CSC 498R: Internet of Things

Lecture 05: Wireless Sensor Networks

Instructor: Haidar M. Harmanani

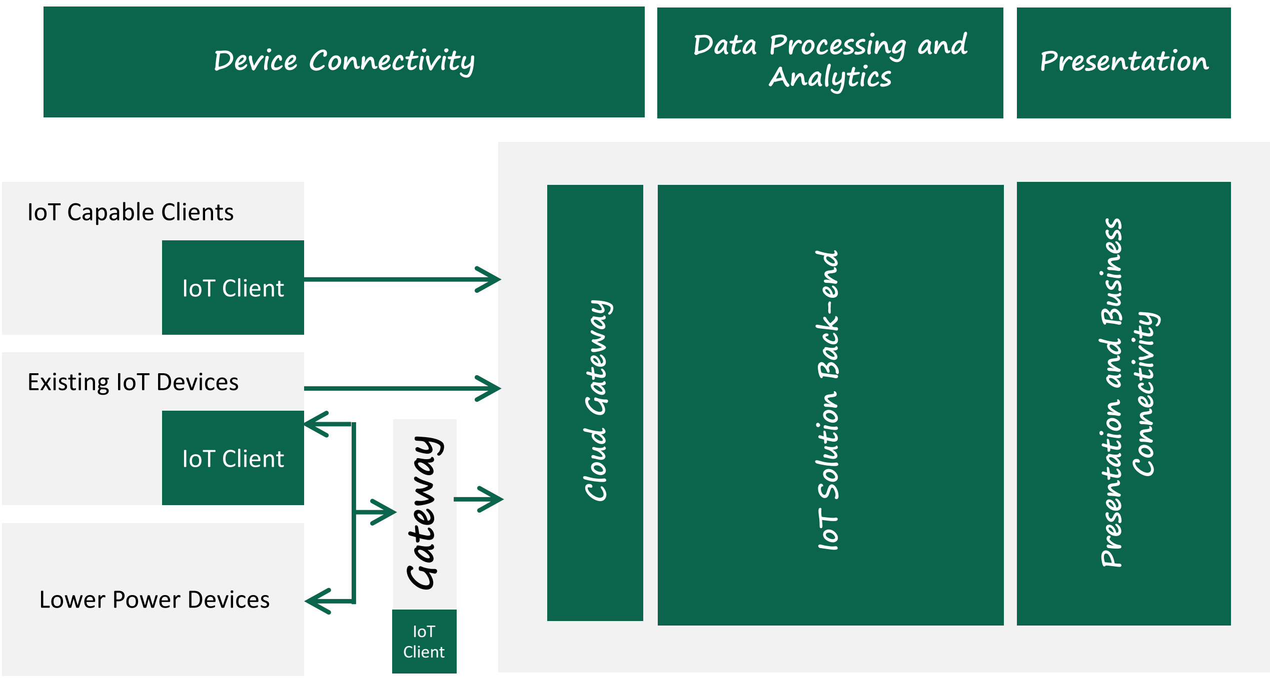
Fall 2017

Topics

- Wireless Sensor Networks

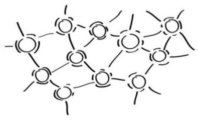
Recall: IoT Definitions

- The *Internet of Things* is a system of physical objects that can be discovered, or interacted with by electronic devices that communicate over various networking interfaces and eventually can be connected to the wider internet.
- A *Thing* may be:
  - A *sensor* or *actuator*
  - Able to execute computations and or communicate over wired or wireless interfaces.
  - *Tagged* (*passive*) or *active*



IoT Components

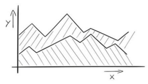
- Things we connect: **Hardware, sensors *and* actuators**



- Connectivity
  – Medium we use to connect things

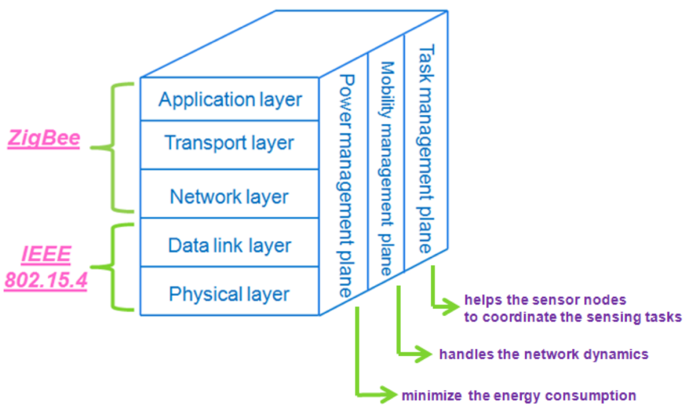
- Platform
  – Processing and storing collected data
    - Receive and send data via standardized interfaces or API
    - Store the data
    - Process the data.

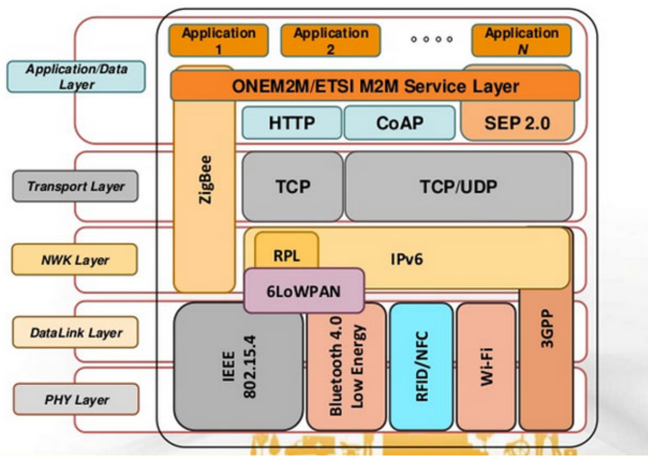
- Analytics
  – Get insights from gathered data



- User Interface

Lecture Context





IoT Network Architecture: Autonomous Network Architecture

- Autonomous networks are not connected to public networks
  - Internet access is possible via a gateway, if needed.
- An IP protocol suite is commonly adopted due to its scalability and flexibility.
- The large address capacity provided by IPv6 is required in most cases.

Example: Autonomous information collected by the parking sensor due to the occupancy of parking slots in a wireless manner and sent to the control center.

An Autonomous System (AS) is a collection of routers whose prefixes and routing policies are under common administrative control. This could be a network service provider, a large company, a university, a division of a company, or a group of companies.

Definition: Autonomous Systems

IoT Network Architecture: Ubiquitous Network Architecture

- Smart objects or "things" network are part of the Internet
  - Using the internet gateway, authorized users will have access to the information provided by smart objects networks, either directly fetching from the device or by means of intermediate servers.
  - The servers act as a sink to collect data from each object.

IoT Network Architecture: Ubiquitous Network Architecture

- Features
  - Multitier: The network architecture is hierarchical, comprised of both multi-access networks and wireless multi-hop networks.
  - Multiradio: It is not uncommon to have a number of radio access technologies available to connect to the internet, either covering the same or complimenting geographical areas
    - Networks could be WLAN, WiMAX, macro-cellular, femto-cellular or even ad-hoc.
    - The synergy and integration of multiple networks in multi-access and multi-operator environment introduces new opportunities for better communication channels and an enhanced quality of provided applications and services.

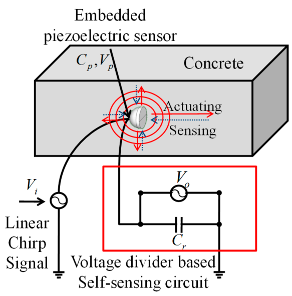
Monitoring the health of any structure, large or small, like buildings, bridges and so on.

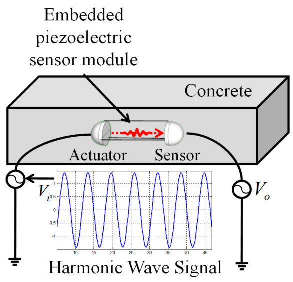
- Passive wireless sensors are embedded within a concrete structure that sends radio signals of suitable amplitude and phase characteristics periodically using radio frequencies.
- The data collected from these sensors are then analyzed to detect anomalies.

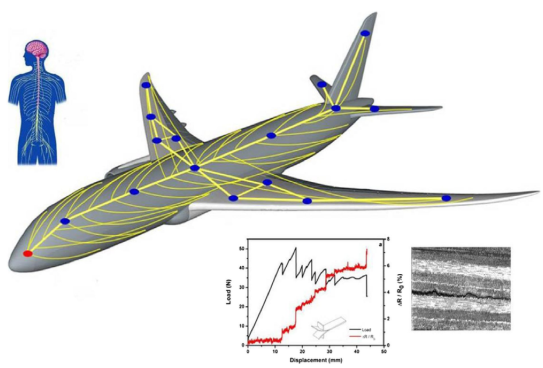
Ubiquitous Network Architecture: Structural Health Monitoring Example

Piezoelectric sensors

- *Piezoelectric sensors are used* in order to measure changes in pressure, acceleration, temperature, strain, or force by converting them to an electrical charge.







Wireless Sensor Networks (WSN)

- Spatially deploy distributed autonomous sensors
- May incorporate a gateway that provides wireless connectivity back to the wired world and distributed nodes

Roles of participants in WSN

- Sources of data: Measure data, report them "somewhere"
  - Typically equip with different kinds of actual sensors
- Sinks of data: Interested in receiving data from WSN
  - May be part of the WSN or external entity, PDA, gateway, …
- Actuators: Control some device based on data, usually also a sink

Examples

- Facility management
  - Intrusion detection into industrial sites
  - Control of leakages in chemical plants, …
- Machine surveillance and preventive maintenance
  - Embed sensing/control functions into places no cable has gone before
  - E.g., tire pressure monitoring
- Precision agriculture
  - Bring out fertilizer/pesticides/irrigation only where needed
- Medicine and health care
  - Post-operative or intensive care
  - Long-term surveillance of chronically ill patients or the elderly

More Examples

- Logistics
  - Equip goods (parcels, containers) with a sensor node
  - Track their whereabouts – total asset management
  - Note: passive readout might suffice – compare RF IDs
- Telematics
  - Provide better traffic control by obtaining finer-grained information about traffic conditions
  - Intelligent roadside
    - Cars as the sensor nodes

Structuring WSN application types

- Interaction patterns between sources and sinks classify application types
  - Event detection: Nodes locally detect events (maybe jointly with nearby neighbors), report these events to interested sinks
    - Event classification additional option
  - Periodic measurement
  - Function approximation: Use sensor network to approximate a function of space and/or time (e.g., temperature map)
  - Edge detection: Find edges (or other structures) in such a function (e.g., where is the zero degree border line?)
  - Tracking: Report (or at least, know) position of an observed intruder

Deployment options for WSN

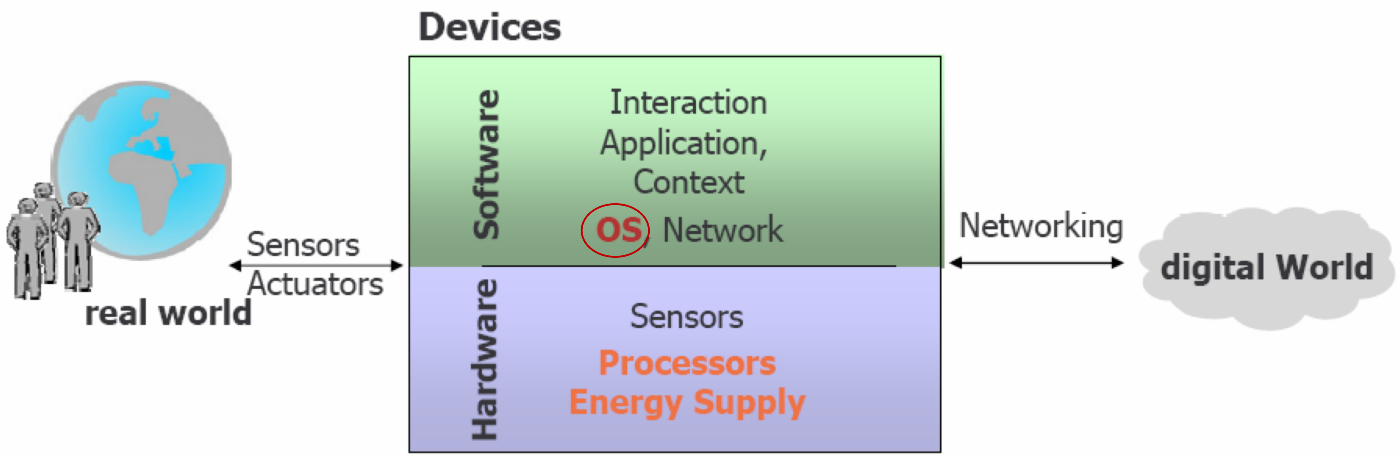
- How are sensor nodes deployed in their environment?
  - Random deployment: Dropped from aircraft
    - Usually uniform random distribution for nodes over finite area is assumed
    - Is that a likely proposition?
  - Regular deployment : Well planned, fixed
    - E.g., in preventive maintenance or similar
    - Not necessarily geometric structure, but that is often a convenient assumption
  - Mobile sensor nodes
    - Can move to compensate for deployment shortcomings
    - Can be passively moved around by some external force (wind, water)
    - Can actively seek out "interesting" areas

Maintenance Options

- Feasible and/or practical to maintain sensor nodes?
  - E.g., to replace batteries?
  - Or: unattended operation?
  - Impossible but not relevant? Mission lifetime might be very small
- Energy supply?
  - Limited from point of deployment?
  - Some form of recharging, energy scavenging from environment?
  - E.g., solar cells

Sensor and Actuators

- A sensor is a device that measures a physical quantity and converts it into a signal which can be read by an observer or by an instrument
- An actuator is a device for moving/controlling a mechanism/system, or generate some output, e.g., motor, LED, buzzer, speaker, etc.



Sensors and Actuators are Bridges Between Real and Digital Worlds

Sensor Networks

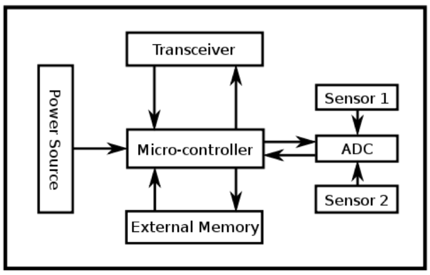
- A sensor network (SN) consists of multiple interconnected sensors or *motes*
- Combine sensing, communication and computation into a complete architecture
  - Possible by advances in low power wireless communication technology
  - MEMS brings a rich array of cheap, tiny sensors
- See https://www.youtube.com/watch?v=urWv-_EqS9M for a good tutorial!

Sensor Nodes

- Processor in various modes (sleep, idle, active)
- Power source (AA or Coin batteries, Solar Panels)
- Memory used for the program code and for in-memory buffering
- Radio used for transmitting the acquired data to some storage site
- Sensors for temperature, humidity, light, etc

Sensor Nodes

- A sensor node, also called a mote, is a WSN node that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the WSN



Wireless Sensor Networks

- A self-configuring network of small sensor nodes communicating among themselves using radio signals, and deployed in quantity to sense, monitor and understand the physical world.
  – Coordinate to perform a common task.
- Prolonging network lifetime is a critical issue.
- Sensors often have long period between transmissions (e.g., in seconds).

Wireless Communication

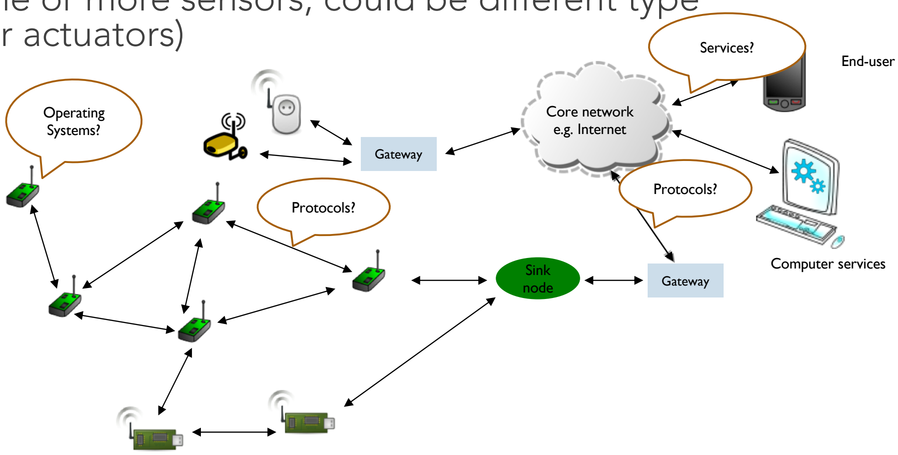
- The two wireless standards used by WSN are *802.15.4* and *Zigbee*
  – They are low-power protocols
  – Performance is an issue
  – Max distance is around 100 m

Wireless Sensor Networks

- Another attribute is scalability and adaptability to change in network size, node density and topology.
  - In general, nodes can die, join later or be mobile.
- Often high bandwidth is not important.
- Nodes can take advantage of short-range, multi-hop communication to conserve energy.

Wireless Sensor (and Actuator) Networks

- The networks typically run *Low Power Devices*
- Consist of one or more sensors, could be different type of sensors (or actuators)



A good WSN MAC protocol needs to be energy efficient.

Wireless Sensor Networks

- Sources of energy waste:
  - Idle listening, collisions, overhearing and control overhead and overmitting.
  - Idle listening dominates (measurements show idle listening consumes between 50-100% of the energy required for receiving.)
- Idle listening
  - Listen to receive possible traffic that is not sent.
- Overmitting
  - Transmission of message when receiver is not ready.

Wireless Sensor Networks Characteristics

Limited power they can harvest or store

Ability to withstand harsh environmental conditions

Ability to cope with node failures

Mobility of nodes

Dynamic network topology

Communication failures

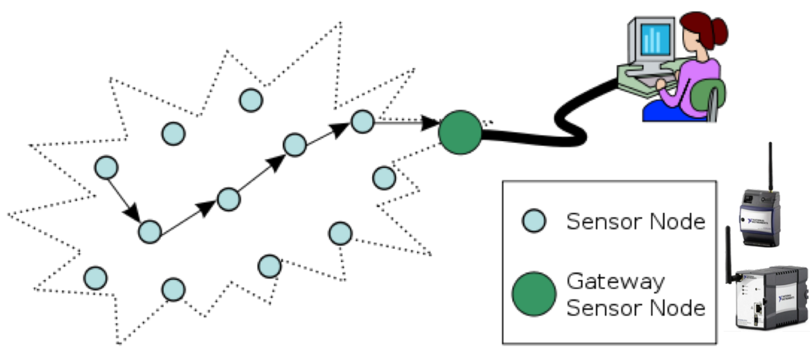
Heterogeneity of nodes

Large scale of deployment

Unattended operation

Nodes are scalable, only limited by bandwidth of gateway node

Typical WSN Architecture



A sensor network normally constitutes a wireless ad-hoc network, and each sensor supports a multi-hop routing algorithm where nodes function as forwarders, relaying data packets to a base station.

WSN Communication Patterns

- Broadcast
  - Base station transmits to all sensor nodes in WSN.
- Multicast
  - Sensor transmit to a subset of sensors (e.g. cluster head to cluster nodes)
- ConvergeCast
  - Data is collected from outlying nodes through a direct spanning tree to the root (BS, cluster head, or data fusion center).
- Local Gossip
  - Sensor sends message to neighbor sensors.

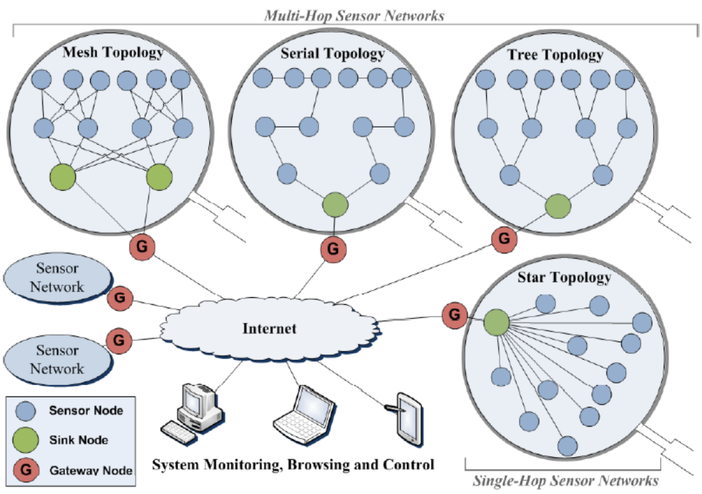
Wireless Sensor Networks

- Central approach:
  - Lower the duty cycle by turning the radio off part of the time.
  - Duty cycle is the ratio between listen time and the full listen-sleep cycle
- Three techniques to reduce the duty cycle:
  - TDMA
  - Scheduled contention periods
  - LPL (Low Power Listening)

Techniques to Reduce Idle Listening

- TDMA requires cluster-based or centralized control.
- Scheduling – ensures short listen period when transmitters and listeners can rendezvous and other periods where nodes sleep (turn off their radios).
- LPL – nodes wake up briefly to check for channel activity without receiving data.
  – If channel is idle, node goes back to sleep.
  – If channel is busy, node stays awake to receive data.
  – A long preamble (longer than poll period) is used to assure than preamble intersects with polls.

WSN Topologies



Tree Routing

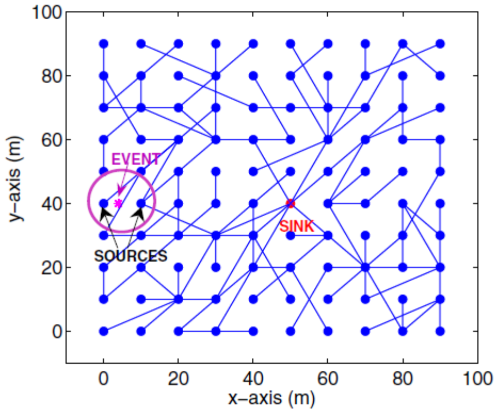


Fig. 1. Simulation scenario: black points represent sensor nodes and edges correspond to *parent-child relationships*

Tiered WSN Architectures

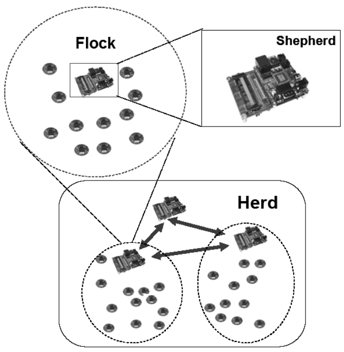


Figure 1: The Mote Herding architecture and its components, the *flock*, the *shepherd* and the *herd*

Group motes into *flocks* that are connected via a multihop network to a microserver acting as a *shepherd*.

Example System: NI WSN-9791 Wireless Sensor Network Ethernet Gateway

- Features
  - 2.4 GHz, IEEE 802.15.4 radio
  - 10/100 Ethernet
  - Connect up to 36 measurement nodes
  - Outdoor range up to 300 m
  - 9 to 30 VDC power input
- Specifications
  - 2U compact form factor
  - Panel or DIN rail mounting
  - Industrial ratings
  - Operating temperature -30 to 70 °C
  - 50 grms shock 5 g vibration
  - Status LEDs

NI WSN-3202 and NI WSN-3212 Wireless Sensor Network Measurement Nodes

- 2.4 GHz IEEE 802.15.4 radio
  - Outdoor range up to 300 m
  - Up to 3-year battery life with 4 AA batteries
    - Optional 9 to 30 VDC power input
- Configurable as a mesh router
- Four bidirectional digital I/O lines
- Industrial ratings
  - Operating temperature -40 to 70 °C
  - 50 grms shock 5 g vibration

Outdoor Enclosure

NI WSN-3202 and NI WSN-3212
Wireless Sensor Network Measurement Nodes

WSN-3202

Analog Input Node for WSN

16-Bit, 4-Channel, ±10 V Analog Input Node for WSN—The WSN-3202 is a wireless device that provides analog input channels and four bidirectional digital channels that you can configure on a per channel basis for input, sinking output, or sourcing output. You can configure the WSN-3202 as a mesh router to increase network distance and connect more nodes to your gateway. You can connect eight end nodes (star topology) or up to 36 measurement nodes (mesh topology) to a single wireless sensor network (WSN) gateway, with an outdoor range up to 300 m with line of sight. The device also offers programmable input ranges to maximize measurement accuracy and industrial temperature and shock and vibration ratings.

The included NI WSN software delivers easy network configuration in Measurement & Automation Explorer (MAX).

- Read Less

NI WSN-3202 and NI WSN-3212
Wireless Sensor Network Measurement Nodes

WSN-3212

Thermocouple Input Node for WSN

4-Channel Thermocouple Input Node for WSN—The WSN-3212 is a wireless device that provides four 24-bit thermocouple input channels and four bidirectional digital channels that you can configure on a per channel basis for input, sinking output, or sourcing output. You can configure the WSN-3212 as a mesh router to increase network distance and connect more nodes to your gateway. You can connect eight end nodes (star topology) or up to 36 measurement nodes (mesh topology) to a single WSN gateway, with outdoor range up to 300 m with line of sight. The device also offers programmable input ranges to maximize measurement accuracy and industrial temperature and shock and vibration ratings.

NI-WSN software delivers easy network configuration and data extraction.

- Read Less

General Features of Sensor Node

- Small Size
  - From few mms to few inches
- Limited processing and communication
  - Mhz clock, MB flash, KB RAM, 100's Kbps bandwidth (wireless)
- Limited power
  - MICA: 7-10 days at full blast
- Failure prone nodes and links
  - Due to deployment, fabrication, wireless medium, …
- Easy to manufacture
- Needs to offset this with scalable and fault-tolerant OS'es and protocols

Power Aware MAC Protocols

- Three approaches to saving power:
  - TDMA: TRAMA, EMACs, L-MAC
  - Schedule: PAMAS, S-MAC, T-MAC, D-MAC, PMAC, SCP-MAC, Crankshaft, AS-MAC
  - Low Power Listening: LPL, B-MAC, WiseMAC, X-MAC
    - Newest approaches include
  - Receiver Initiated: RI-MAC, A-MAC, LPP

Sensor-MAC (S-MAC)

- All nodes periodically listen, sleep and wakeup. Nodes listen and send during the active period and turn off their radios during the sleep period.
- The beginning of the active period is a SYNC period used to accomplish periodic synchronization and remedy clock drift {nodes broadcast SYNC frames}.
- Following the SYNC period, data may be transferred for the remainder of the fixed-length active period using RTS/CTS for unicast transmissions.

Sensor-MAC (S-MAC)

- Long frames are fragmented and transmitted as a burst.
- SMAC controls the duty cycle by trading off energy for delay.
- However, as density of WSN grows, SMAC incurs additional overhead in maintaining neighbors' schedules.

S-MAC

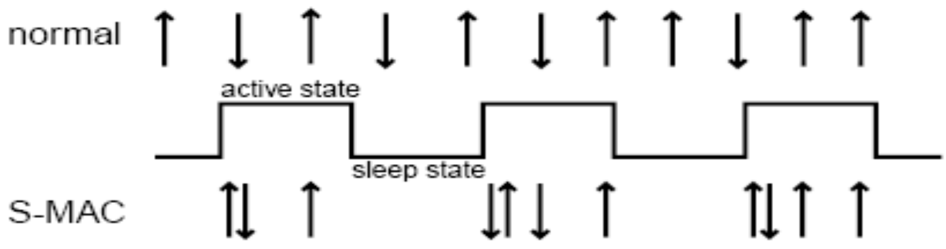


Figure 1: The S-MAC duty cycle; the arrows indicate transmitted and received messages; note that messages come closer together.

Timeout-MAC (T-MAC)

- TMAC employs an adaptive duty cycle by using a very short listening window at the beginning of each active period.
- After the SYNC portion of the active period, RTS/CTS is used in a listening window. If no activity occurs within a timeout interval (15 ms), the node goes to sleep.
- TMAC saves power at the cost of reduced throughput and additional delay.

T-MAC

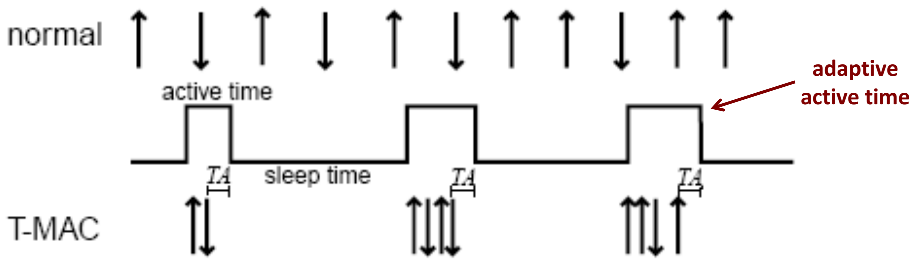


Figure 2: The basic T-MAC protocol scheme, with adaptive active times.

LPL and SCP-MAC

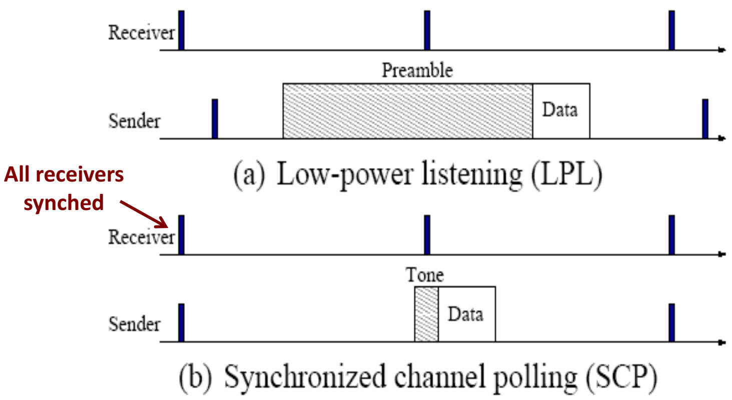


Figure 1. Sender and receiver synchronization schemes.

X-MAC

- X-MAC is an LPL variant that aims to address:
  - Overhearing, excessive preamble and incompatibility with packetizing radios (e.g.,CC2420).
- Uses strobed preambles where preambles contain receiver(s) address information.
- Addresses multiple transmissions to one receiver by having subsequent transmitters view the ACK, back-off and then send without any preamble.

X-MAC

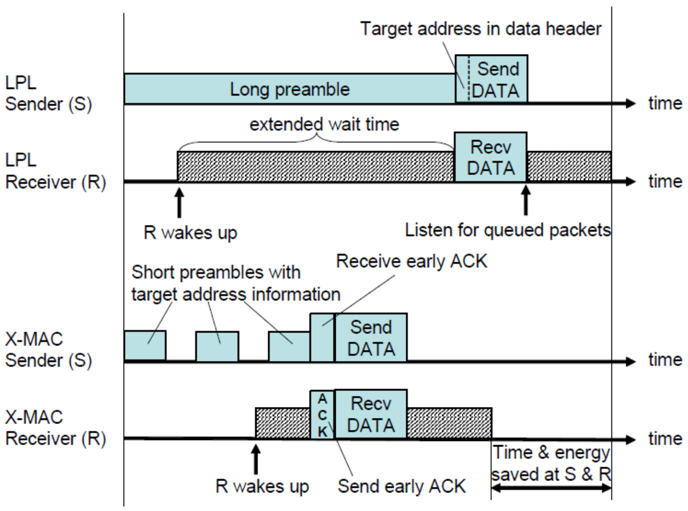


Figure 1. Comparison of the timelines between LPL's extended preamble and X-MAC's short preamble approach.

Nodes and Applications in Wireless Sensor Networks

- Sensor Networks consist of nodes with different capabilities.
  – Large number of heterogeneous sensor nodes
  – Spread over a physical location
  – It includes physical sensing, data processing and networking
- In ad-hoc networks, sensors can join and leave due to mobility, failure etc.
- Data can be processed in-network, or it can be directly communicated to the endpoints.

Types of Nodes

- Sensor nodes
  – Low power
  – Consist of sensing device, memory, processor and radio
  – Resource-constrained
- Sink nodes
  – Another sensor node or a different wireless node
  – Normally more powerful/better resources
- Gateway
  – A more powerful node
  – Connection to core network
  – Could consist service representation, cache/storage, discovery and other functions

Types of Applications

- Event detection
  - Reporting occurrences of events
  - Reporting abnormalities and changes
  - Could require collaboration of other nearby or remote nodes
  - Event definition and classification is an issue
- Periodic measurements
  - Sensors periodically measure and report the observation and measurement data
  - Reporting period is application dependent
- Approximation and pattern detection
  - Sending messages along the boundaries of patterns in both space/time
- Tracking
  - When the source of an event is mobile
  - Sending event updates with location information

Requirements and Challenges

- Fault tolerance
  - The nodes can get damaged, run out of power, the wireless communication between two nodes can be interrupted, etc.
  - To tolerate node failures, redundant deployments can be necessary.
- Lifetime
  - The nodes could have a limited energy supply;
  - Sometimes replacing the energy sources is not practical (e.g. underwater deployment, large/remote field deployments).
  - Energy efficient operation can be a necessity.

Requirements and Challenges

- Scalability
  - A WSN can consists of a large number of nodes
  - The employed architectures and protocols should scale to these numbers.
- Wide range of densities
  - Density of the network can vary
  - Different applications can have different node densities
  - Density does not need to be homogeneous in the entire network and network should adapt to such variations.

Requirements and Challenges

- Programmability
  - Nodes should be flexible and their tasks could change
  - The programmes should be also changeable during operation.
- Maintainability
  - WSN and environment of a WSN can change;
  - The system should be adaptable to the changes.
  - The operational parameters can change to choose different trade-offs (e.g. to provide lower quality when energy efficiency is more important)

Required Mechanisms

- Multi-hop wireless communications
  - Communication over long distances can require intermediary nodes as relay (instead of using high transmission power for long range communications).
- Energy-efficient operation
  - To support long lifetime
  - Energy efficient communication/dissemination of information
  - Energy efficient determination of a requested information
- Auto-configuration
  - Self-xxx functionalities
  - Tolerating node failures
  - Integrating new nodes

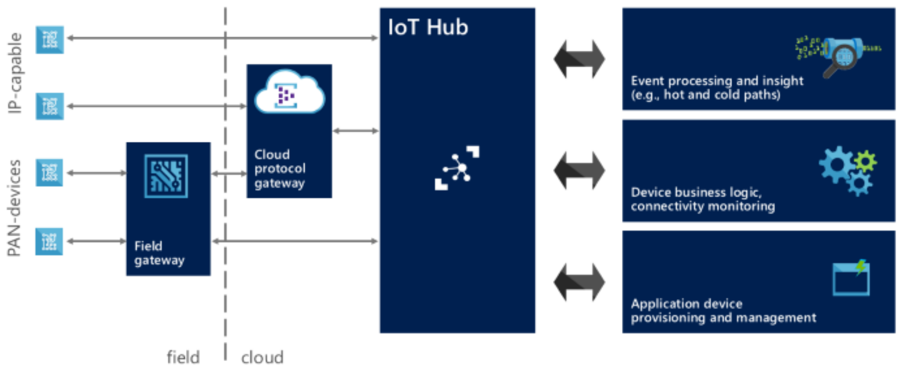
Required Mechanisms

- Collaboration and in-network processing
  - In some applications a single sensor node is not able to handle the given task or provide the requested information.
  - Instead of sending the information form various source to an external network/node, the information can be processed in the network itself.
    - e.g. data aggregation, summarisation and then propagating the processed data with reduced size (hence improving energy efficiency by reducing the amount of data to be transmitted).
- Data-centric
  - Conventional networks often focus on sending data between two specific nodes each equipped with an address.
  - Here what is important is data and the observations and measurements not the node that provides it.

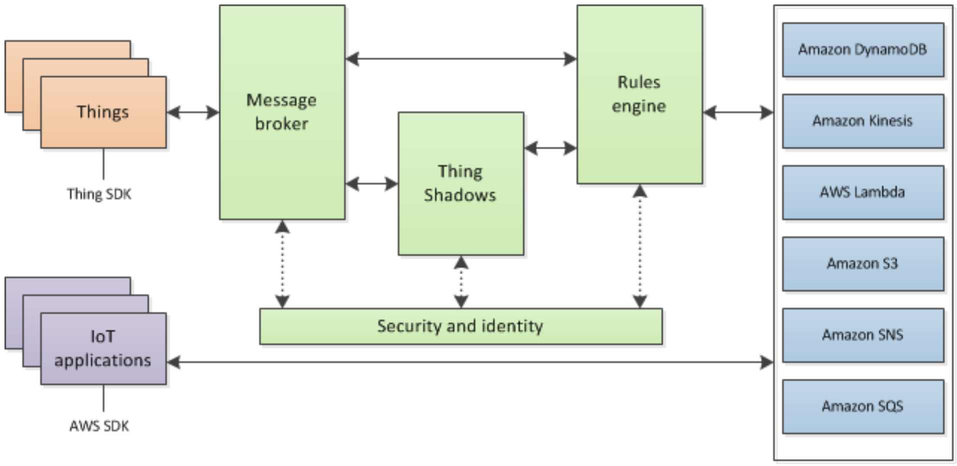
IoT Cloud Solutions

- IoT Hub from Microsoft
- AWS IoT
- PubNub
- Initial State
- SmartThings, Thingsee

IoT Hub



AWS IoT data services



WSN Applications

- Environmental/ Habitat Monitoring
  - Scientific, ecological applications
    - Non-intrusiveness
    - Real-time, high spatial-temporal resolution
    - Remote, hard-to-access areas
  - Acoustic detection
  - Seismic detection
- Surveillance and Tracking
  - Military and disaster applications
  - Reconnaissance and Perimeter control
  - Structural monitoring (e.g., bridges)

WSN Applications

- "Smart" Environments
  - Precision Agriculture
  - Manufacturing/Industrial processes
    - Inventory (RFID)
    - Process Control
  - Smart Grid
- Medical Applications
  - Hospital/Clinic settings
  - Retirement/Assisted Living settings

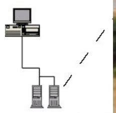
Environment Monitoring: Great Duck Island

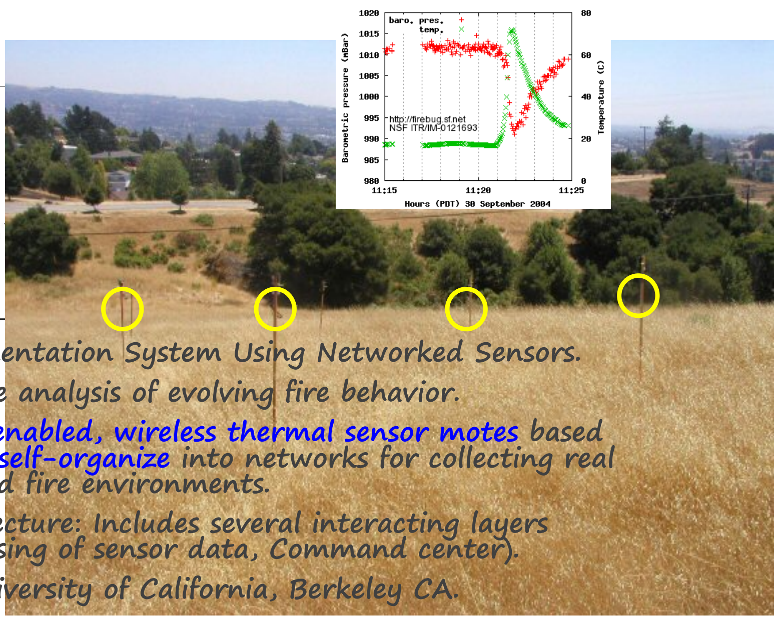
- *150 sensing nodes deployed throughout the island relay data temperature, pressure, and humidity to a central device.*
- *Data was made available on the Internet through a satellite link.*

Habitat Monitoring: The ZebraNet Project

- Margaret Martonosi, Princeton University
- Collar-mounted sensors with GPS
- Use peer-to peer info communication
- monitor zebra movement in Kenya

FireBug





Wildfire Instrumentation System Using Networked Sensors.

Allows predictive analysis of evolving fire behavior.

Firebugs: GPS-enabled, wireless thermal sensor motes based on TinyOS that self-organize into networks for collecting real time data in wild fire environments.

Software architecture: Includes several interacting layers (Sensors, Processing of sensor data, Command center).

A project by University of California, Berkeley CA.

Precision Agriculture

- Richard Beckwith, Intel Corporation
- The "Wireless Vineyard"
  - Sensors monitor temperature, moisture
  - Roger the dog collects the data

Camalie Vineyards

- Case Study in Crossbow Mote Deployment

Water in the Vineyard

Vineyard Installation

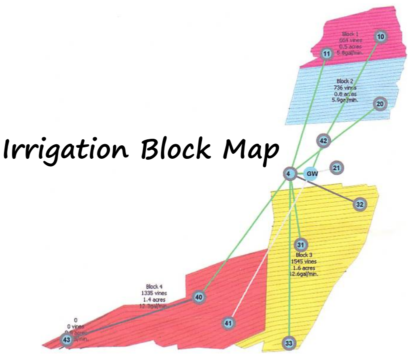
- At each Mote location:
  - 2 soil moisture sensors
  - 12" and 24" depth
  - 1 soil temp sensor to calibrate soil moisture sensors

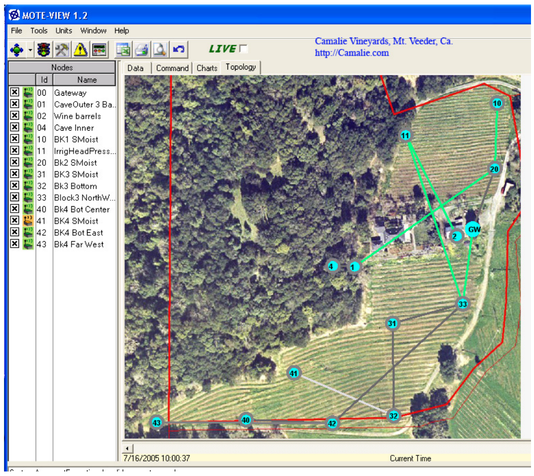
Power Supply

- 2 month max battery life now with 10 minute sampling interval.
- Decided to use solar power, always there when doing irrigation. Solar cell $10 in small quantities and need a $.50 regulator.

Network Maps

- 13 nodes late 2005, 18 nodes in 2006





A Vision for Wireless MIS

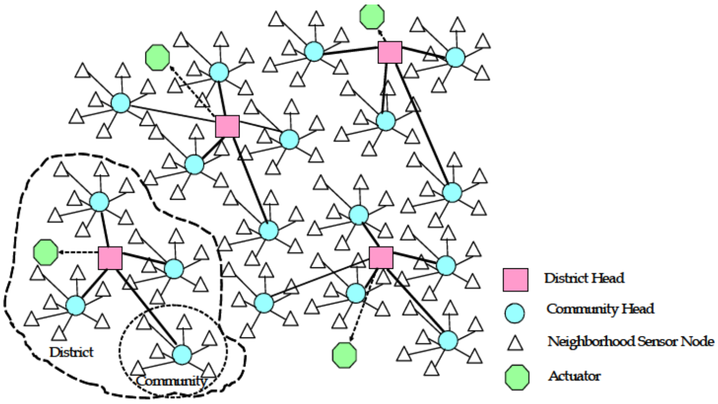


Figure 1 Hierarchical Scalable Sensor Network Architecture

Concept includes smart phone platforms to streamline continuous monitoring.

A Vision for Wireless MIS

Community head: In-body sensor node that communicates with the outside world, and is in direct communication range from other in-body sensors. Community head node is dynamically selected and rotated.

Hierarchy 1: In-body sensors form a 1-hop ad-hoc community network. Can operate in unused 412 MHz spectrum with 802.11e based QoS MAC protocol

Hierarchy 2: Inter-person communication (district network). Medical data diffusion to central processing facilities using the same band and protocols as the in-body network

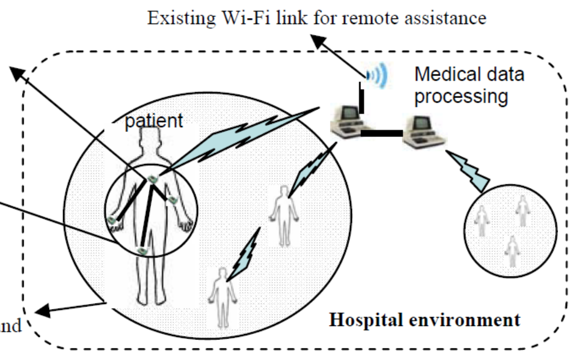


Figure 2: Medical Information System Architecture in Hospital Environment

Health surveillance region provides a multi-hop path from body sensor networks to central data log and processing nodes.

WSNs for Assisted Living

Alarm-Net
University of Virginia

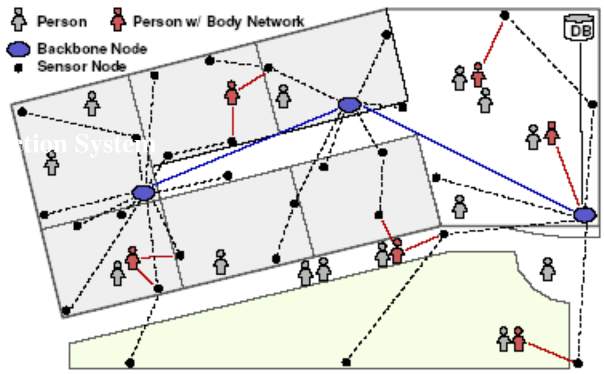


Figure 1. Assisted-living deployment example, showing connections among sensors, body networks, and backbone nodes.

WSNs for Assisted Living

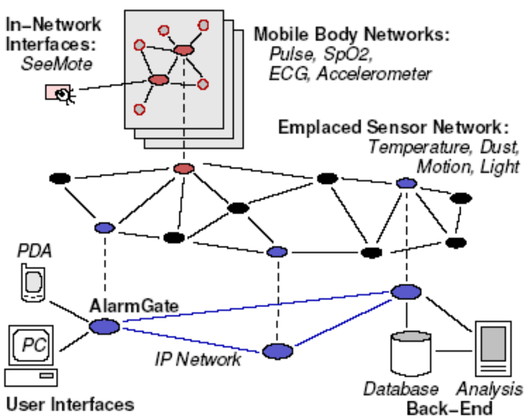


Figure 2. ALARM-NET architecture components and logical topology.

WSNs for Assisted Living

Two-Tiered
WSN
Architecture

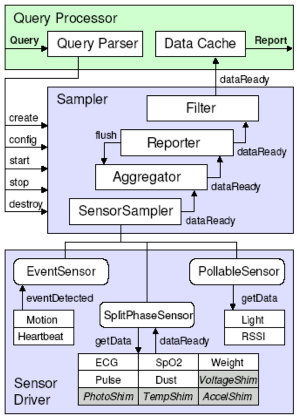


Figure 3. Query processing stack on sensor devices. The Query Processor parses queries, and starts the Sampler, which reads data from the sensor drivers on schedule, generating data that flows up the processing chain toward the Query Processor for reporting.

Berkeley Fall Detection System

Using Smart Sensors and Camera Phone to Detect and Verify The Fall of Elderly Persons

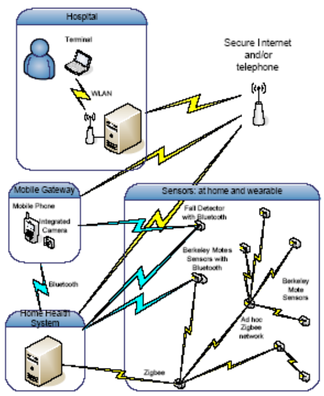


Figure 1: The Information Technology for Assisted Living at Home (ITALH) system overview

Berkeley Fall Detection System

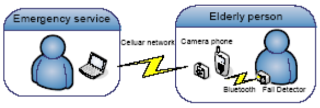


Figure 2: Fall detector system setup

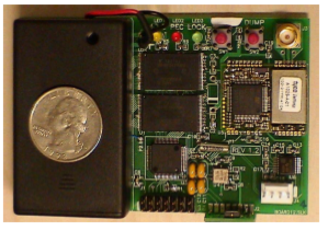


Figure 3: The Berkeley GPSADXL fall sensor