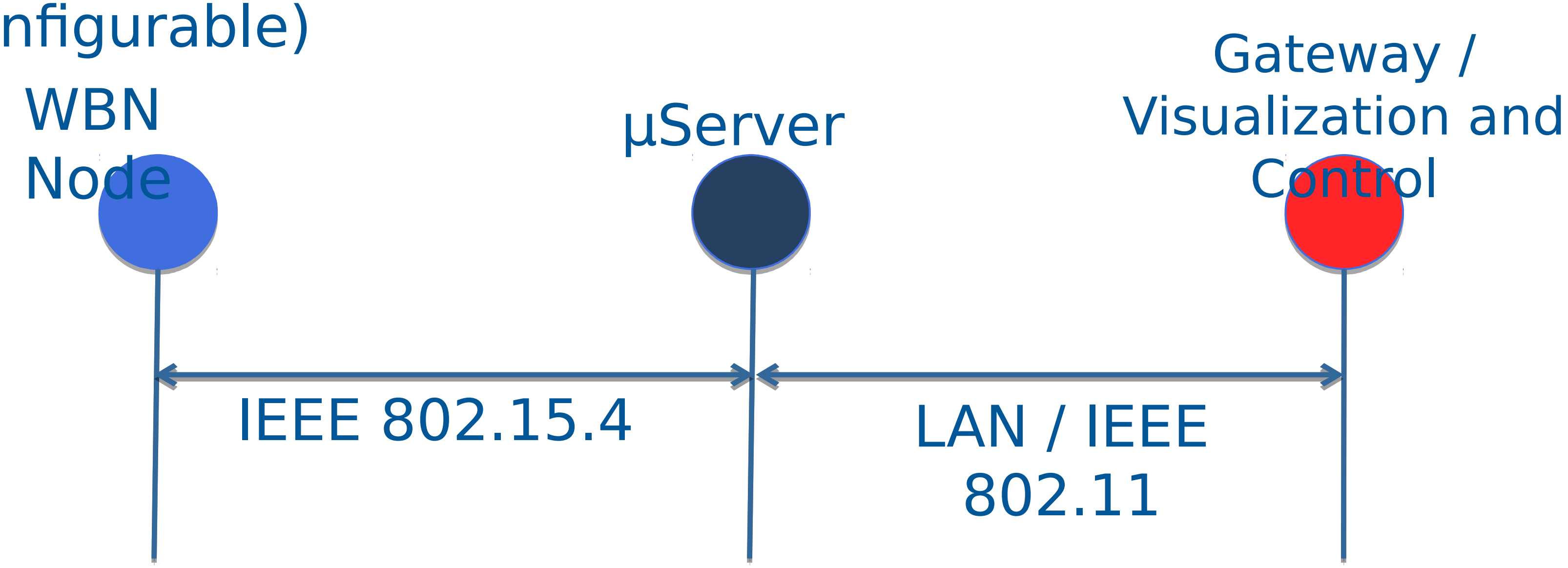
- Implementation of evaluation metrics per layer
- On-demand reconfiguration of radio propagation characteristics @ Contiki / Cooja.

WBN Protocol Stack (reconfi-gurable)

WP4. Self-organized communications for WBN

Experimental-based WBN Evaluation Framework

- 2 WBN clusters / 6 nodes per cluster
- Identical WBN protocol stack as simulation-based testbed (& reconfigurable)



+ performance of PHY / Antenna w.r.t industrial environment

+ Application Level Gateway, between WBN and Gateway
+ Increased computational efficacy

WP4. Self-organized communications for WBN

Experimental-based WBN Evaluation Framework

WBN Nodes

Product Name	Extras	Notes:
XM1000	Indoors RF range: ~30 m (without Line-of-Sight).	Not advisable for industrial environments due to antenna. SMA connector / Dipole antenna **is not supported**.
[redacted]		
CM5000-SMA	Similar as XM1000, less powerful. 5dBi dipole antenna	Advisable for industrial environments, due to antenna option. **Network compatible to XM1000**

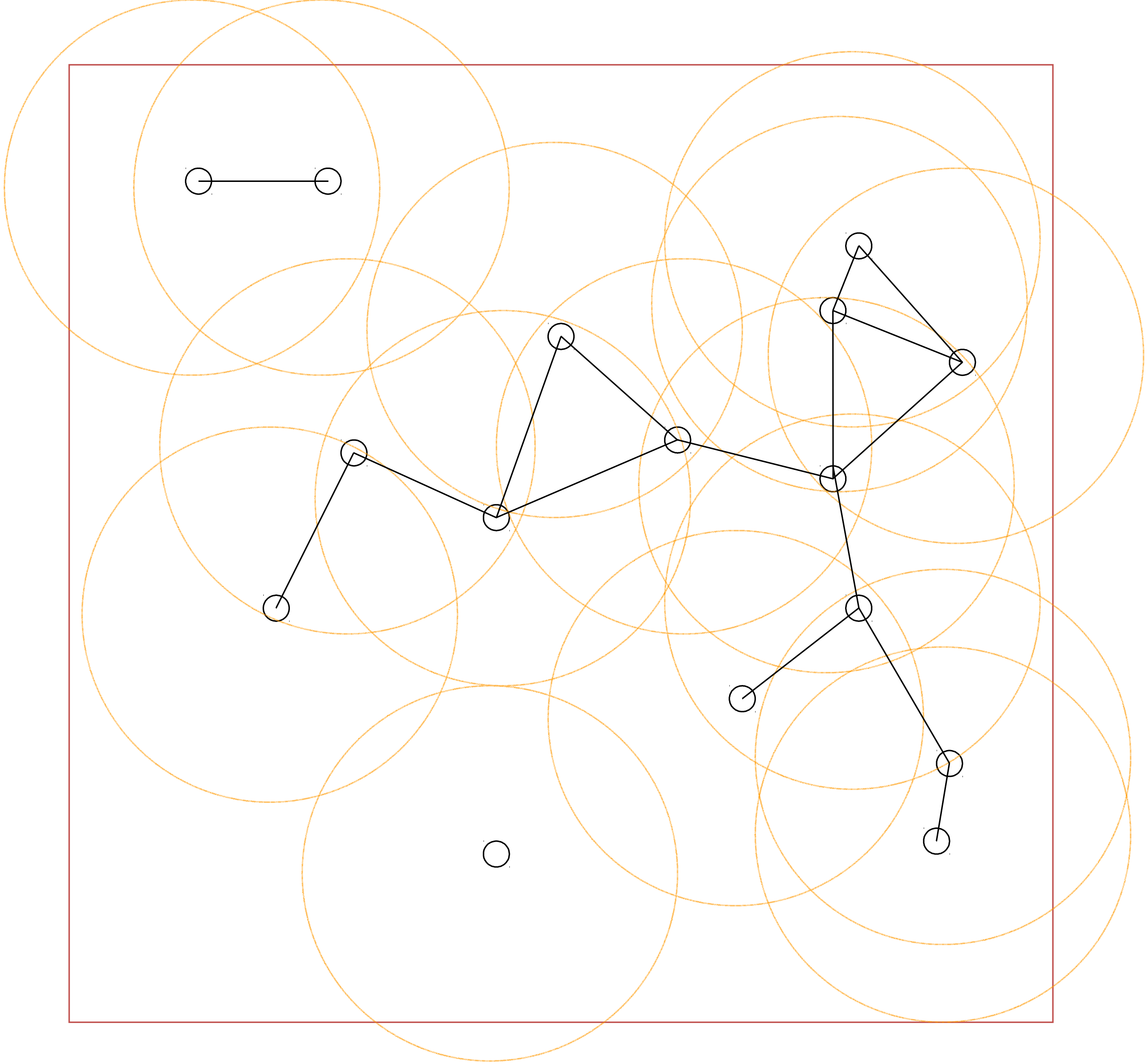
XM1000 carrying the advanced sensing functionalities – CM5000 sensing + relay nodes between XM1000 and µServer

WP4. Self-organized communications for WBN

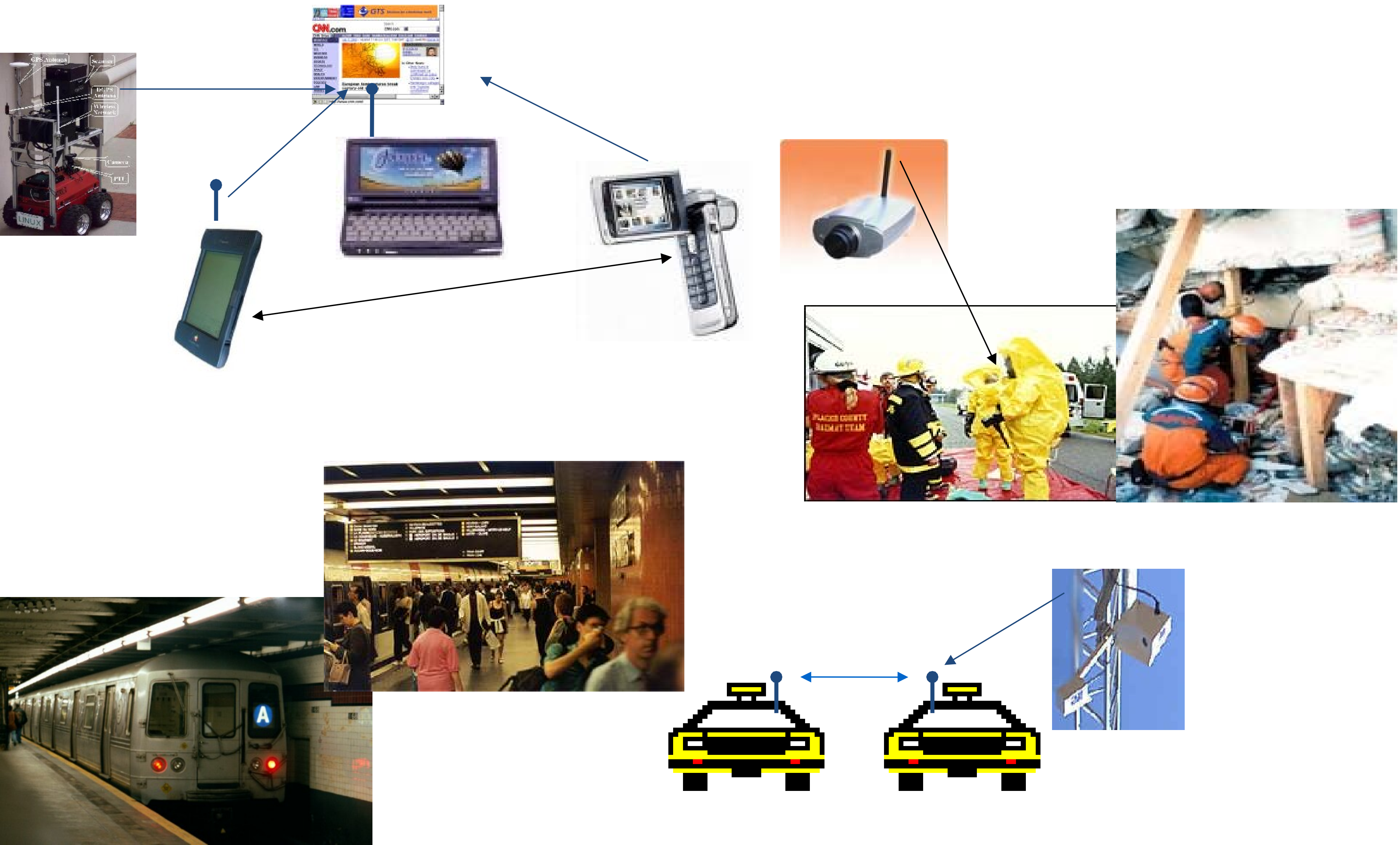
Experimental-based WBN Evaluation Framework

µServer
2-stages implementation:

- Stage 1: Application-Level Gateway Functionality
 (implementation on standard host machine, with mounted WBN node)
- Stage 2: Transition of functionality at Single-Board-Computer with mounted WBN node (to allow for portability within the industrial plant)



Παραδείγματα με κινητά υπολογιστικά συστήματα που μπορούν να χρησιμοποιήσουν το mobile p2p μοντέλο



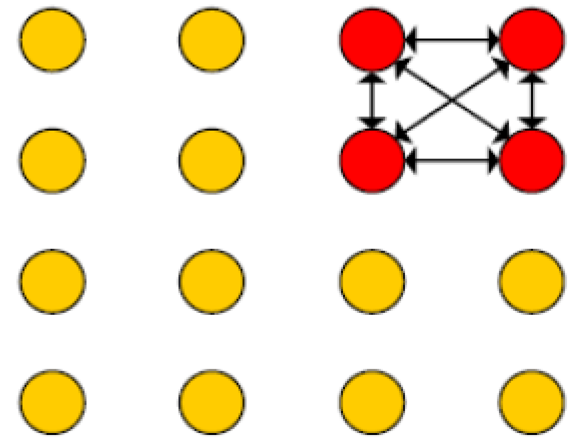
Traffic patterns in WSNs

WSN applications:

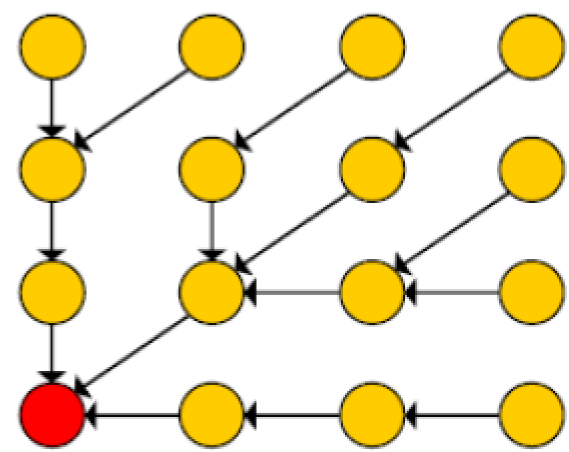
- Local collaboration when detecting a physical phonomenon
- Periodic reporting to sink

Characteristics:

- Low data rates < 1000 bps
- Small messages (~ 25 bytes)
- Fluctuations (in time and space)
- Network management
  - Periodic reporting
  - Event-driven reporting



local gossip

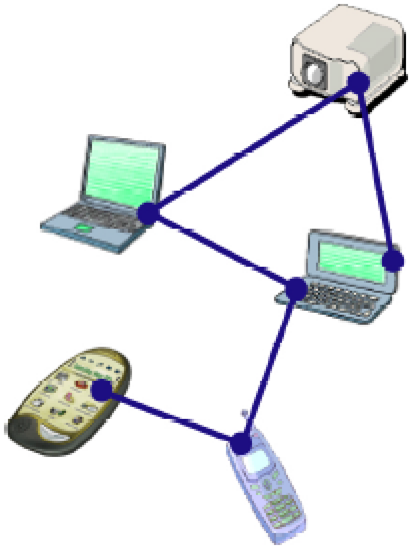


convergecast

The Basic Principle of Ad Hoc Networking

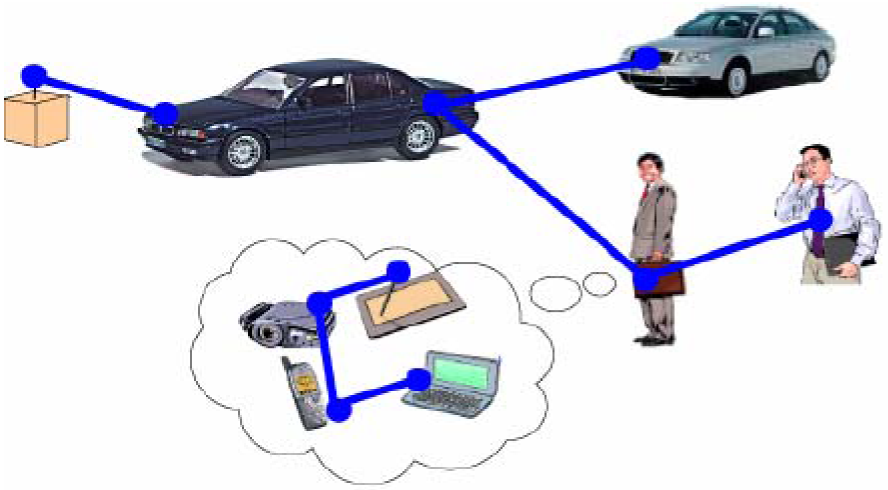
Mobile device communicate in peer-to-peer fashion

- Self-organizing network without the need of fixed network infrastructure
- Multi-hop communication
- Decentralized, mobility-adaptive operation



“The art of networking without a network”
[Frodigh et al.]

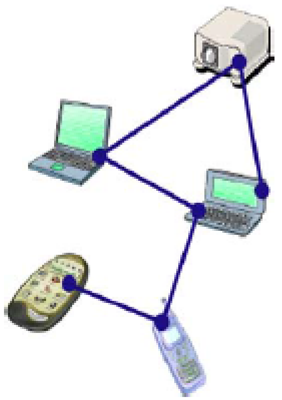
Applications: Vehicular Networks



Applications

- Accident warning
- Floating car data
- Multihop extensions of Infostations

Ad Hoc Networks: Pros and Cons



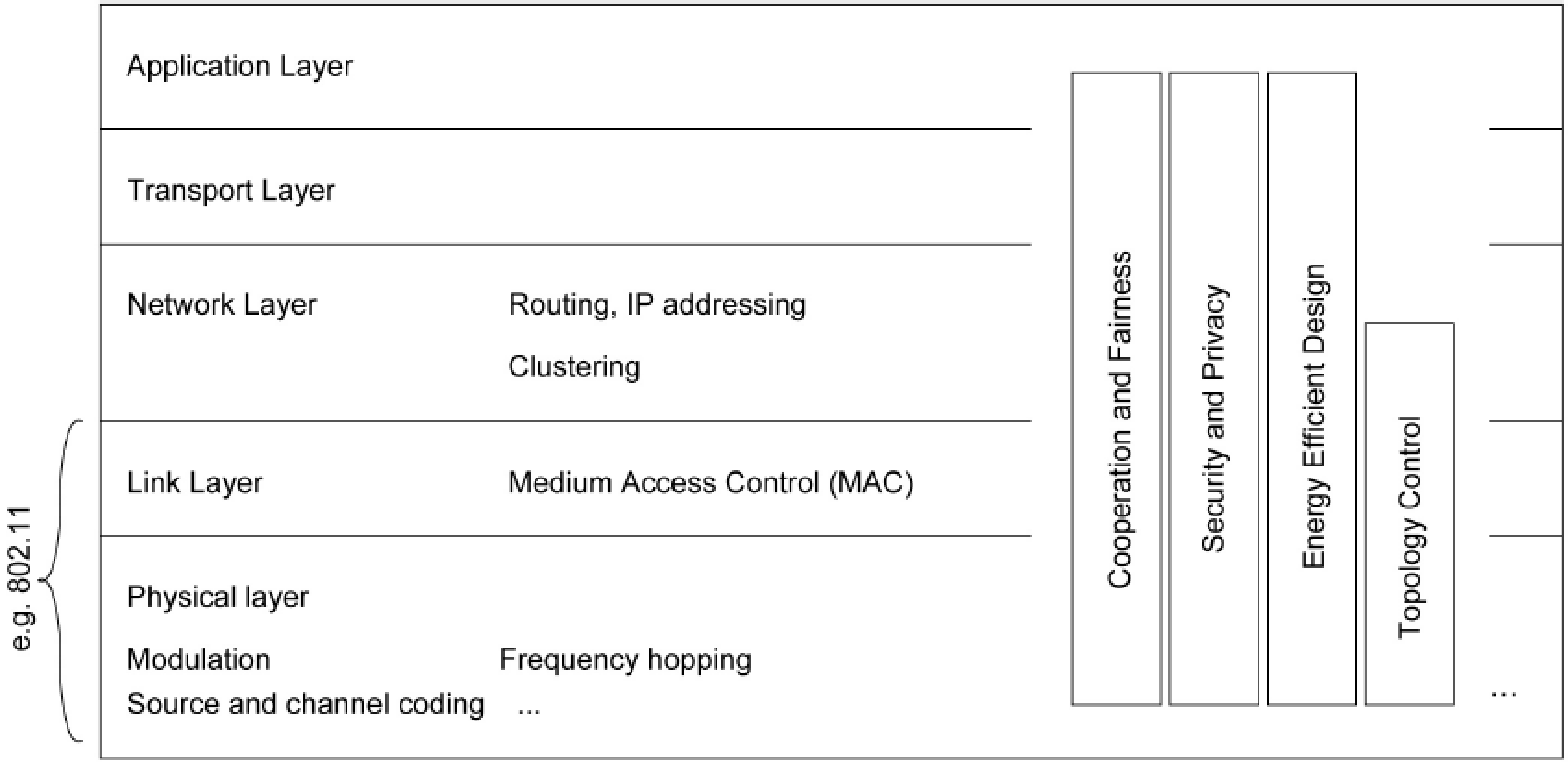
Key Advantages

- No expensive infrastructure must be installed
- Use of unlicensed frequency spectrum
- Quick distribution of information around sender

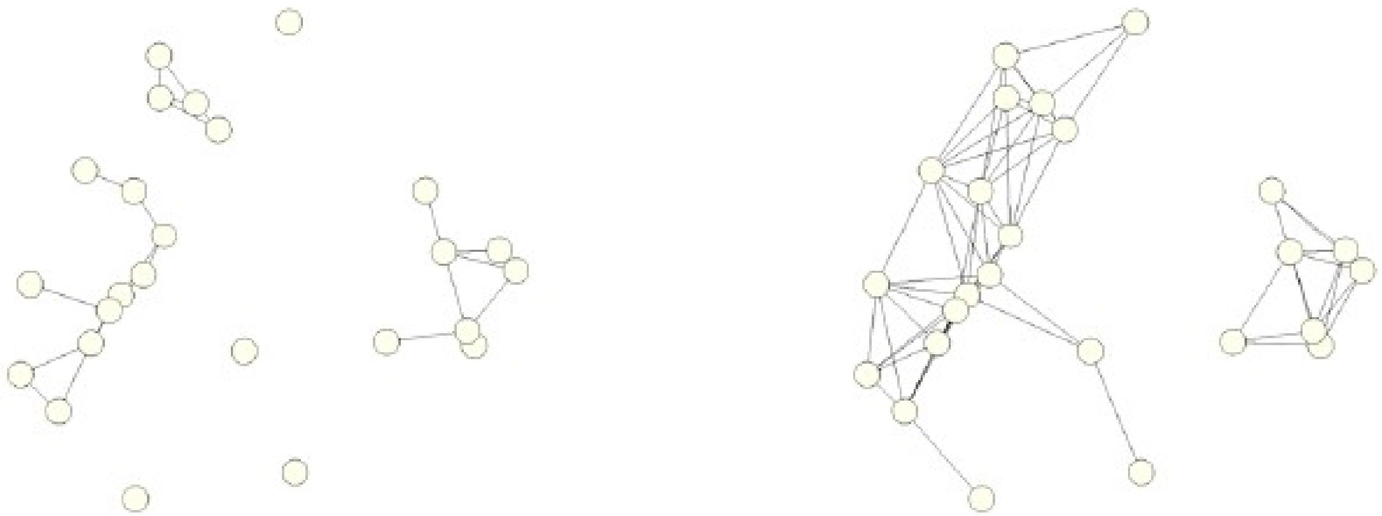
Key Challenges

- All network entities may be mobile ⇒ very dynamic topology
- Network functions must have high degree of adaptability (mobility, outage)
- No central entities ⇒ operation in completely distributed manner

Research Issues on All Layers



High versus low transmission power



(a) Ad hoc network with low transmission power

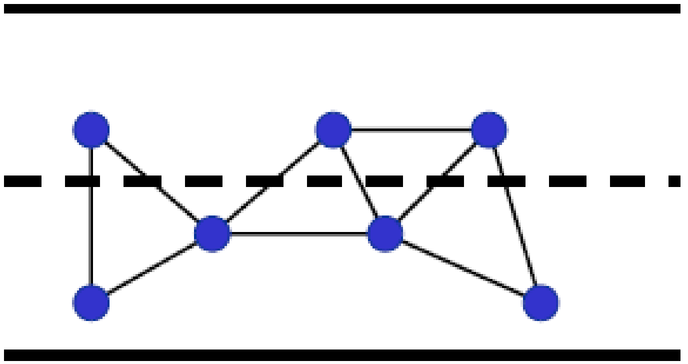
(b) Ad hoc network with high transmission power

Transmission power	low	high
Interference between nodes	low	high
Spatial reuse of radio resources	good	bad
Number of hops from source to dest.	many	few
Relaying load per node	high	low
Message queuing delay from source to dest.	high	low
Connectivity	bad	good

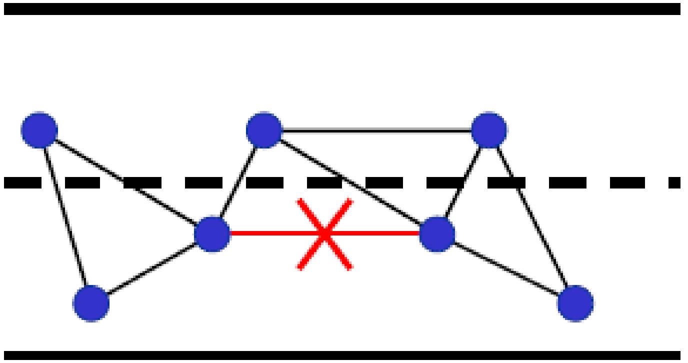
from C. Bettstetter PhD thesis

Why is Routing for Ad-Hoc Networks a Problem?

- Well known from the Internet:
  - link state routing (OSPF)
  - distance vector routing (RIP)
- Proactive approach:
  - always maintain all routes



- Problem:
  - topology changes ⇒ significant network traffic
  - even when the route is not used



Flooding!

Unicast Routing Protocols

- Many protocols have been proposed
- Some have been invented specifically for MANETs
- Others are adapted from previously proposed protocols for wired networks
- No single protocol works well in all environments
  - some attempts made to develop adaptive protocols

Routing Protocols

- Proactive protocols
  - Determine routes independent of traffic pattern
  - Traditional link-state and distance-vector routing protocols are proactive
- Reactive protocols (this tutorial)
  - Maintain routes only if needed
- Hybrid protocols
  - Combine proactive and reactive elements
- Position-based (this tutorial)
  - Use the geographic position of nodes for forwarding decisions

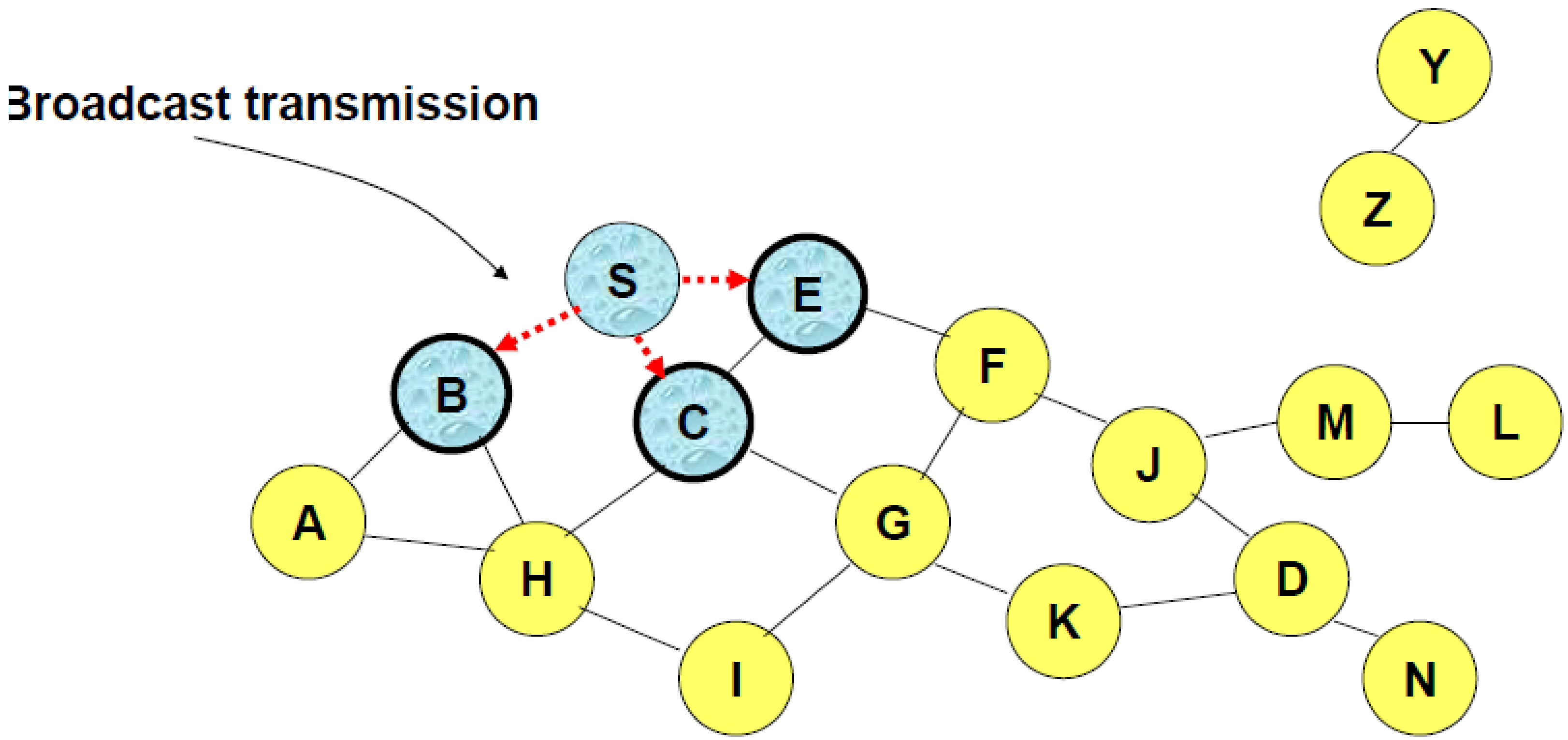
Trade-Off

- Latency of route discovery
  - Proactive protocols may have lower latency since routes are maintained at all times
  - Reactive protocols may have higher latency because a route from X to Y will be found only when X attempts to send to Y
- Overhead of route discovery/maintenance
  - Reactive protocols may have lower overhead since routes are determined only if needed
  - Proactive protocols can (but not necessarily) result in higher overhead due to continuous route updating
- Which approach achieves a better trade-off depends on the traffic and mobility patterns

Flooding for Data Delivery

- Sender S broadcasts data packet P to all its neighbors
- Each node receiving P forwards P to its neighbors
- Sequence numbers used to avoid the possibility of forwarding the same packet more than once
- Packet P reaches destination D provided that D is reachable from sender S
- Node D does not forward the packet

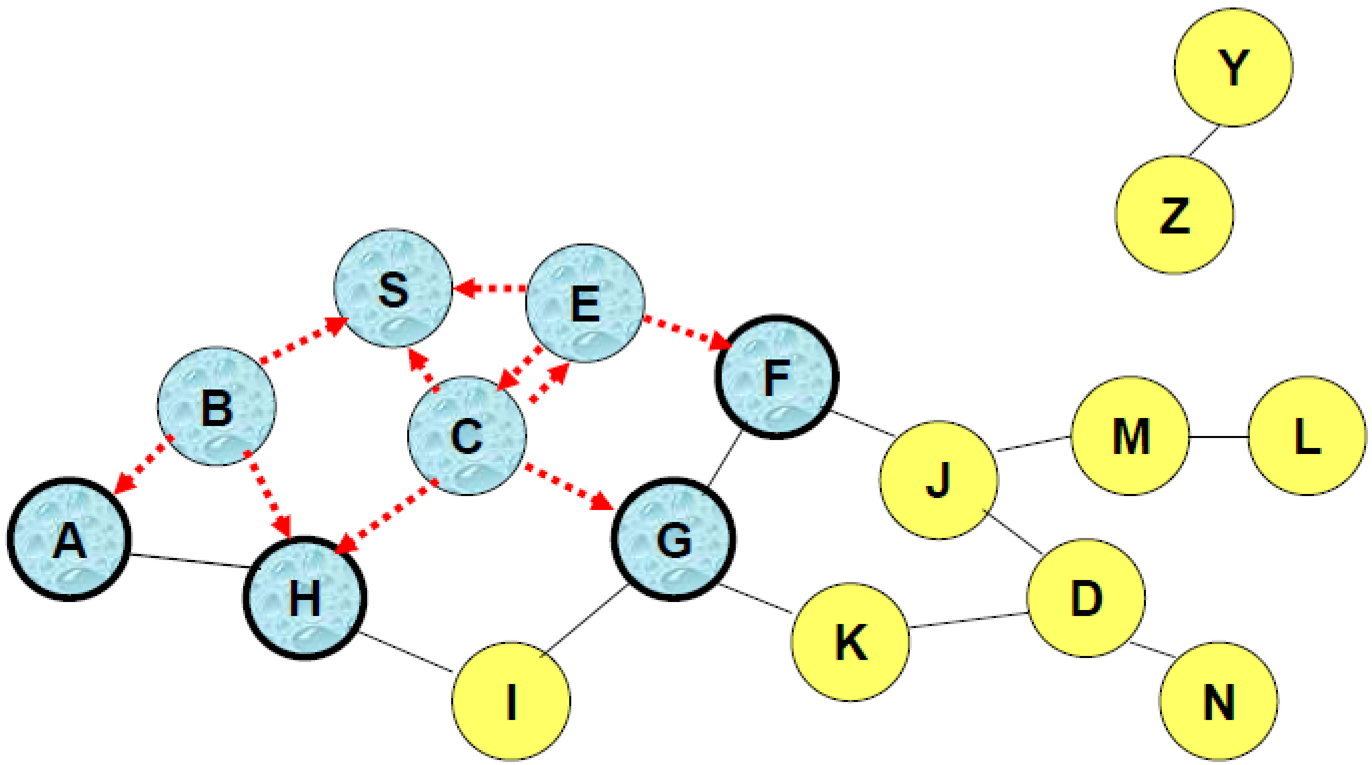
Flooding for Data Delivery



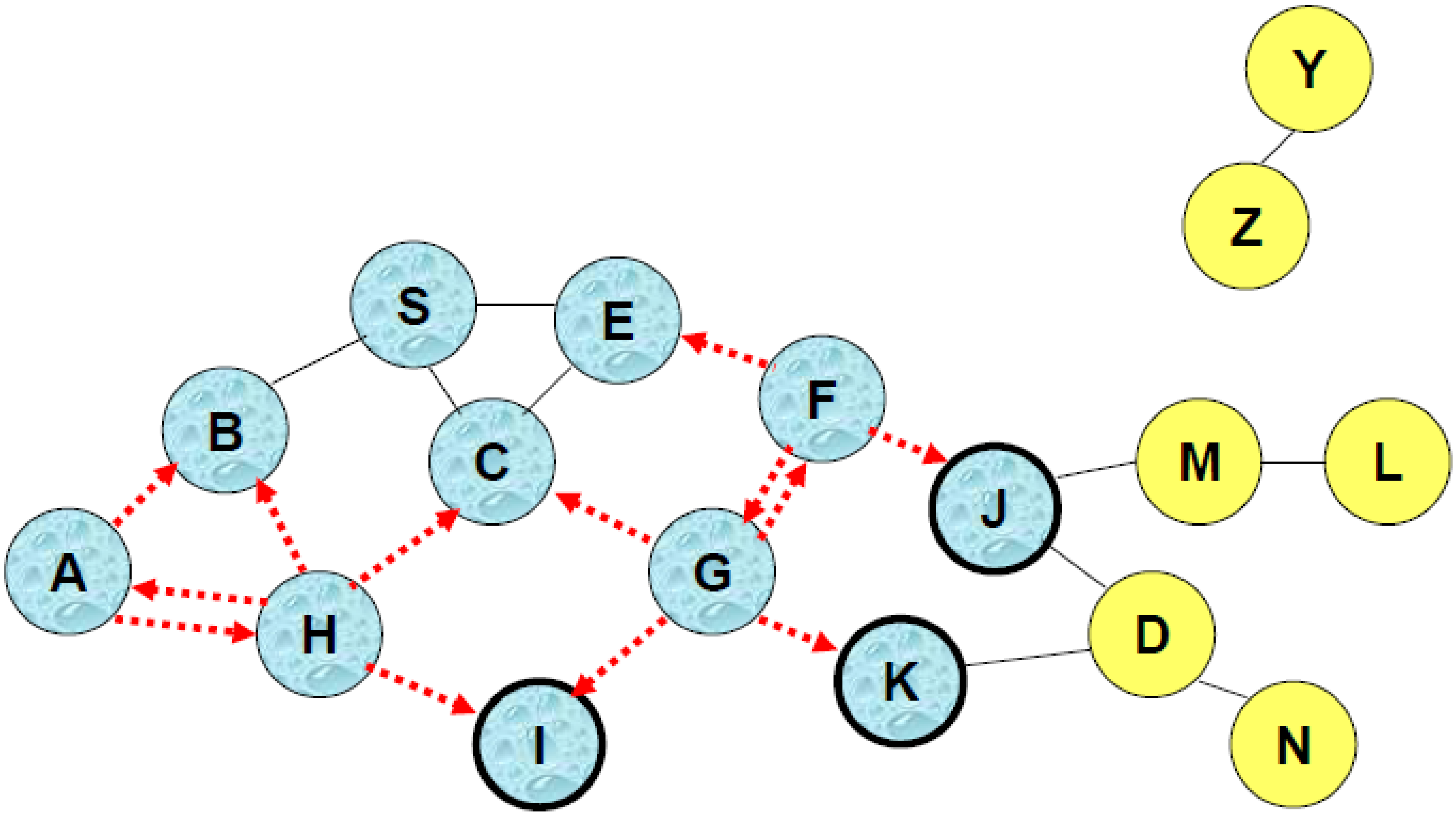
Represents a node that receives packet P for the first time

Represents transmission of packet P

Flooding for Data Delivery

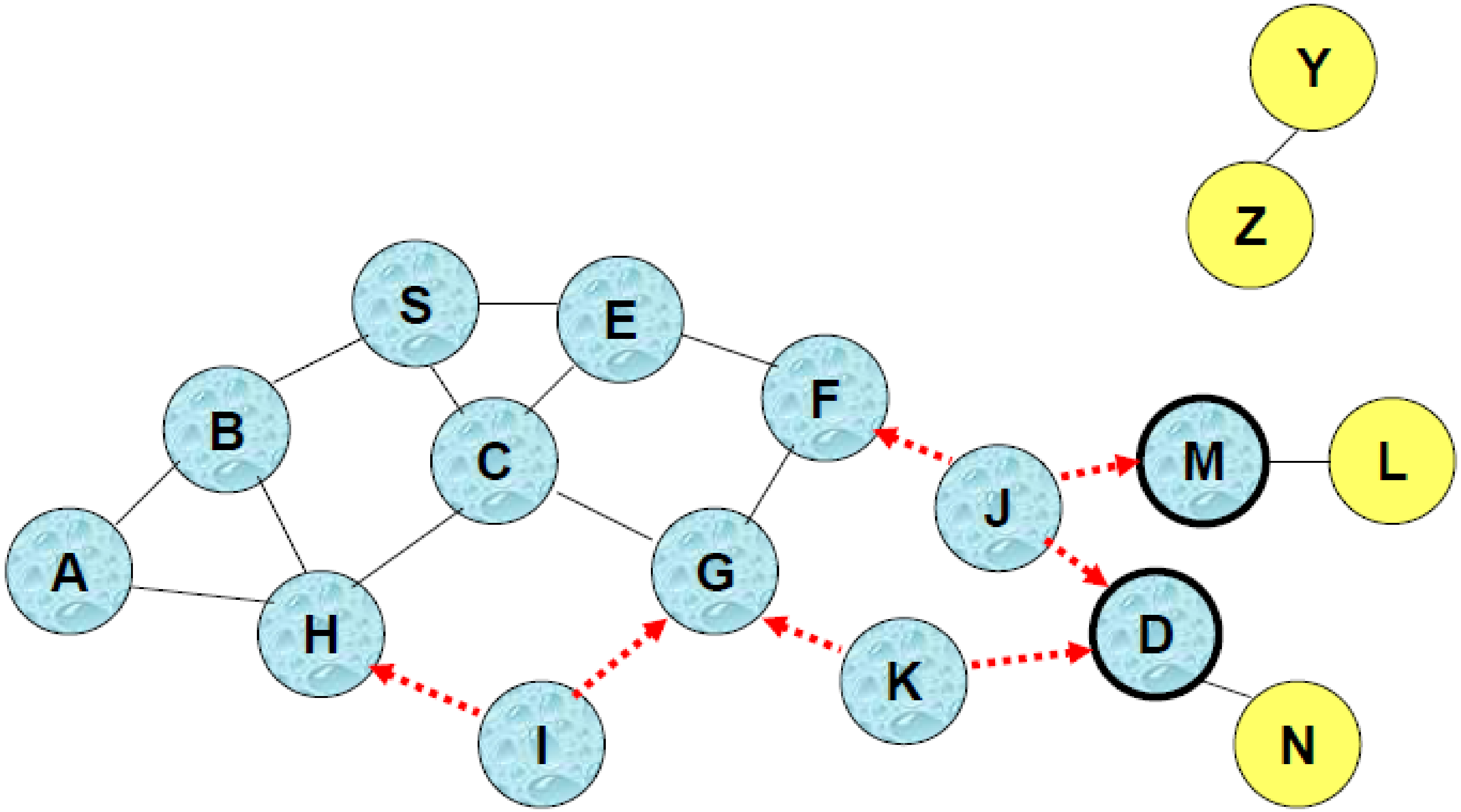


Flooding for Data Delivery



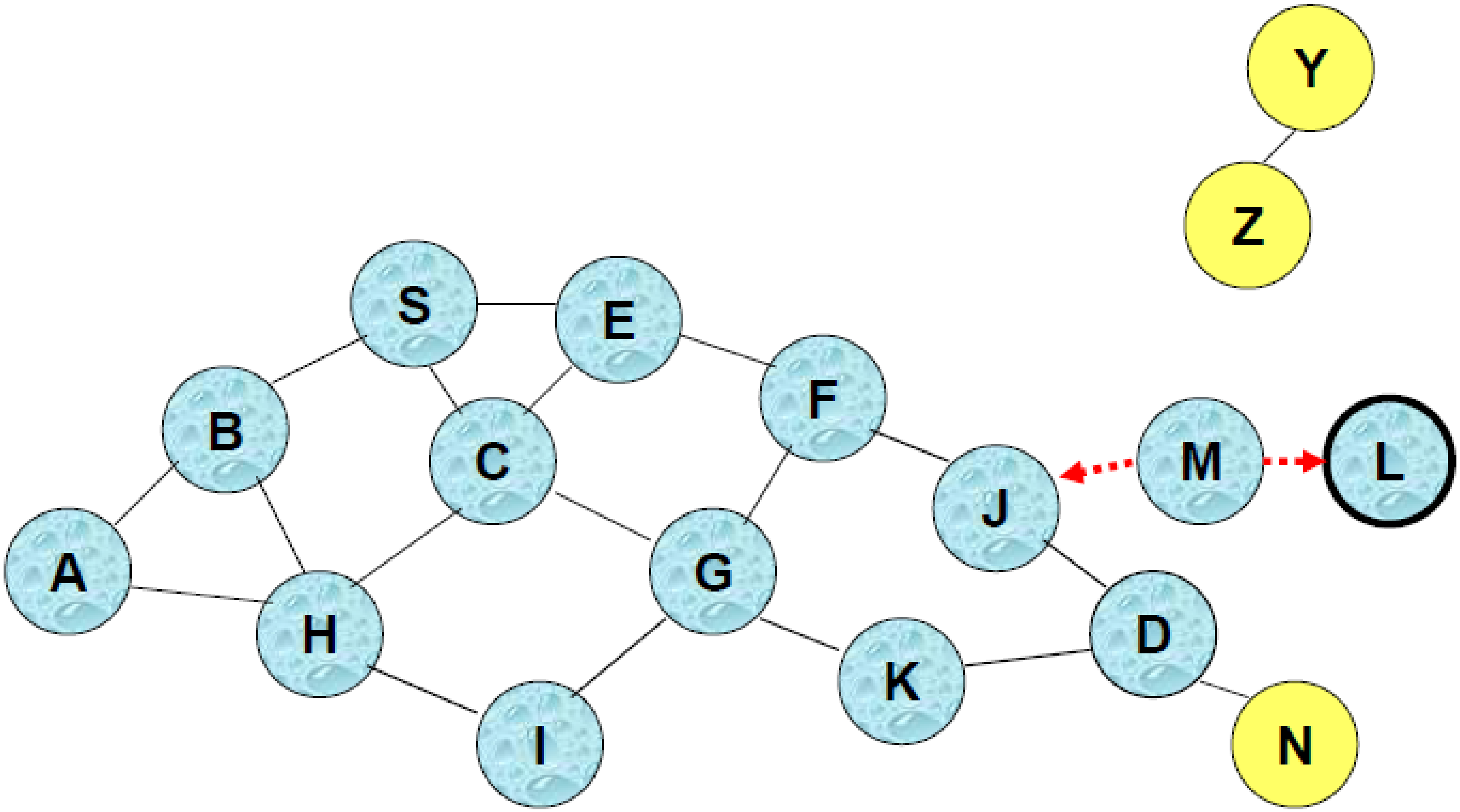
- Node C receives packet P from G and H, but does not forward it again, because node C has already forwarded packet P once

Flooding for Data Delivery



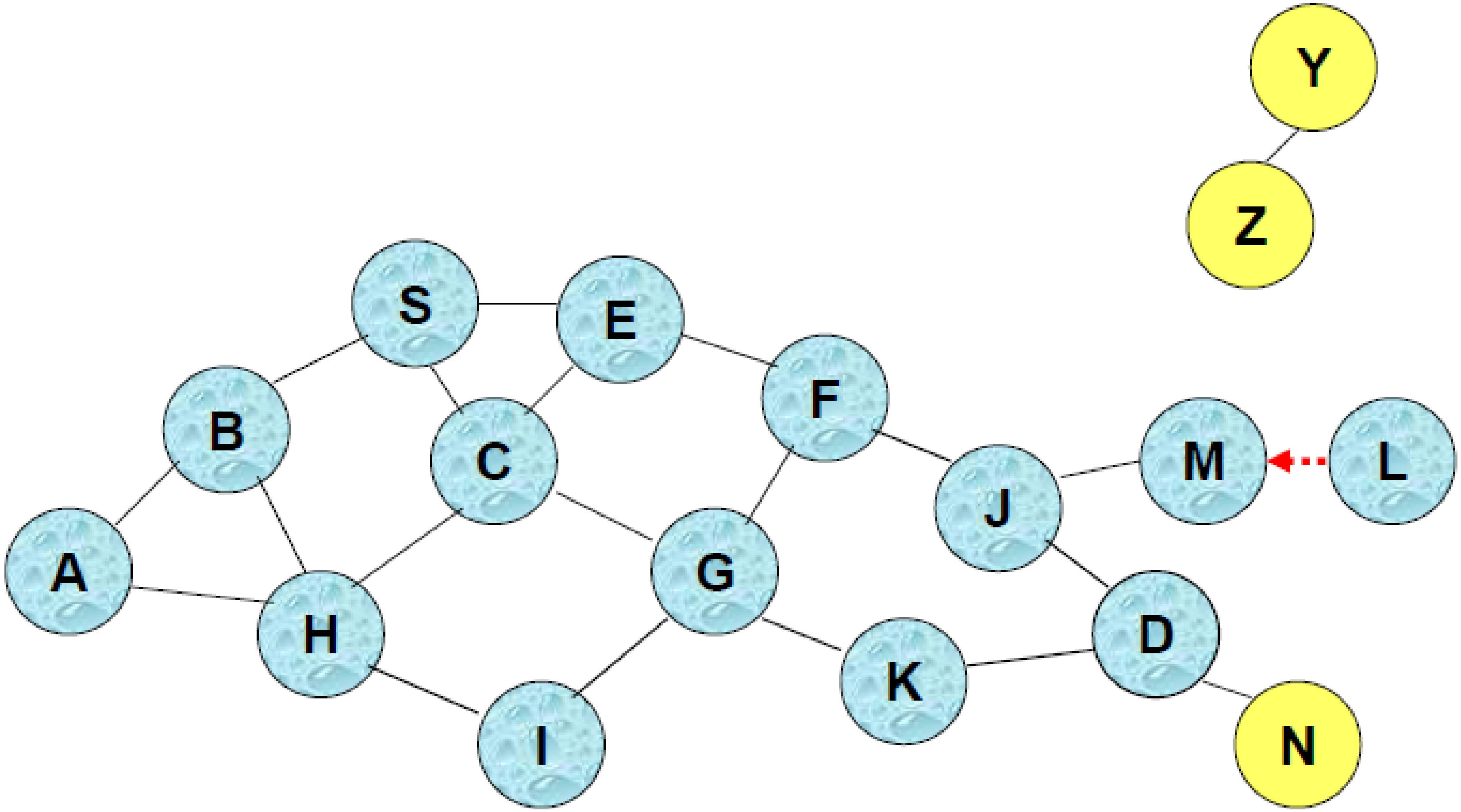
- Node D receives packet P from two neighbors: potential for collision, packet may get lost despite flooding

Flooding for Data Delivery



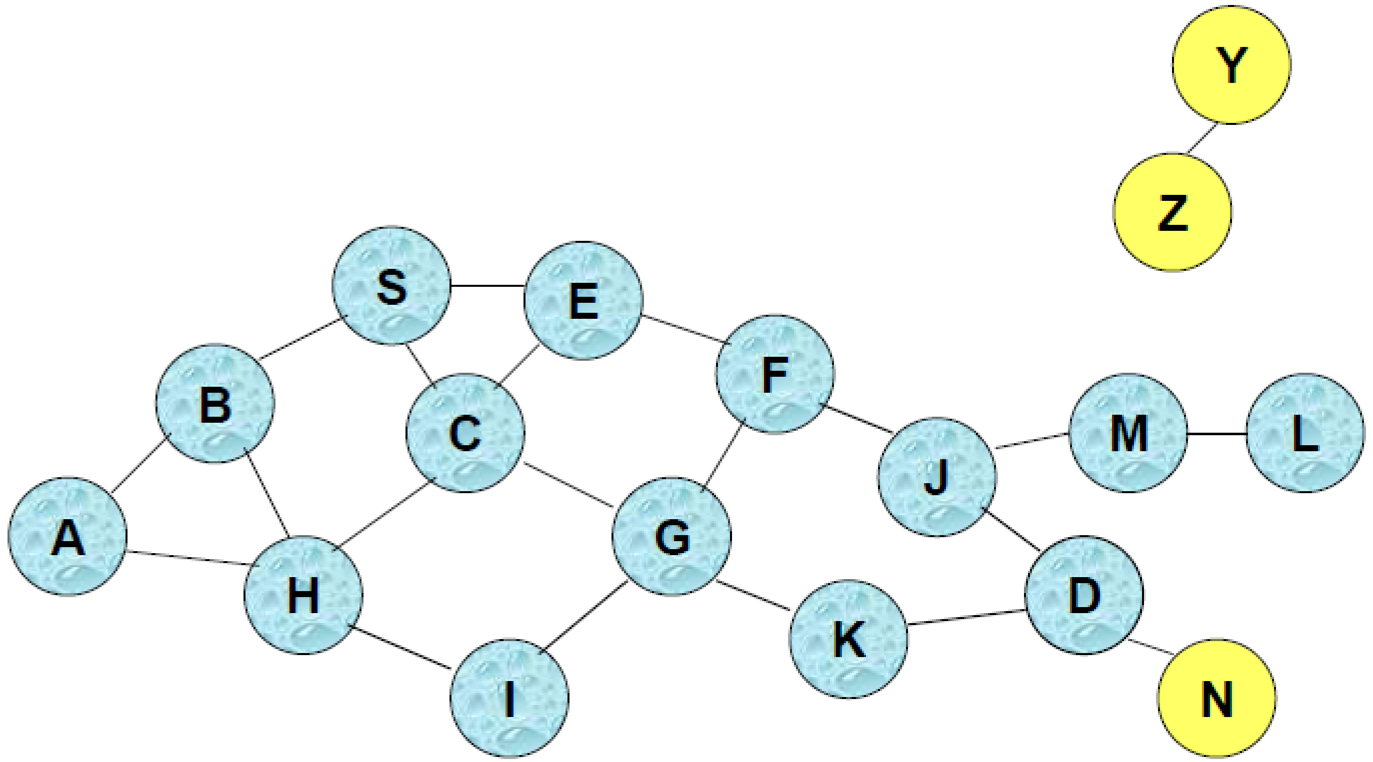
- Node D does not forward packet P, because node D is the intended destination of packet P

Flooding for Data Delivery



- Flooding completed
- Nodes unreachable from S do not receive packet P (e.g., node Z)
- Nodes for which all paths from S go through the destination D also do not receive packet P (example: node N)

Flooding for Data Delivery



- Flooding may deliver packets to too many nodes (in the worst case, all nodes reachable from sender may receive the packet) => High Overhead

Flooding of Control Packets

- Many protocols perform (potentially *limited*) flooding of control packets, instead of data packets
- The control packets are used to discover routes
- Discovered routes are subsequently used to send data packet(s)
- Overhead of control packet flooding is amortized over data packets transmitted between consecutive control packet floods

Position-based routing: building blocks

Positioning	• Get own position
Position Service	• Get current position of an (arbitrary) node
Forwarding Strategy	• Determine next hop • based on own position, neighbor's positions, position of the destination, maybe also based on source's position.

Directed diffusion: gradients

- Every node maintains an 'interest cache' (soft state).
  - Cache entry: `interest : timestamp : gradient(s)`
    - Gradient: `r-neighbor : data rate : duration`
- 'Sink' broadcasts interest periodically to all one-hop neighbors.
- After receiving an interest, a node may decide to re-send the interest to some neighbors.
  - Re-broadcast; leads to flooding.
  - Geographic routing.
  - Based on cached data.

- 'Data rate' can be tuned to first find nodes that actually can responed to an interest with moderate network load. Upon success, the data rate is increased but only for 'suitable' paths/nodes.

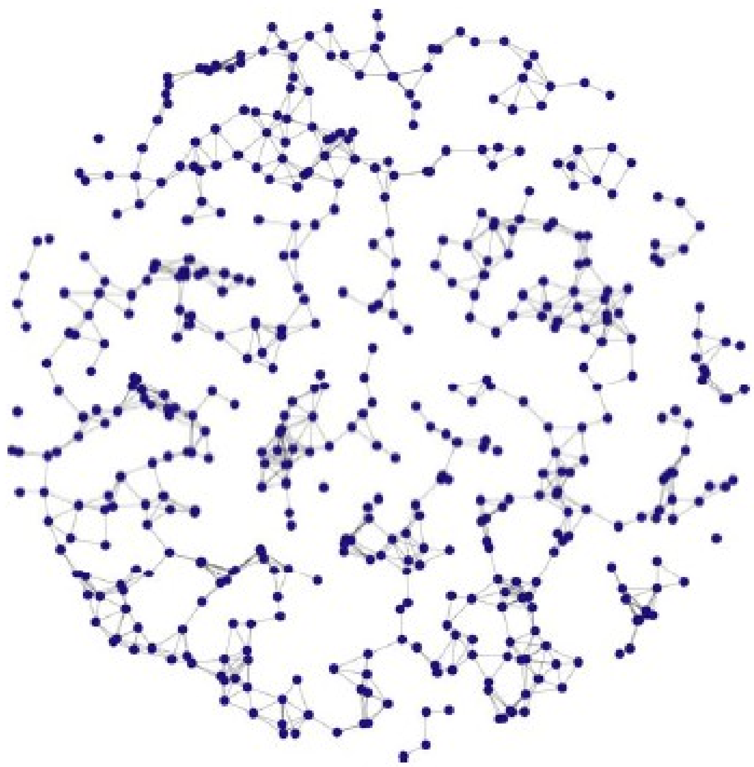
Directed diffusion: data propagation/reinforcement

- Sensor node in the interest's area sends data to all r-neighbors of this interest.
- Nodes receiving data
  - check with their interest cache
  - check with their data cache
  - re-send data again, maybe with 'downconversion'.

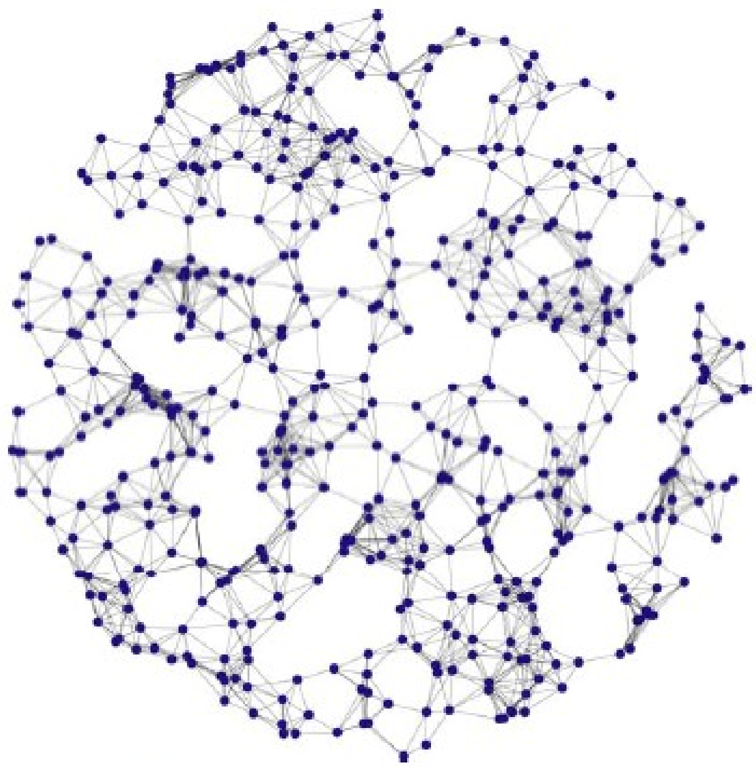
- Sink might reinforce a specific neighbor that appears to be 'optimal' w.r.t. some metrics.

Motivation and Definition

The ad hoc network should be **connected**.



(a) disconnected network



(b) connected network

Performance of data dissemination in an ad hoc network

Examples of measurements:

- Average throughput for the communication of a random pair of nodes
- Total time required for a specific message to be transmitted to all nodes
- Average delay for a node to receive a specific message

Capacity in an ad hoc network

Capacity decreases with node density

- an ad hoc network with N nodes
- Pairs of nodes communicating
- Source and destination nodes are randomly chosen

Throughput is in the order of Θ (W/□ (n* log(n)))

# of simple epidemic models for data dissemin

A simple epidemic model can be then used to compute the expected delay for a message to be propagated to the population of an area, as described in [321]. For the epidemic model, the following assumptions are made:

- A population of N peers at time 0 consists of one dataholder (the "infected" node) and $N-1$ queriers (the "susceptibles" ones).
- Once a peer acquires the data, the data will be locally stored permanently.
- In any time interval h, any given dataholder will transmit data to a querier with probability $h\alpha + o(h)$.

If $X(t)$ denotes the number of data holders in the population at time t, the process $\{X(t),\ 0 \leq t\}$ is a pure birth process with rate λ_k

$$\lambda_k = \left\{ \begin{matrix} (N-k)N\alpha, & k = 1, .., N-1 \\ 0, & \text{otherwise} \end{matrix} \right\} \tag{3.2}$$

Thus, when there are k dataholders, each of the remaining mobiles will get the data at a rate equal to $k\alpha$. If T denotes the time until the data has been spread amongst all the mobiles, then T can be represented as

$$T = \sum_{i=1}^{N-1} T_i, \tag{3.3}$$

Use of simple epidemic models for data dissemination (cont'd)

where T_i is the time to go from i to $i+1$ dataholders. As the T_i are independent exponential random variables with respective rates $\lambda_i = (m-i)i\alpha$, $i = 1, .., m-1$, the expected value of T is given by

$$E[T] = \frac{1}{\alpha} \sum_{i=1}^{N-1} \frac{1}{i(N-1)}. \qquad (3.4)$$

Use of
Particle kinetics
& classical physics
to model
data dissemination

We apply a theoretical framework based on diffusion-controlled processes, random walks and kinetics of diffusion-controlled chemical processes [280] to model FIS. Let us first describe a diffusion process that is closely related to information dissemination. Consider a diffusion process that takes place in a medium with randomly distributed static traps and two types of particles, namely, S-type (stationary traps or sinks) and M-type (mobile particles) [196]. In such a static trapping model, particles of M-type perform diffusive motion in d-dimensional space while particles of S-type are static and randomly distributed in space. M-type particles are absorbed by S-type when they collide with them. The simple trapping model assumes traps of infinite capacity. The diffusion-controlled processes focus on the *survival probability*, that is the probability that a particle will *not* get trapped as a function of time.

Rosenstock's trapping model in d dimensions assumes a genuinely d-dimensional, unbiased walk of finite mean-square displacement per step and has a survival probability ϕ_t that for large t follows

$$\log(\phi_t) \approx -\alpha[\log\left(\frac{1}{1-q}\right)]^{(\frac{2}{d+2})}t^{(\frac{d}{d+2})} \tag{3.5}$$

where α is a lattice-dependent constant, and q denotes the concentration of the independently distributed, irreversible traps.

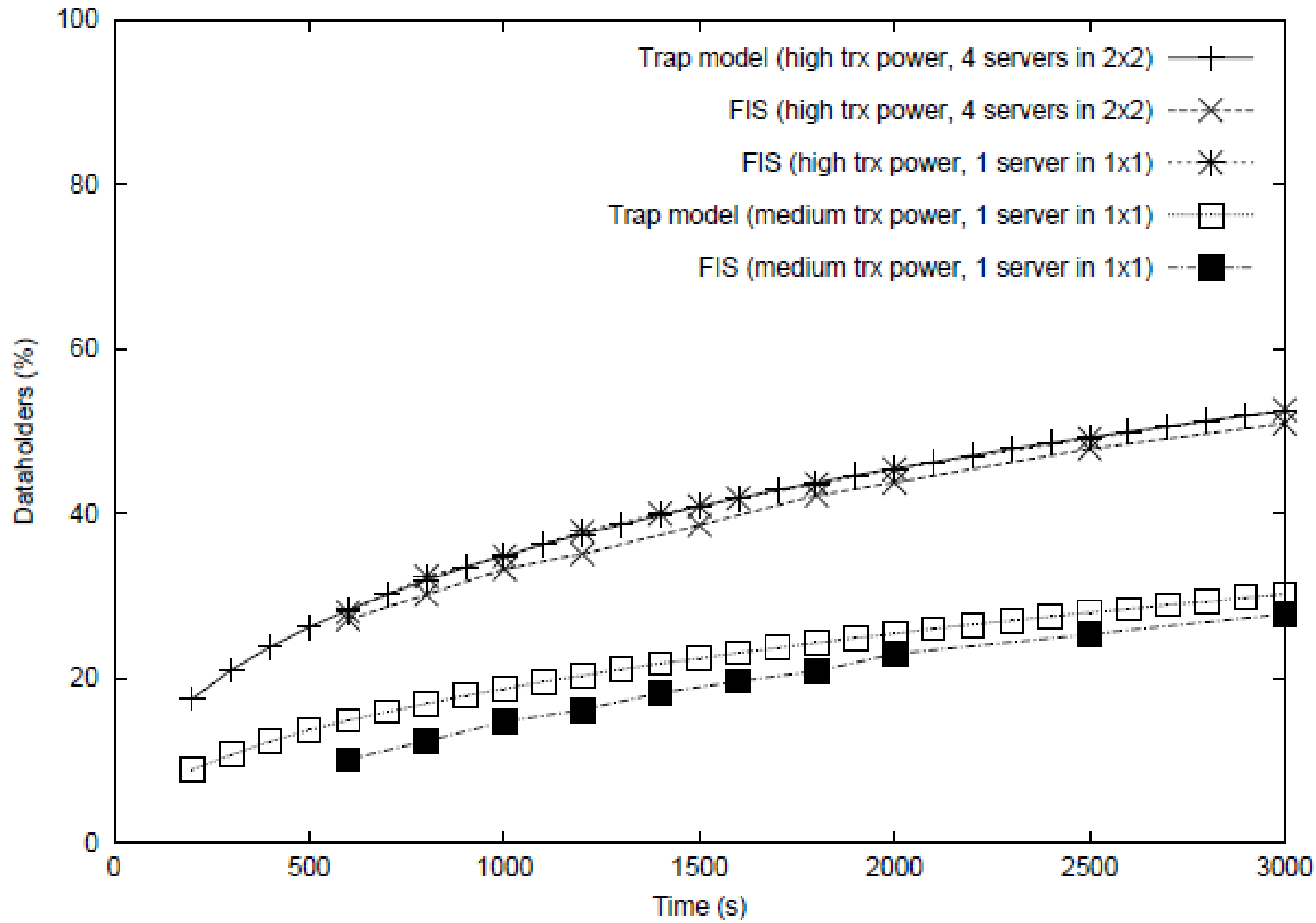
One question is: when Eq. 3.5 is a useful approximation? To answer this question, most studies have relied on simulations, but so far there is no information available on the range of validity of Eq. 3.5. In [174], Havlin *et al.* presented evidence suggesting that Eq. 3.5 is a useful approximation when

$$\rho > 10 \tag{3.6}$$

where ρ is the scaling function

$$\rho = \ln\left(\frac{1}{1-q}\right)^{\frac{2}{d+2}} t^{\frac{d}{d+2}}. \tag{3.7}$$

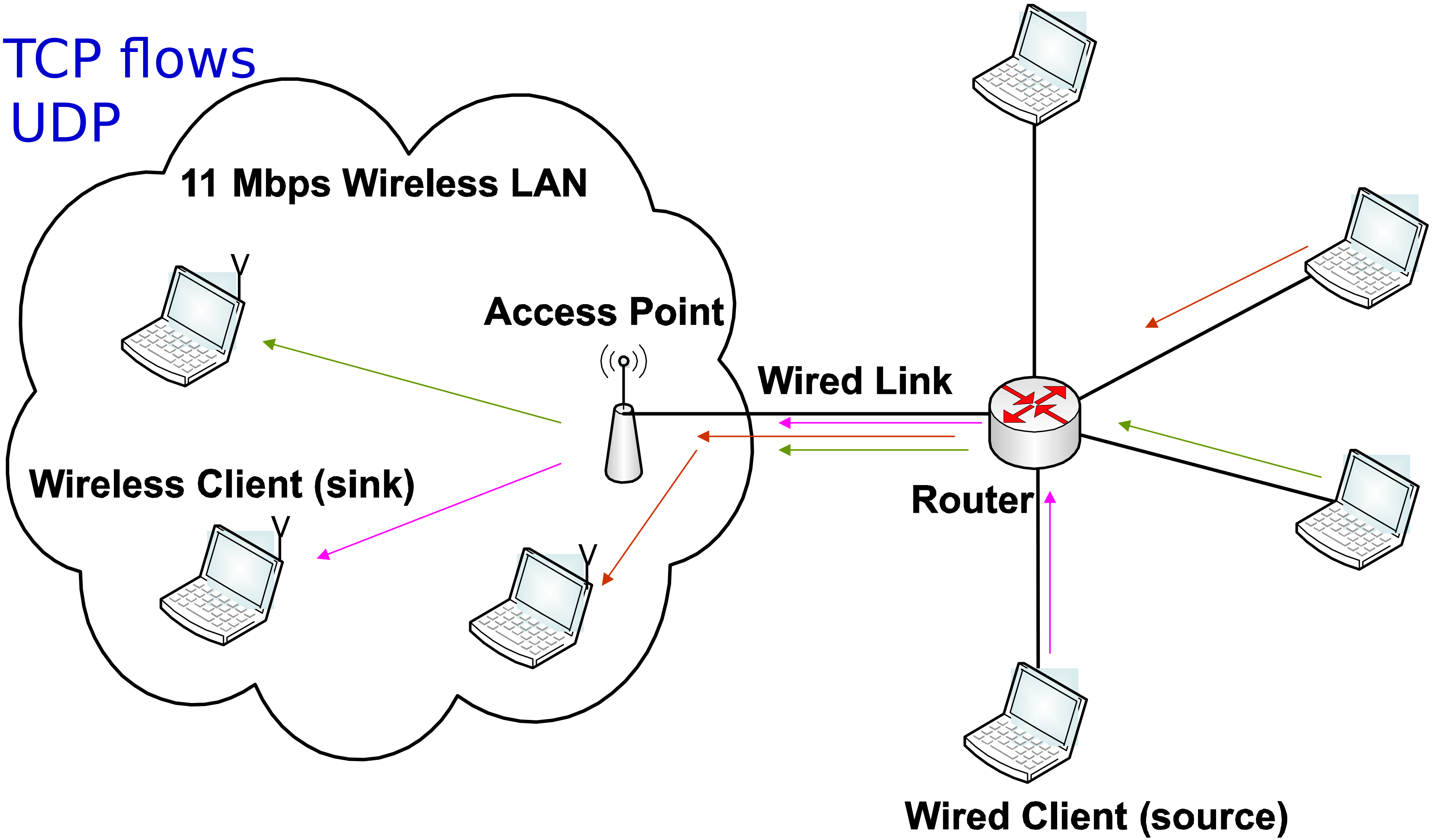
This value of ρ corresponds to a survival probability which is equal to 10^{-13}



Trap model (high trx power, 4 servers in 2x2)
FIS (high trx power, 4 servers in 2x2)
FIS (high trx power, 1 server in 1x1)
Trap model (medium trx power, 1 server in 1x1)
FIS (medium trx power, 1 server in 1x1)
Dataholders (%)
Time (s)
0
20
40
60
80
100
0
500
1000
1500
2000
2500
3000

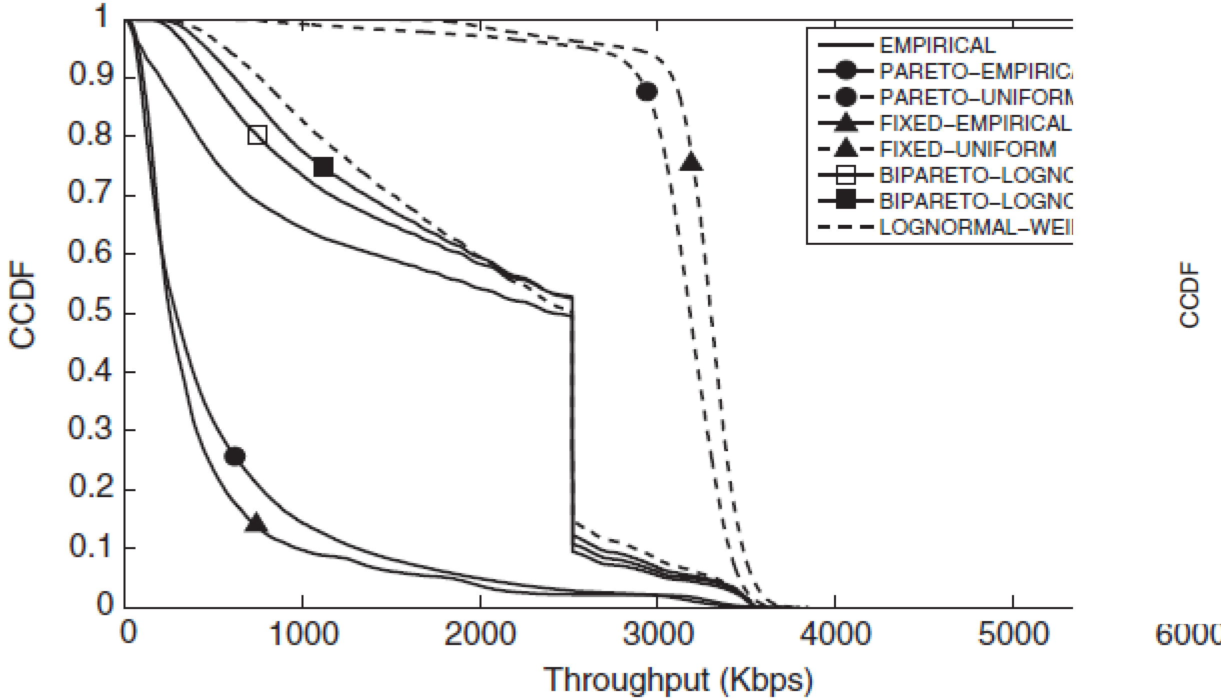
Simulation/Emulation testbed

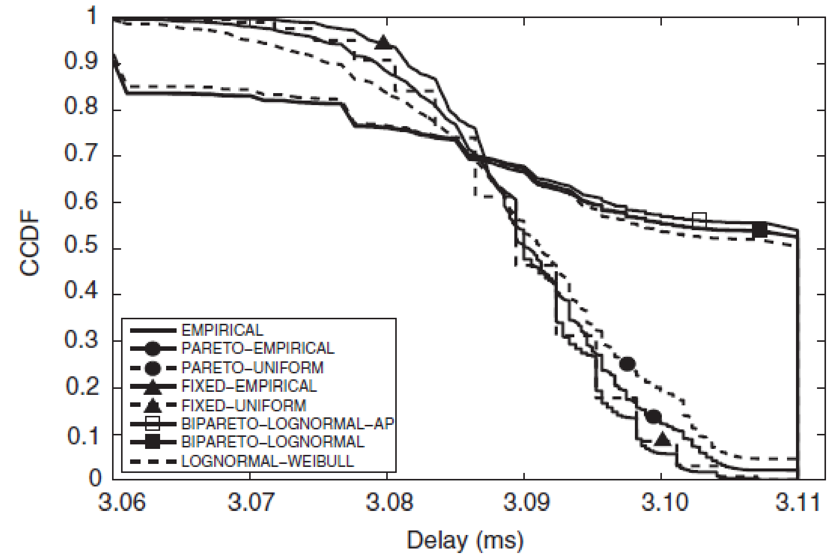
- TCP flows
- UDP

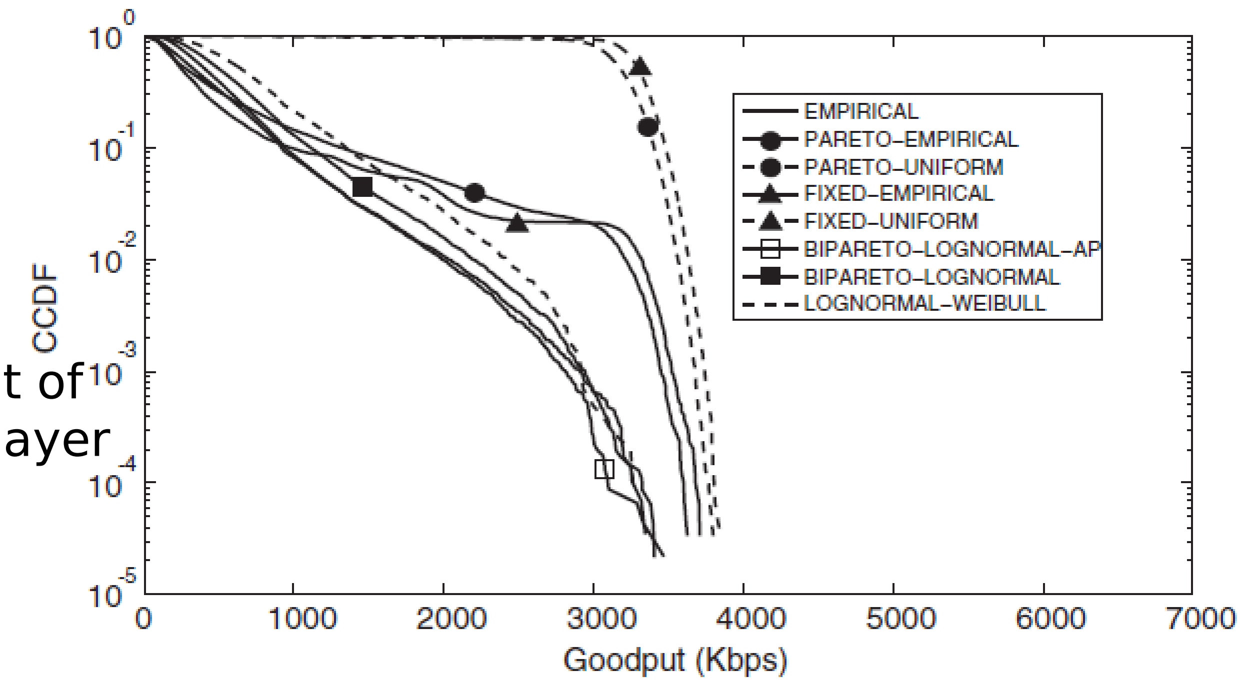


- Wired clients: senders
- Wireless clients: receivers

ut & goodput per flow in a wireless hotspot AP simulated with real-tra

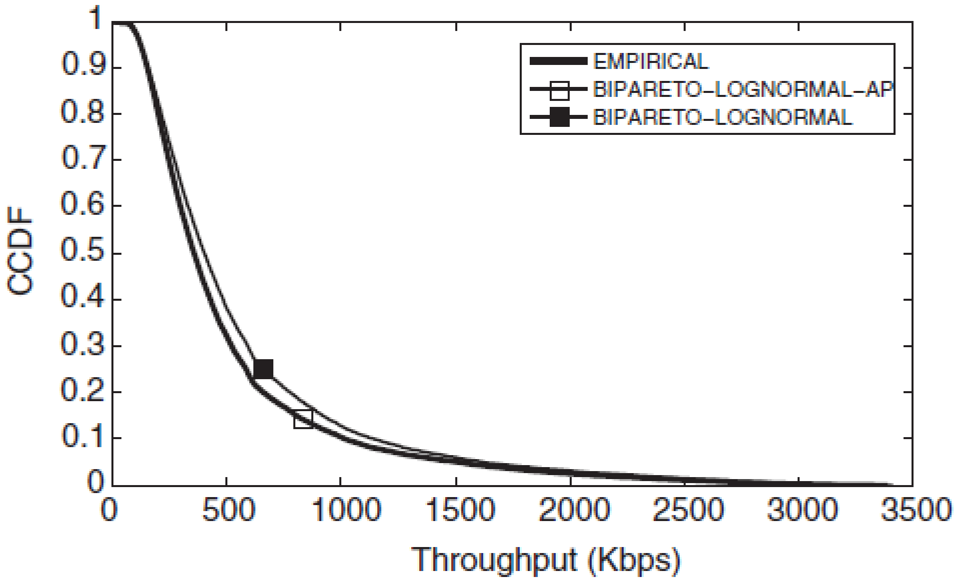




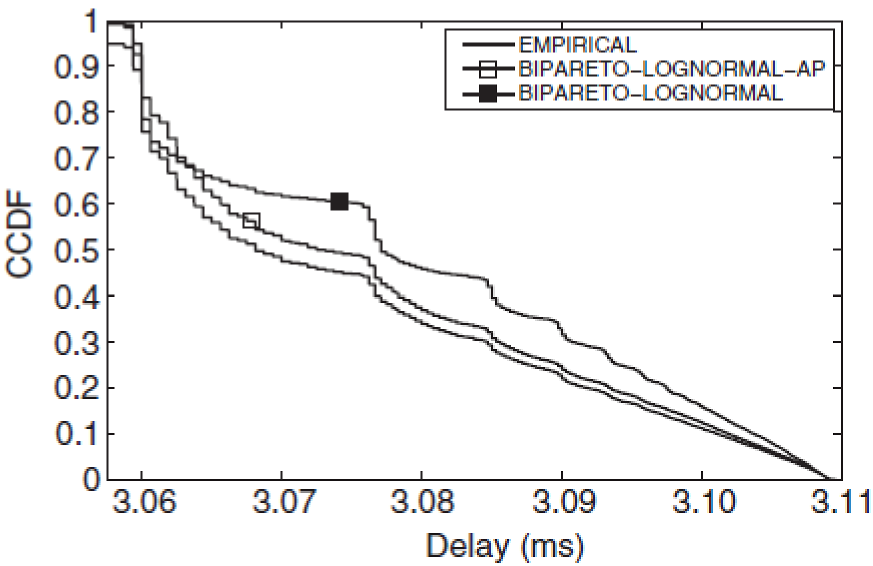


Goodput: only considers the amount of
Bytes delivered from the transport layer
to the application layer

rmance of an AP using emulation and “replaying” real-tra

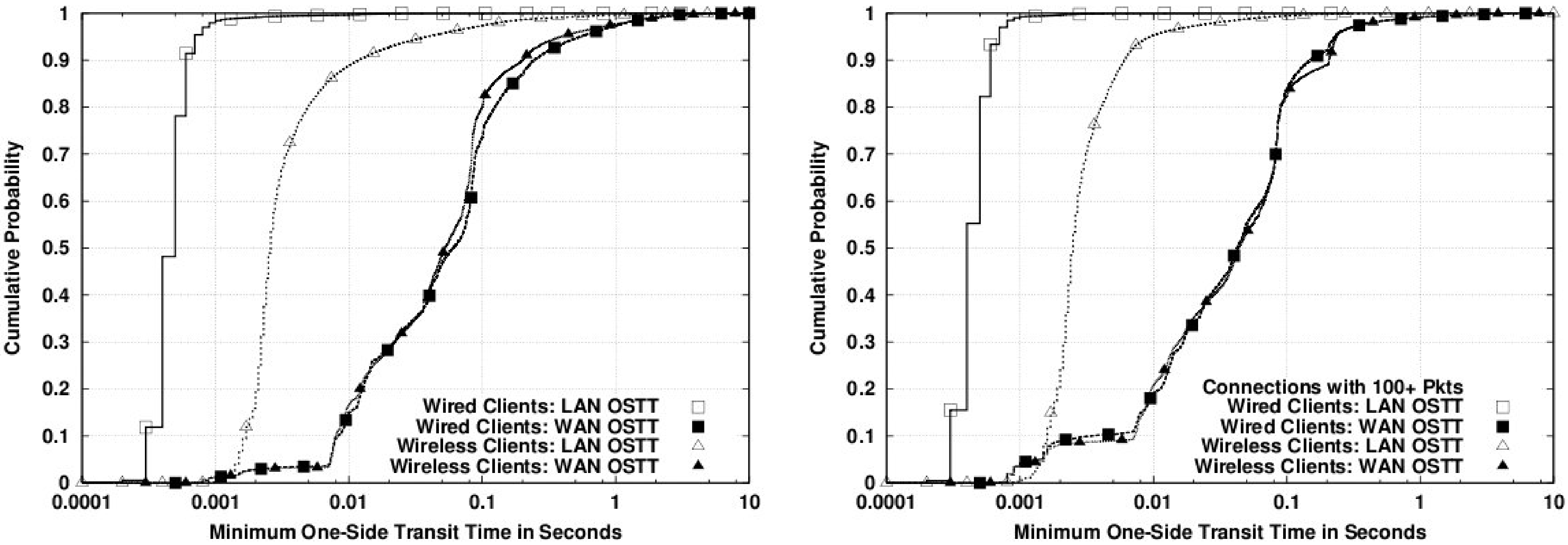


(a) hotspot with 85% web traffic



(a) hotspot with 85% web traffic

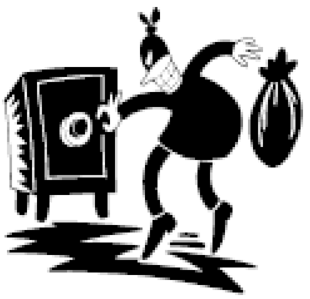
Real-life delay measurements



Attack types & Building blocks of countermeasures

- Passive attacks
  - get ‘content’
  - profiling

- Active attacks
  - fabricating or ‘stealing’ of packets
  - modification of packets
  - DoS attacks



- Counter measures can be based on
  - cryptography
  - monitoring

What are 'ad hoc specific' attack types?

Equipment Battery	No obvious 'line of defence'; side channel attacks 'Sleep deprivation torture' [Stajano2002]
Radio	Jamming
DLC	Attacks on MAC, MAC address
Routing	No infrastructure support; no clear line of defense
Cooperation	Based on principle of mutual assistance. Simple 'attack': drop packet.
Transport	Congestion control
Application	Attacks on key distribution and trust management; attacks on 'content' when content is used for forwarding decisions, data aggregation

Fairness and reliability