

15th TF-Mobility Meeting

Sensor Networks

Torsten Braun

Universität Bern

braun@iam.unibe.ch

www.iam.unibe.ch/~rvs

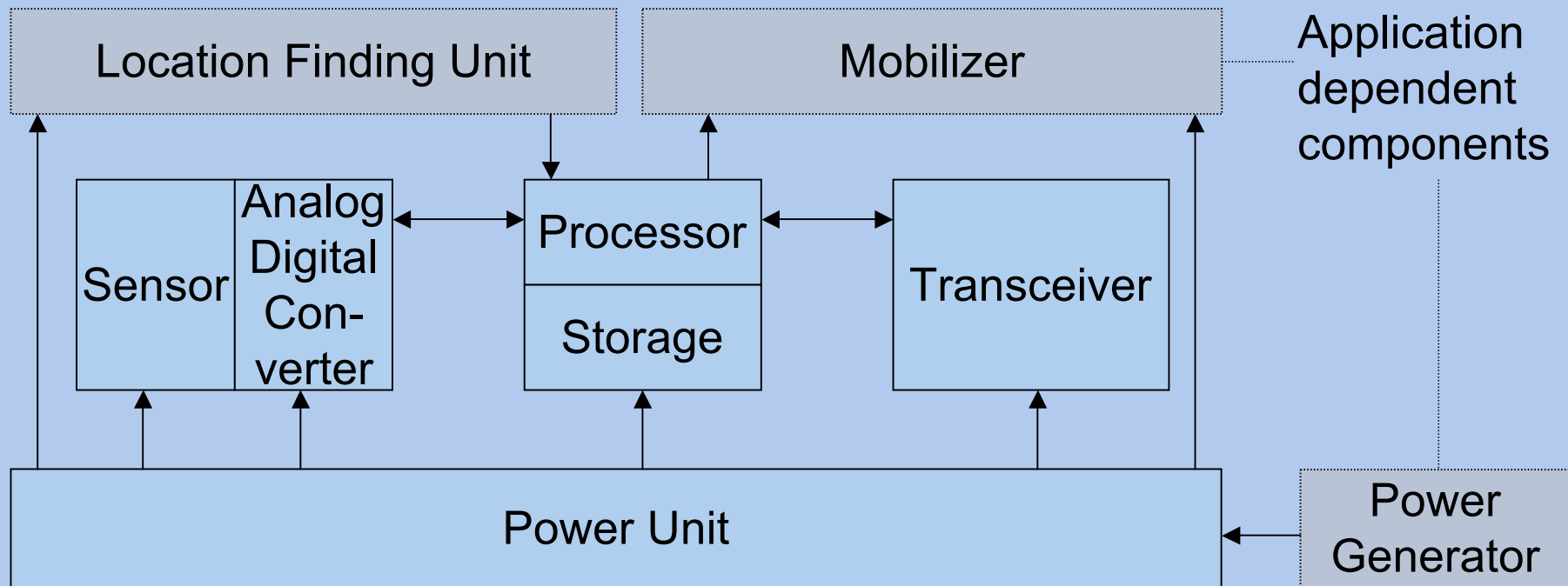
Overview

- > Introduction
 - Ubiquitous Computing
 - Sensor Node Architecture
 - Sensor Hardware
 - Sensing Parameters
- > Wireless Sensor Networks
 - Definition: Sensor Network
 - Wireless Sensor Network Structure
 - Requirements
 - Challenges
 - Energy Issues
 - Applications
 - Protocol Stack
 - Management & Middleware
- > Security and Privacy
 - Security Related Properties in Wireless Sensor Networks
 - Cell-based Sensor Networks
 - Ad Hoc Sensor Networks
- > Conclusions and Outlook
- > Sensor Access via Internet

Ubiquitous Computing

- > Vision defined by Mark Weiser in 1991
 - Seamless integration of computers into the world at large
 - PCs will disappear, become invisible, and will be replaced by intelligent things.
 - Many computers per person
- > Sensors and actuators as key technology
 - Advancements in Micro-Electro-Mechanical System (MEMS) technology allows integration of sensors, transmission units, and CMOS building blocks on a chip.
 - Current size is determined by battery size, but is expected to be in the cm and mm range within a few years.

Sensor Node Architecture



Sensor Hardware

ESB		tmote			
Flash memory (kB)	60	48	128	128	
RAM (kB)	1	4	4	10	
Supported operating systems	TinyOS Contiki	TinyOS Contiki	TinyOS	TinyOS	
Sleep (mW)	0.023	0.015	9.9	0.048	
CPU on, Radio off	28.1	5.4	39.6	36	
CPU on, Radio listen	52.8	65.4	82.5	95.1	
CPU on, Radio rx/tx	57.2	58.5	102.3	88.2	

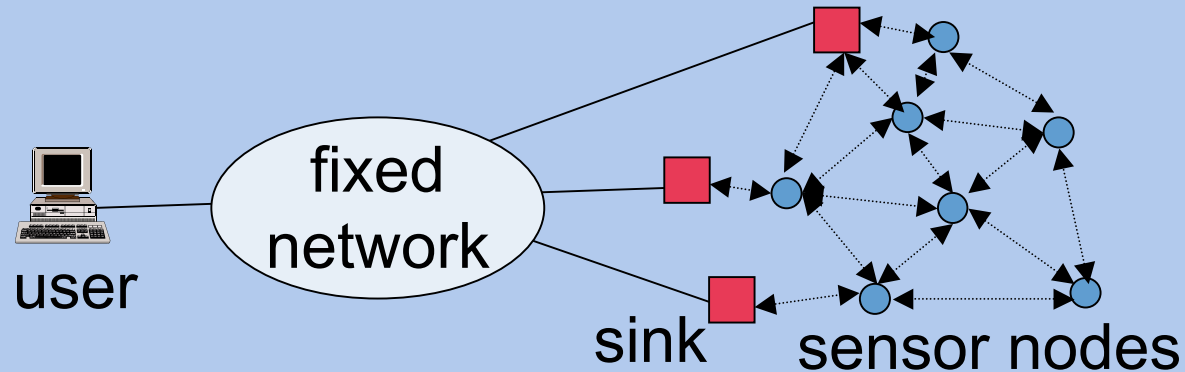
Sensing Parameters

- > Pressure
- > Humidity
- > Temperature
- > Light
- > Chemicals
- > Strain and tilt
- > Speed and acceleration
- > Magnetic fields
- > Vibrations
- > Motion
- > Metal detection
- > Sound
- > ...

Definition: Sensor Network

- > A **sensor network** is a deployment of massive numbers of small, inexpensive, self-powered devices that can sense, compute, and communicate with other devices for the purpose of gathering local information to make global decisions about a physical environment.
- > Source: SmartDust program sponsored by DARPA

Wireless Sensor Network (WSN) Structure



- > Sink
 - is a (mobile) gateway between fixed and wireless sensor network
 - controls and manages (mobile) sensor nodes on behalf of a user
- > Sensor data from sensor nodes to sink by multi-hop communication and data aggregation
- > Broadcast / multicast communication from sink to sensors

Requirements

- > Long network lifetime
- > Low costs
- > Wide area availability
- > Fault tolerance
- > Scalability
- > Security
- > Quality-of-Service (delay and data throughput)
- > Programmability and maintainability



from: Talzi et al.: PermaSense: Investigating Permafrost with a WSN in the Swiss Alps, 4th Workshop on Embedded Networked Sensors, Cork, 25-26 June 07

Challenges

- > Finite energy resources → energy-efficient operation
 - > Limited processing, communication, and storage capabilities
→ in-network processing
 - > High degree of uncertainty → redundancy
 - > Importance of time and location of events
→ synchronization and localization
 - > Untethered/unattended operation of sensors and dynamic structures due to
 - sleep cycles
 - node failures, unreliable nodes
 - energy depletion
 - varying workload, e.g. by simultaneous related events
 - mobility of sensors, targets, and observers
 - changing environmental conditions
 - ...
- self-configuration capabilities

Energy Issues

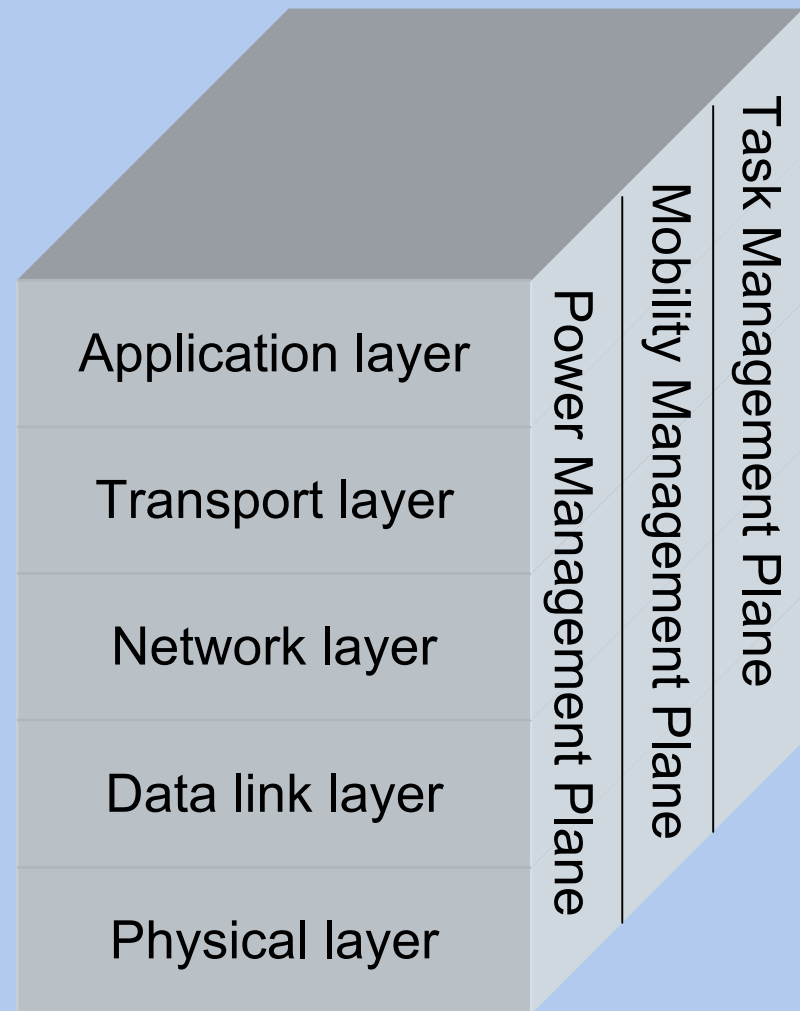
- > Energy is the main concern in wireless sensor networks.
- > Energy sources: batteries, fuel cells, scavenging
- > Battery-driven sensors can not be recharged and become useless after depletion.
- > Communication
 - Tradeoff between processing and communication:
Transmission of 1 bit costs same energy as 100-1000 instructions.
 - 1 nJ per instruction / sample
 - Bluetooth: 100 nJ per bit for a distance of 10 – 100 m
 - Transmission and reception costs are nearly the same.
 - Overhearing is relatively expensive.

Applications

- > Military and security applications
- > Disaster detection / recovery and emergency response
- > Supply chain management and asset tracking
- > Industrial, environmental and agricultural monitoring
- > Habitat and building monitoring / surveillance
- > Animal tracking
- > Education
- > Medical applications: medical monitoring and micro-surgery
- > Traffic and vehicle control, telematics
- > Location and context-sensitive computing
- > Home automation and consumer electronics

Protocol Stack

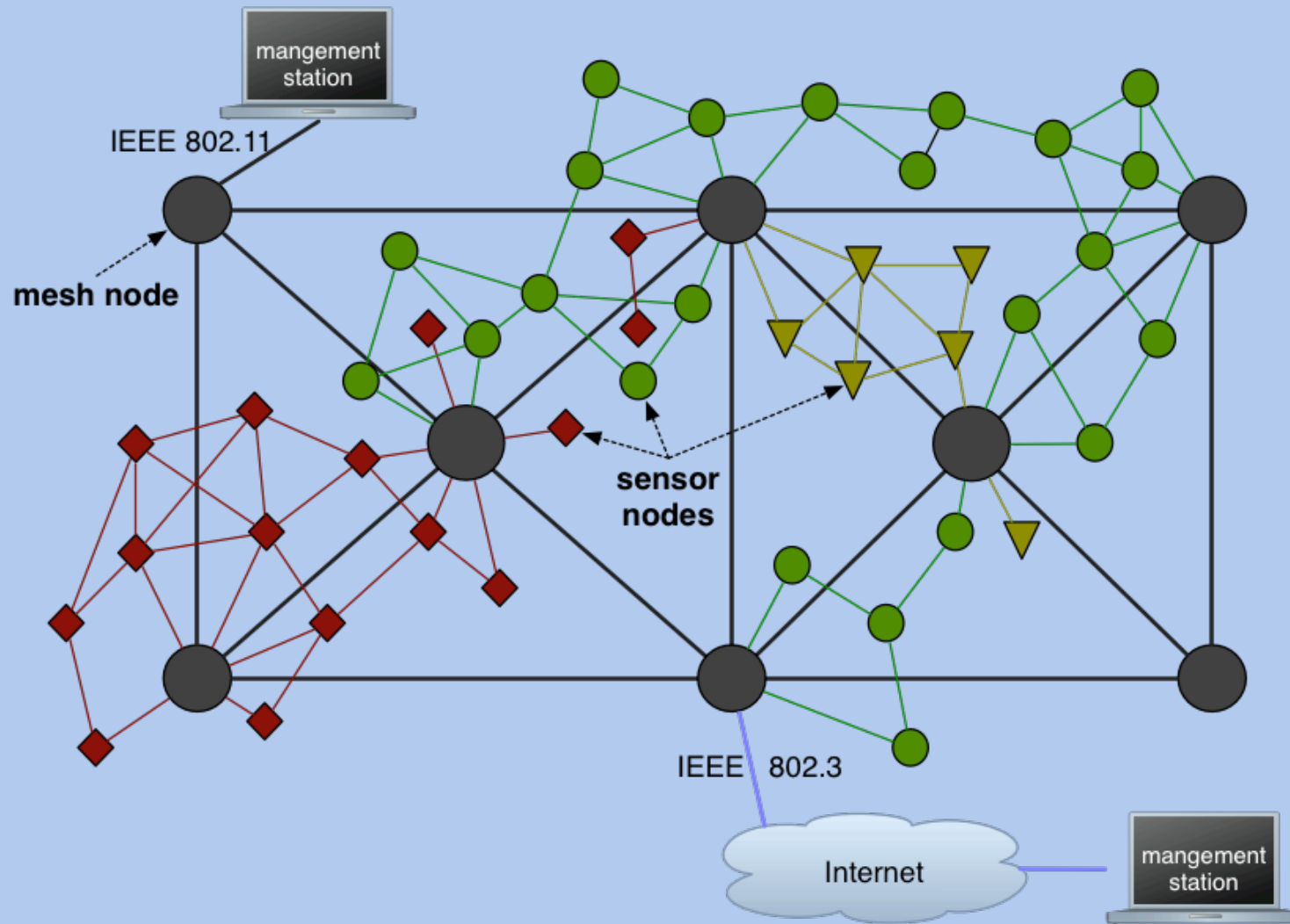
- > Layers
 - **Application**: application software
 - **Transport**: maintain data flow, reliability and congestion control
 - **Network**: routing and topology control
 - **MAC**: fixed and random channel allocation, power awareness, collision avoidance
 - **Physical**: robust modulation, transmission, and reception techniques
- > Management Planes
 - **Power**: management of power usage by a node
 - **Mobility**: detection / registration of sensor movements and neighbors
 - **Task**: balancing and scheduling of sensing tasks in a region



WSN Management and Middleware

- > Dynamic structures require dynamic (re)configuration of sensor nodes
- > Dynamic configuration and code download / installation
 - Traditional network management approaches
 - Database Model: sensor network = distributed data base
 - Active Sensor Model (abstraction of run-time environment by virtual machines or script interpreters to support heterogeneous platforms and code efficiency)
 - Active networks and mobile agents

WSN Management with Wireless Mesh Networks



Security and Privacy

- > Threats to sensor nodes
 - Passive information gathering
 - Traffic analysis
 - Capturing and compromising of nodes, e.g., disclosure of cryptographic information
 - False or malfunctioning nodes, e.g., generation of false data or block routing, and node outage
 - Message corruption
 - Denial of service attacks, e.g., jamming or resource exhaustion, can happen on all layers of the communication system.
- > Privacy Issues
 - Sensor information (about humans) should not be accessible by everyone.
- > Challenge
 - Established security mechanisms require significant computing and communication resources

Security Related Properties in WSNs

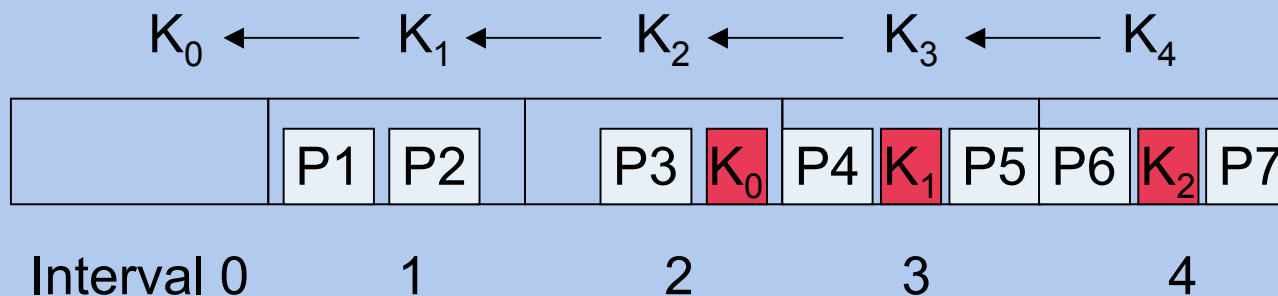
- > Limited memory and computing power → limited set of security protocols
 - Asymmetric encryption is usually not feasible, because of large variables (> 1000 bits) for cryptographic algorithms
 - Energy consumption for 1024 bits on a MC68328 processor: 0.104 mJ (AES) vs. 42 mJ (RSA)
 - Asymmetric digital signatures for authentication cause high overhead (~ 50 – 1000 bytes per packet)
- > Large number of nodes → scalability
- > Hostile environment → difficult physical protection
- > In-network processing
 - use of end-to-end security mechanisms and protocols is prohibited
- > Application-specific software and hardware architectures
 - adaptation of security mechanisms to application needs

Cell-based Wireless Sensor Networks

- > Base station (sink) with more resources and running more sophisticated protocols / algorithms
- > Base station represents a trust base that can not be compromised easily.
→ safe bootstrapping and configuration
- > Access control in base stations to control access by external users.
- > Nodes can still be compromised or malicious nodes can be added.
- > Example: SPINS (Security Protocols for Sensor Networks) protocol suite
 - Sensor Network Encryption Protocol (SNEP)
 - for secure unicast communication between base stations and sensor nodes avoids use of initialization vectors by counters and counter synchronization protocol
 - μ TESLA for authenticated data broadcast
 - Basic idea: delayed disclosure of symmetric keys for (delayed) authentication
 - Operation
 - Packet transmission: Base station broadcasts message with a MAC using symmetric key that is secret at this point of time.
 - Packet reception: Receiver detects that authentication key has not yet been disclosed and can not verify the message authentication.
 - Key disclosure: Base station broadcasts verification key to all receivers, which can then authenticate stored packets.

μTESLA

- > Sender chooses key K_n and applies public one-way function F to all other keys: $K_i = F(K_{i+1})$
- > Division of time into intervals and usage of a single authentication key during a time interval.
- > Broadcasts of disclosed keys are redundant:
A receiver lacking keys K_0 and K_1 reconstructs these after receiving K_2 .
- > Receiver Bootstrapping
 - Receiver needs to have 1 authentic K_i from the chain to authenticate K_{i+1} by verifying $K_i = F(K_{i+1})$. Subsequent keys are self-authenticating !
- > Key disclosure delay δ is in the order of some time intervals.



Ad Hoc Sensor Networks

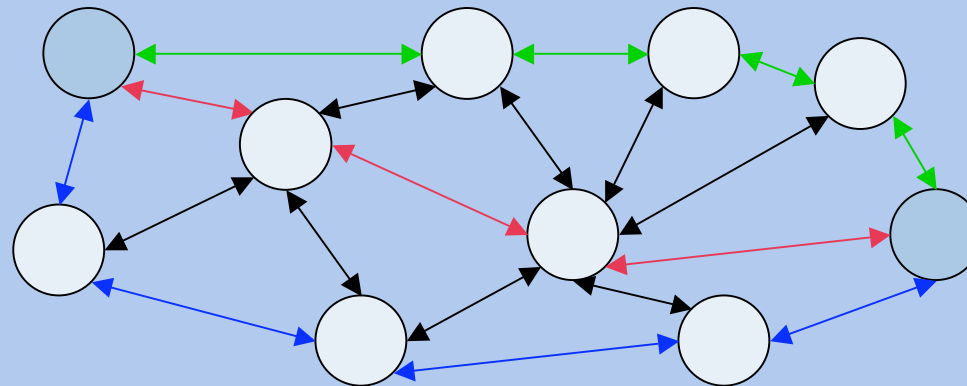
- > Symmetric keys are preferred over asymmetric keys.
- > Lack of trusted base station for key management
- > Algorithms for ad hoc sensor networks are typically based on pre-deployment of keys, because key servers are physically exposed.
- > Extreme options
 - One key for the whole sensor network
 - compromised node can decrypt all messages.
 - One key for each pair of nodes → scalability concerns
 - Approach: (random) key pre-distribution

Key Pre-Distribution and Shared Key Discovery

- > Key pre-distribution
 - Before deployment: generation of a pool of P keys.
 - k ($\ll P$) keys are selected for each node \rightarrow key ring
 - If a node gets compromised, the probability for decrypting a message is k/P .
- > Shared key discovery
 - Two nodes intending to communicate with each other exchange information (key identifiers) about available keys. If they find a common key, they can use it for direct communication.
 - Result of this phase: topology of connected nodes
 - If two nodes do not share a common key
 - \rightarrow path-key establishment

Path-Key Establishment

- > Nodes that do not share a common key, can establish a key via a **secured path**, possibly using keys that have not yet been assigned.
- > Problem: intermediate nodes know key and attacker can get the knowledge too by subverting a single node
- > Approach: Multi-path Key Establishment, $k = k_1 \oplus k_2 \oplus \dots \oplus k_n$
- > Problem: finding disjoint paths



Conclusions and Outlook

- > Manifold opportunities with wireless sensor networks
- > Deployment is slowly emerging.
- > Technology needs to make further progress.
- > Many research challenges remain, see also www.mics.ch
(Swiss National Competence Centre in Research on Mobile Information and Communication Systems)

Sensor Access via Internet

