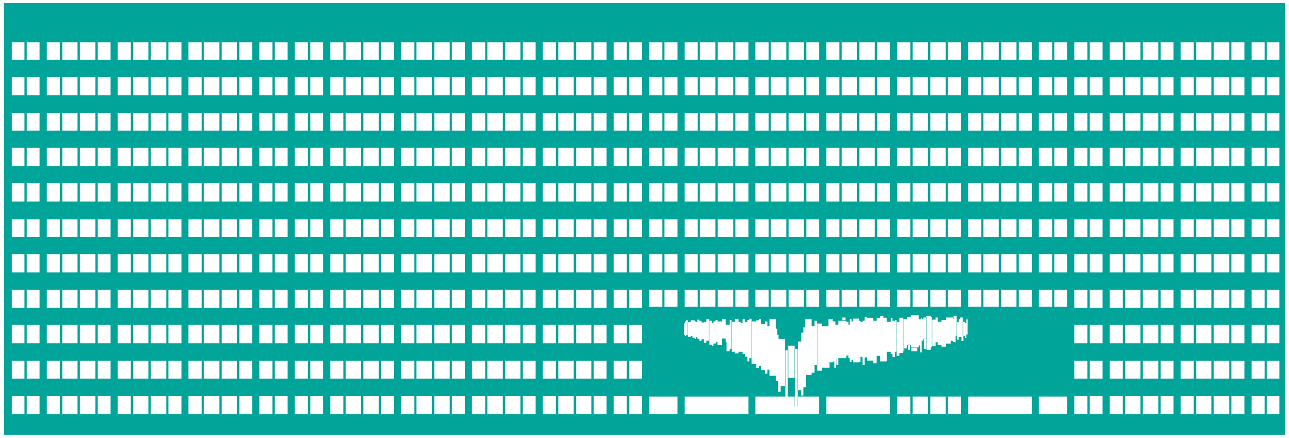
VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

Mesh networks
Sensor networks



MS (Mobile Computing)
Lecture 10

Mesh networking

- Each node in the network may act as an independent router (even if not connected to other networks)
- All nodes interconnected → full mesh
- Mobile ad hoc networks (MANET) – self-configuring network of mobile devices connected by wireless links
  - Internet Based Mobile Ad hoc Networks (iMANET)
  - Vehicular Ad Hoc Networks (VANETs)
  - Intelligent VANET (InVANETs)
- Self-healing – network can operate when one node fails.
- Wireless mesh networks – most common solution

Wireless mesh networks

- Originally developed for military applications
- Router network of wireless nodes
- Signal strength limitation avoided by breaking long distances into sequences of shorter hops
  - Forwarding decisions based on network topology instead of simple signal boosting
- Typical uses of WMNs
  - Infrastructure WMNs – clients connected to them
  - Client WMNs – clients interconnected, routing on clients
  - Hybrid WMNs – clients ↔ clients, clients ↔ network
- Relatively stable topology

WiFi + Wireless mesh

- Originally no support in 802.11 (802.11s, superseded by 802.11-2012)
- Outdoor wireless network solution
  - Combines 2.4 and 5 GHz bands
  - 5 GHz Wireless distribution system & 2.4 GHz hot-spots (ad-hoc network)
- Roof-top APs (RAP) and Mesh APs (MAP)
- Traffic may be bridged into wired infrastructure by RAP or tunneled to a WLAN controller
- Path over the wireless mesh is determined using a special protocol
  - Adaptive Wireless Path protocol
  - Hybrid Wireless Mesh Protocol (HWMP) – IEEE 802.11s

Routing in ad-hoc networks

- Pro-active routing – distributes routing tables through the network – overhead, slow convergence
- Reactive routing – on-demand route by flooding the network with route request packets – high latency, slowing down the network with requests
- Flow-oriented routing – follows existing flows in network to discover routes – long time for new routes, may be locked-in by existing traffic
- Adaptive routing, Hybrid routing – combine pro-active & reactive routing, based on current situation
- Hierarchical routing, Host-specific routing, Geographical routing, Power-aware routing; Multicast routing, …

Wireless mesh routing protocols

- Optimized **Link State** Routing Protocol (OLSR)
  - optimized for mobile ad-hoc networks
  - packets can and do go out the same interface
  - 2-hop neighbor information & distributed election of a set of multipoint relays (MPRs) – relaying & route sel.
  - limited reliability, no link quality checking in ver. 1
- Better Approach To Mobile Adhoc Networking - B.A.T.M.A.N. – Freifunk(.de) community
  - decentralization, directions of incoming data, dynamic routes, high levels of stability but slow convergence
  - detects other B.A.T.M.A.N. nodes and finds the best way to them. Multiple versions (v1-v3)
- AODV & OORP: MANET, Destination-Sequenced DV, TORA, ...

Wireless sensor networks

Spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions.

- Evolution: Military use → disaster relief → industrial process monitoring and control → machine health → human health → environment monitoring → home automation
- Monitored values: Temperature, humidity, vibrations, pressure, vehicular movement, lightning, noise, general telemetry data, …
- Node sizes: grain of dust → shoebox (typically must fit a matchbox-sized module).
- Node cost: ~ 1 cent → hundreds USD (typically ~$10)

WSN versus Ad-hoc network

- Number of sensor nodes in a sensor network can be several orders of magnitude higher than in AH network.
- Sensor nodes are densely deployed
- Sensor nodes are prone to failures
- Topology of a sensor network frequently changes
- Sensor nodes mainly use broadcasts whilst most ad hoc networks are based on point-to-point communications.
- Sensor nodes are limited in power, computational capacities, and memory.
- Sensor nodes may not have global identification (ID) - large amount of overhead and large number of sensors.

Wireless sensor node

- Each node in a sensor network typically contains
  - radio transceiver or other wireless communications device
  - sensing unit
  - processing unit (small microcontroller)
  - energy source (typically battery)
- Additional components are typically
  - location finding system
  - power generator
  - mobilizer – sensor node movement

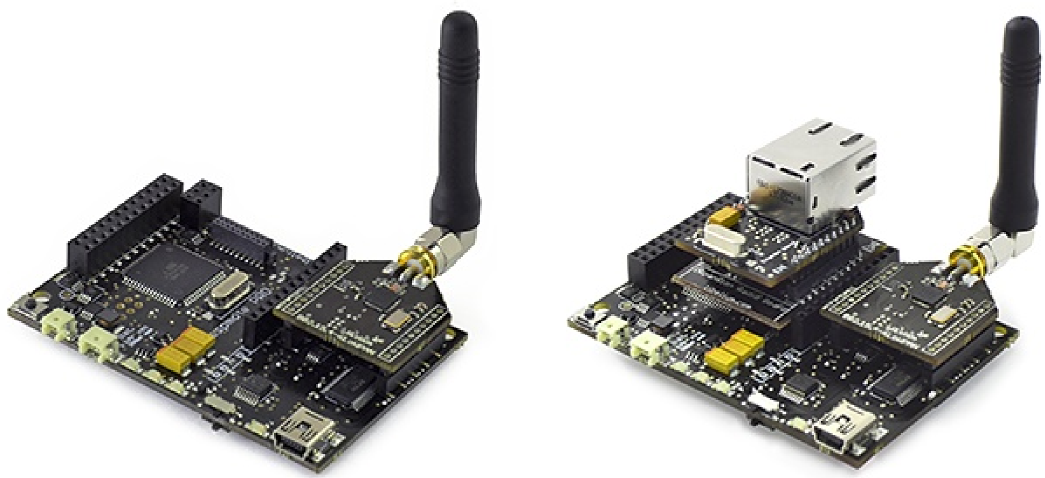
Sensor node properties

- Sensor nodes must
  - consume extremely low power e.g. ~ 30 μA
  - operate in high volumetric densities
  - have low production cost (< $1) and be dispensable
  - be autonomous and operate unattended
  - be adaptive to the environment
- Example of wireless sensor nodes
  - smart dust mote prototype: 4 MHz Atmel micro-controller with 8 kB instruction flash memory, 512 bytes RAM and 512 bytes EEPROM. TinyOS - 3500 B OS & 4500 B code
  - μAMPS wireless sensor node: 59–206 MHz SA-1110, multithreaded μ-OS

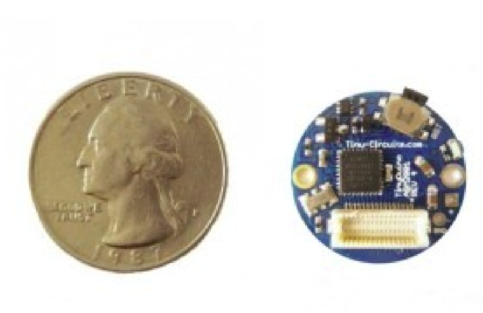
Unique properties of WSN

- Limited power they can harvest or store
- Can withstand harsh environmental conditions
- Must cope with node failures
- Mobility of nodes
- Dynamically-created network topology
- Unattended operation
- Communication failures
- Nodes can be heterogeneous
- Large scale of deployment
- Scalable node capacity, limited by BW of gateway node

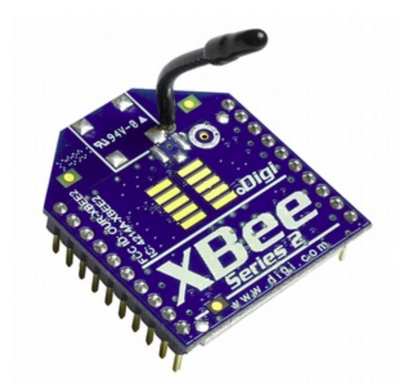
WSN Node Examples



Waspmote Mote Runner node (left) and gateway (right)



TinyDuino



ZigBee

WSN network architecture

- Besides L1-L4,L7 layers, the protocol stack contains 3 following planes:
  - Power management – manages how a sensor node uses its power (e.g. turning off radio after receiving to prevent duplicate messages, disabling routing function on low power, …)
  - Mobility management – detects & registers movement of sensor nodes → route back to the user is always maintained. Sensor nodes can keep track of who are their neighbor sensor nodes
  - Task management – balances & schedules sensing tasks in specific region (not all sensor nodes in the region are required to perform sensing at the same time → sensor nodes with more power perform the task more

Sensor management protocol

- Application-layer protocol
- Management protocol providing software operations needed to perform following administrative tasks:
  - introducing rules related to data aggregation, attribute-based naming and clustering to the sensor nodes,
  - exchange of data related to the location finding
  - time synchronization of the sensor nodes
  - movement of sensor nodes
  - turning sensor nodes on and off
  - querying sensor network configuration & nodes status + re-configuring the sensor network
  - authentication, key distribution and security for comm.

Software of WSNs

- Algorithms and protocols need to
  - maximize the lifetime
  - be robust and fault-tolerant
  - be able to self-configure the WSN
- Distributed algorithms
- Energy-constrained → energy-aware algorithms
- Multi-hop data transfer
- WSN simulators – network simulators
  - TOSSIM – TinyOS, COOJA – Contiki
  - JSim – Java-based, platform-independent
  - WSNSim – C#, VS 2008, …

Operating systems for WSNs

- Less complex than normal OS, prepared for resource-limited environment
  - eCos, μC/OS – originally for embedded systems, RTOS function may not be required for WSN environment
  - TinyOS – event-driven programming, non-blocking, asynchronous I/O, handlers & tasks – run to completion nesC extension of C, race condition detection between tasks and event handlers.
  - C-programming based OS:
    - Contiki – ELF binaries, module loading over network, event-driven, multithreading, protothreads – low overhead
    - MANTIS, Nano-RK – pre-emptive multithreading, Nano-RK real-time resource kernel – fine control of task access to CPU time, networking and sensors.
    - LiteOS – RTOS, UNIX-like abstraction – cp (data), ls

WSN applications (1)

- Military (C4ISRT) – dense deployment of low-cost disposable nodes (artillery shell, …)
  - OPFOR, friendly force and battlefield monitoring
  - Targeting – guiding systems of intelligent ammunition
  - Battle damage assessment
  - Non-conventional attack detection
- Environmental applications – sensors in the wild
  - Forest fire detection, flood detection, landslide, …
  - Biocomplexity monitoring
  - Permafrost in Alps
- Health monitoring – drug administration, telemonitoring of human physiological data, tracking doctors & patients

WSN applications (2)

- Home applications
  - Home automation – sensor nodes in domestic devices
  - Smart environment
    - Human-centered – adaptation to user needs (I/O capabilities)
    - Technology-centered – new HW, networking technologies, example: room server, intelligent furniture with different capabilities & services – e.g. printing, scanning, and faxing
- Building applications
  - Environmental control in office buildings
  - Interactive museums – objects in museums reacting on touch & speech, cause-effect, paging, localization
- Industrial applications
  - Machine health monitoring – less cables, inaccessible locations

WSN applications (3)

- Other commercial applications
  - Fleet monitoring / Vehicle tracking and detection
    - Mote with a GPS module on-board of each vehicle of a fleet, gathering position & reporting its coordinates so that the location is tracked in real-time (GSM & other localization technologies when no GPS signal)
    - Line of bearing of the vehicle is determined locally within the clusters and then it is forwarded to the base station, or the raw data collected by the sensor nodes are forwarded to the base station to determine the location of the vehicle.
  - Managing inventory control
    - Each item in a warehouse may have a sensor node attached. The end users can find out the exact location of the item and tally the number of items in the same category
  - Water/Wastewater Monitoring