Pervasive Computing 2: Sensors and Networks

IAT 351

Week10 Lecture 1

27.02.2008

Lyn Bartram

lyn@sfu.ca

SCHOOL OF INTERACTIVE ARTS + TECHNOLOGY

Today’s agenda

- Technologies in context: ubicomp revisited
- RFID
- Communication networks
- Sensor networks

What is Ubiquitous Computing?

- **Ubiquitous computing** (ubicomp) integrates computation into the environment, rather than having computers which are distinct objects.
- The idea of ubicomp enable people to interact with information-processing devices more *naturally* and *casually*, and in ways that suit *whatever location* or *context* they find themselves in.

Wikipedia.org

Goals of Pervasive (Ubiquitous) Computing

- Ultimate goal:
  - Invisible technology
  - Integration of virtual and physical worlds
  - Throughout desks, rooms, buildings, and life
  - Take the data out of environment, leaving behind just an enhanced ability to act

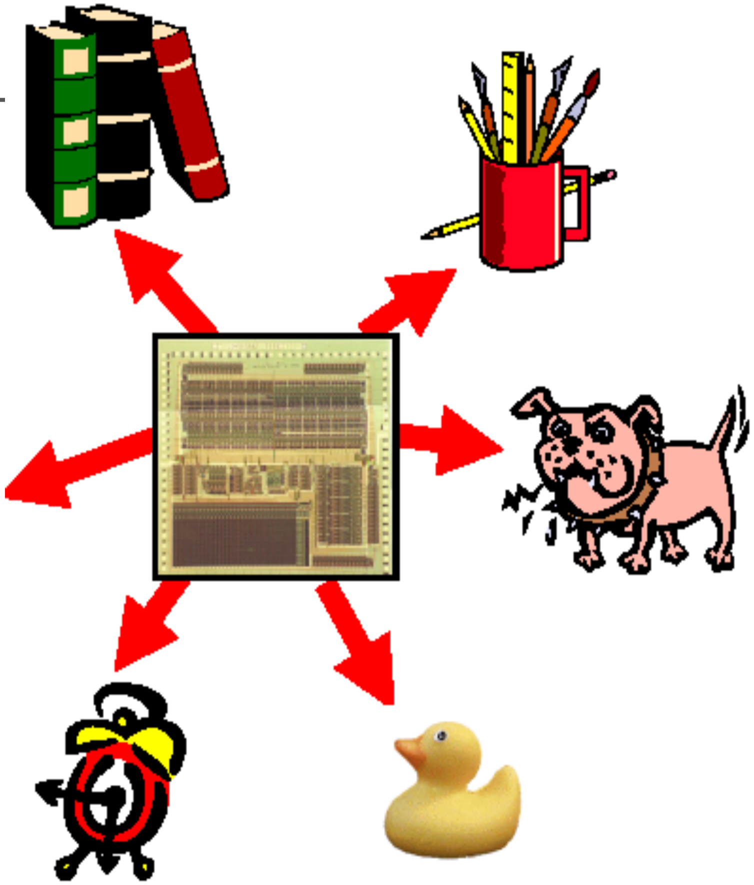
Pervasive Computing Phase I

- Smart, ubiquitous I/O devices: tabs, pads, and boards
- Hundreds of computers per person, but casual, low-intensity use
- Many, many “displays”: audio, visual, environmental
- Wireless networks
- Location-based, context-aware services

- “Using a computer should be as refreshing as a walk in the woods”

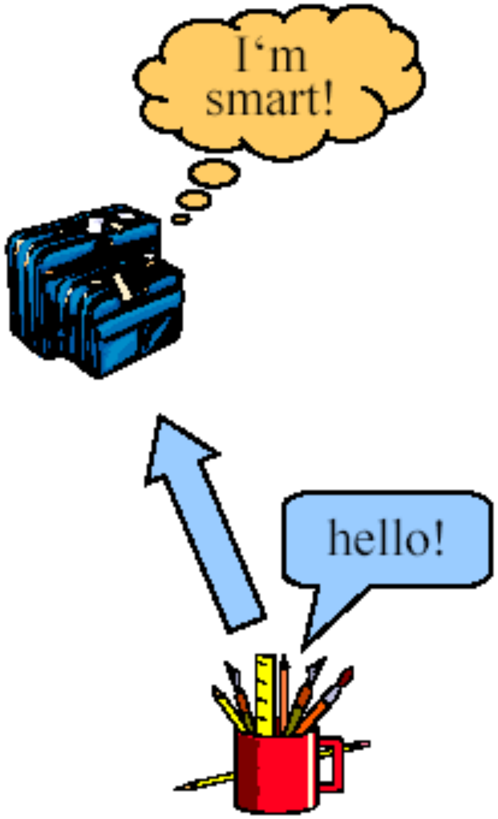
Smart Objects

- Real world objects are enriched with information processing capabilities
- Embedded processors
  - in everyday objects
  - small, cheap, lightweight
- Communication capability
  - wired or wireless
  - spontaneous networking and interaction
- Sensors and actuators

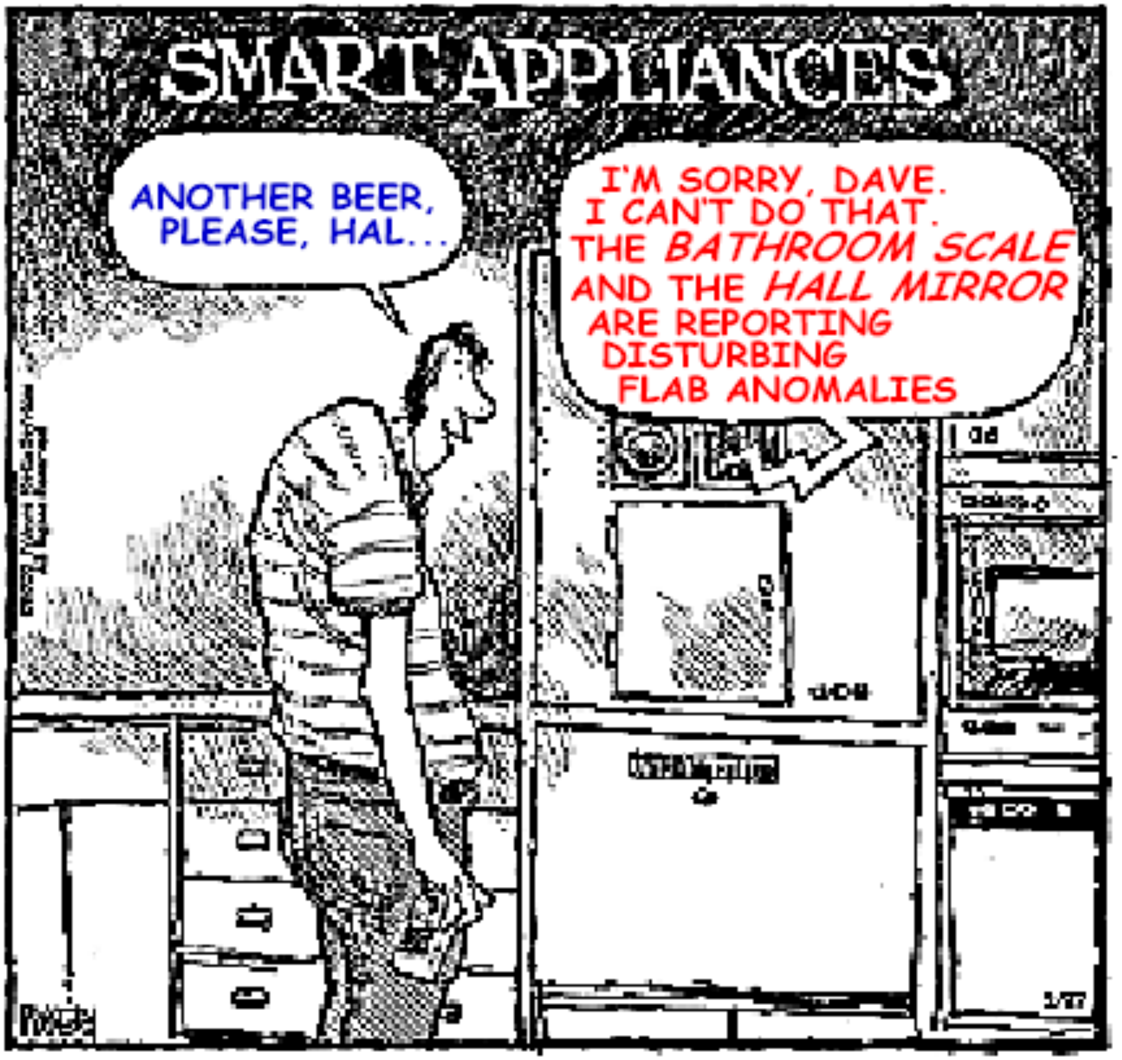


Smart Objects (cont.)

- Can remember pertinent events
  - They have a memory
- Show context-sensitive behavior
  - They may have sensors
  - Location/situation/context awareness
- Are responsive/proactive
  - Communicate with environment
  - Networked with other smart objects



Smart Objects (cont.)


SMART APPLIANCES
ANOTHER BEER, PLEASE, HAL...
I'M SORRY, DAVE. I CAN'T DO THAT. THE BATHROOM SCALE AND THE HALL MIRROR ARE REPORTING DISTURBING FLAB ANOMALIES

Cartoon by Jeff MacNelly

SCHOOL OF INTERACTIVE ARTS + TECHNOLOGY

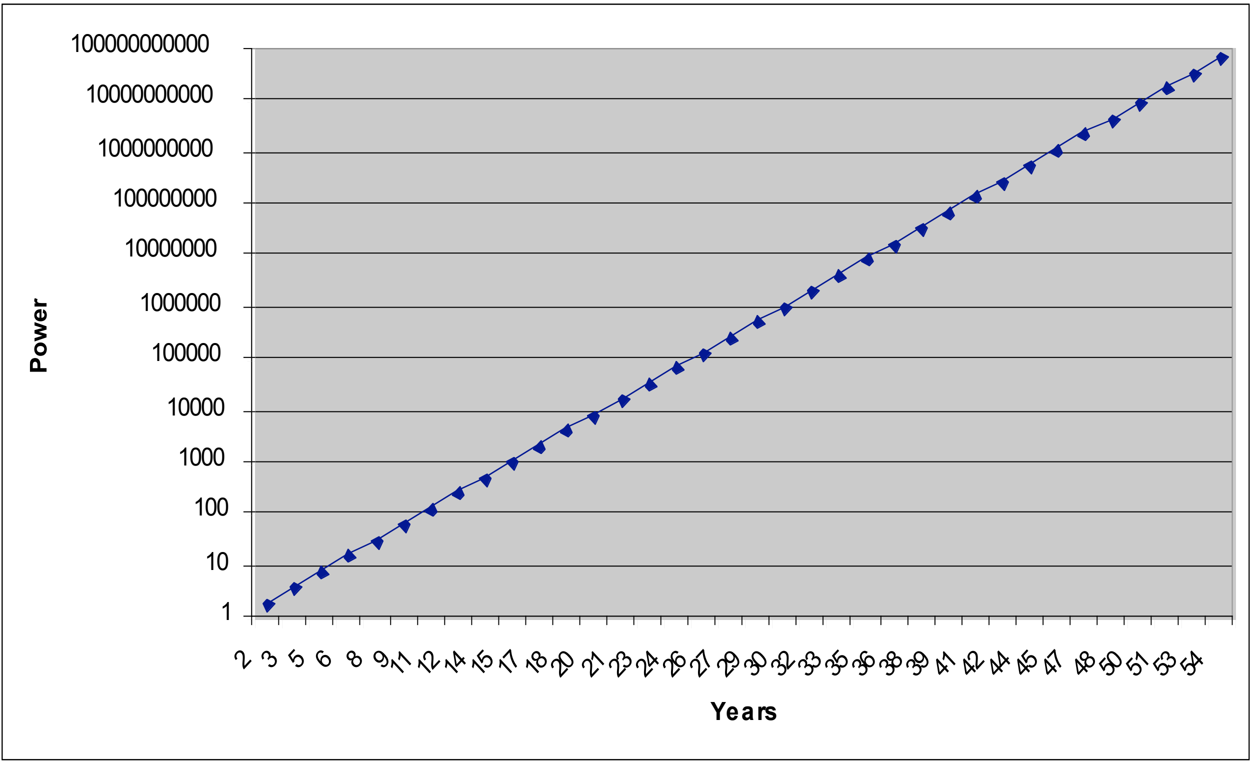
Pervasive Computing Enablers

- Moore’s Law of IC Technologies
- Communication Technologies
- Material Technologies
- Sensors/Actuators

Pervasive Computing Enablers

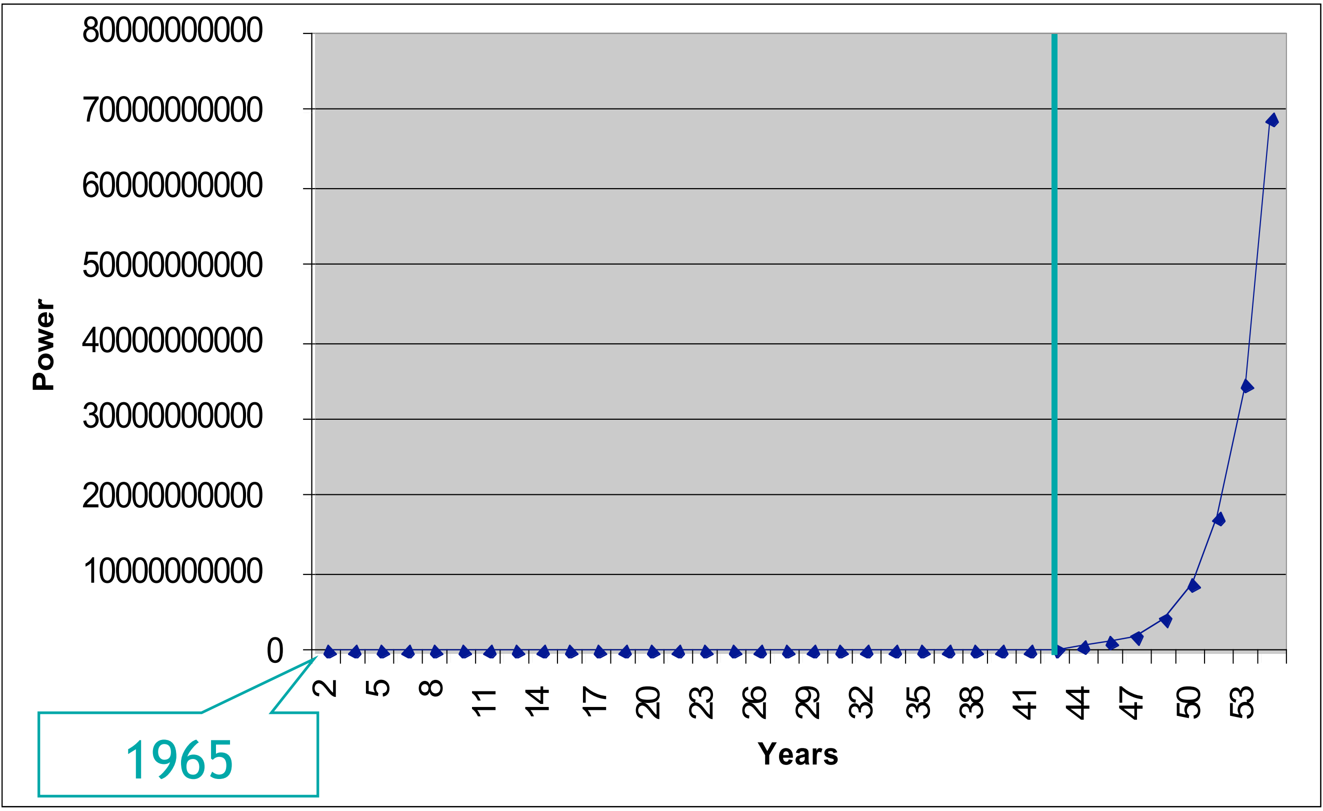
- Moore’s Law of IC Technologies
- **Communication Technologies** ✔ (by the end of the course)
- Material Technologies (other SIAT courses) ✔
- Sensors/Actuators (last week) ✔

Moore’s Law



- Computing power (or number of transistors in an integrated circuit) doubles every 18 months

Moore’s Law



- Computing power (or number of transistors in an integrated circuit) doubles every 18 months

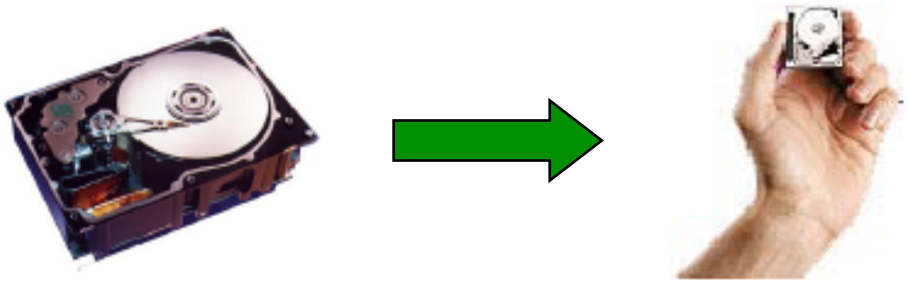
Generalized Moore’s Law

- Most important technology parameters double every 1–3 years:
  - computation cycles
  - memory, magnetic disks
  - Bandwidth

- Consequence:
  - scaling down

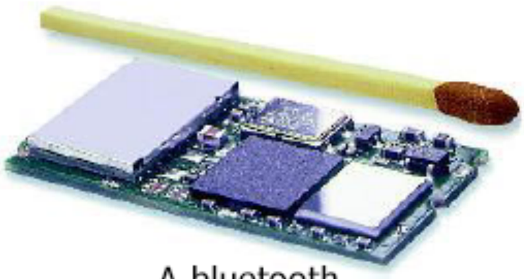
Problems:

- **increasing cost**
- **energy**



2nd Enabler: Communication

- Bandwidth of single fibers ~10 Gb/s
  - 2002: ~20 Tb/s with wavelength multiplex
  - Powerline
  - coffee maker “automatically” connected to the Internet
- Wireless
  - mobile phone: GSM, GPRS, 3G
  - wireless LAN (> 10 Mb/s)
  - PAN (Bluetooth), BAN

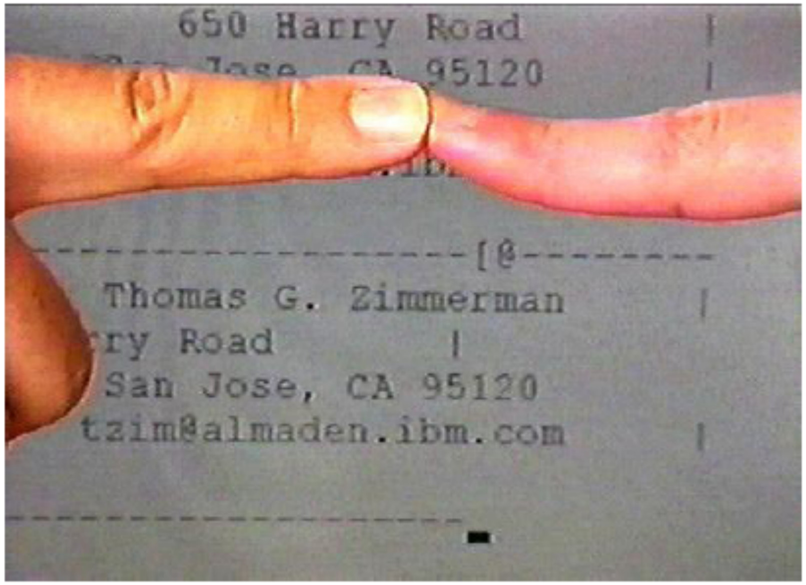


A bluetooth module

Body Area Networks

- Very low current (some nA), some kb/s through the human body

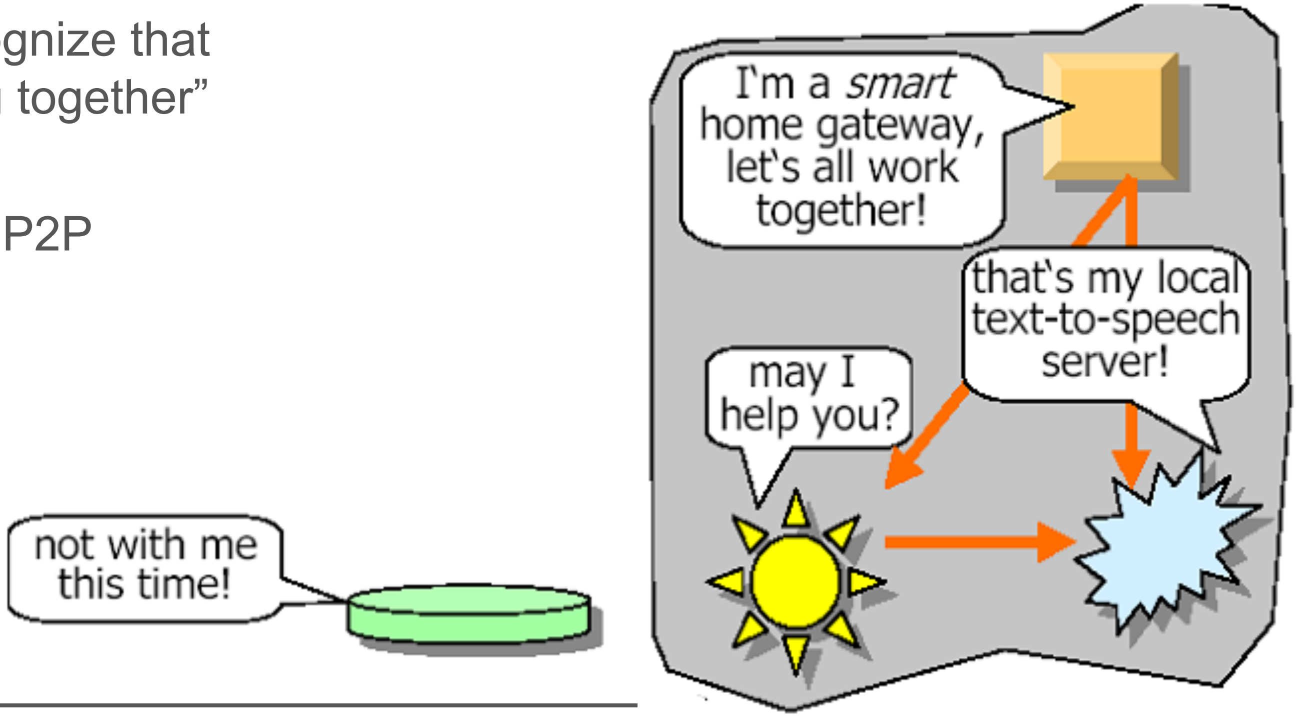
- Possible applications:
  - Car recognize driver
  - Pay when touching the door of a bus
  - Phone configures itself when it is touched



business card exchange (IBM)

Spontaneous (“Ad Hoc”) Networking

- Objects in an open, distributed, dynamic world find each other and form a transitory community
  - Devices recognize that they “belong together”
  - Extension of P2P

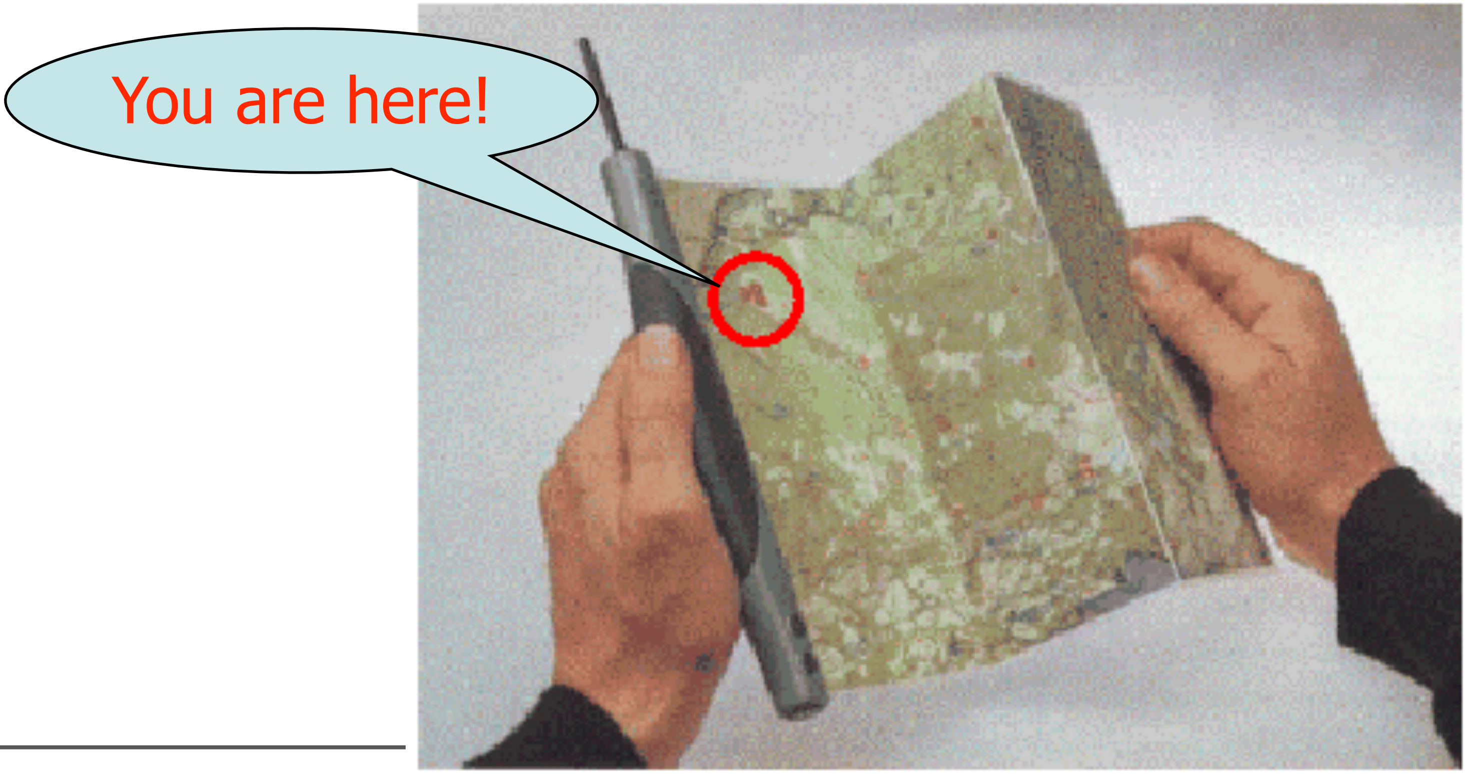

I'm a *smart* home gateway, let's all work together!
that's my local text-to-speech server!
may I help you?
not with me this time!

3rd Enabler: New Materials

- Important: whole eras named after materials
  - e.g., “Stone Age”, “Iron Age”, “Pottery Age”, etc.
- Recent: semiconductors, fibers
  - information and communication technologies
- Organic semiconductors
  - change the external appearance of computers
- “Plastic” laser
  - Flexible displays,…

Interactive Map

- Foldable and rollable



Smart Clothing

- Conductive textiles and inks
  - print electrically active patterns directly onto fabrics
- Sensors based on fabric
  - e.g., monitor pulse, blood pressure, body temperature
- Invisible collar microphones
- Kids' wear
  - game console on the sleeve?
  - integrated GPS-driven locators?
  - integrated small cameras (to keep the parents calm)?

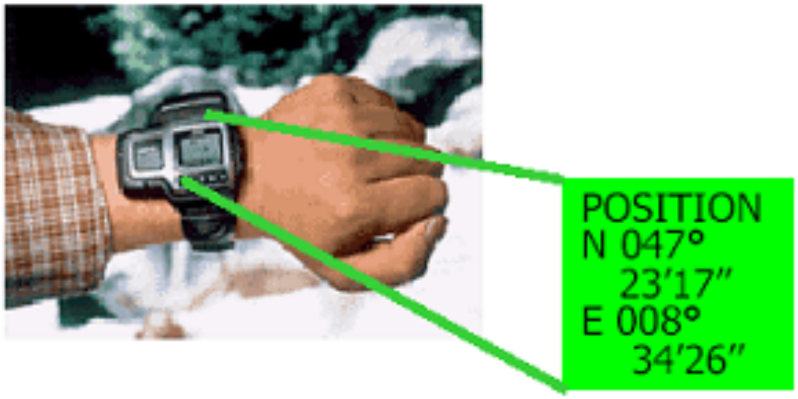
Smart Glasses

- By 2009, computers will disappear. Visual information will be written directly onto our retinas by devices in our eyeglasses and contact lenses
  -- Raymond Kurzweil

4th Enabler: Sensors/Actuators

- Miniaturized cameras, microphones,...
- Fingerprint sensor
- Radio sensors
- RFID
- Infrared
- Location sensors
  - e.g., GPS

- Micro-sensors and sensor nets



Example: Radio Sensors

- No external power supply
  - energy from the actuation process
  - piezoelectric and pyroelectric materials transform changes in pressure or temperature into energy

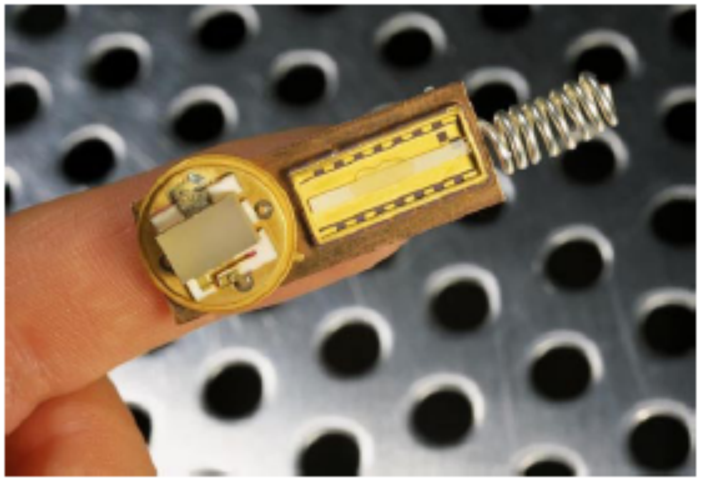


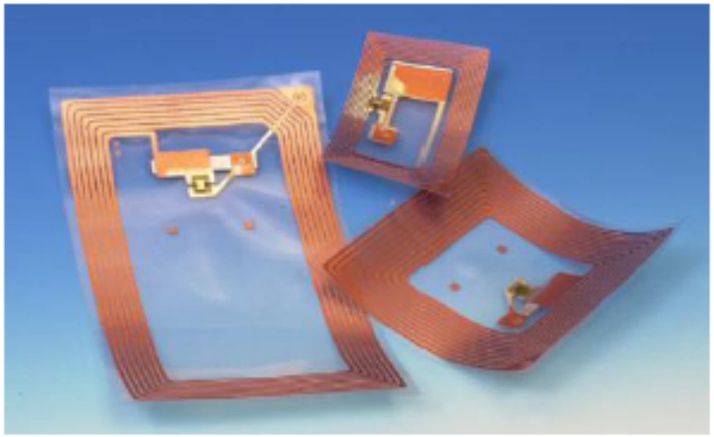
image source: Siemens

- RF signal is transmitted via an antenna (20 m distance)
- Applications: temperature surveillance, remote control (e.g., wireless light switch),...

RFID : **R**adio **F**requency **Id**entification

- Automatic identification procedures exist to provide information about people, animals, goods and products.
- Barcode labels (based on optical principles): are being found to be inadequate in an increasing number of cases
  - (low storage capacity, cannot be reprogrammed).
- Alternative solution to barcode labels: storage of data in a silicon chip (telephone chip cards, bank cards).
  - Disadvantage: impractical mechanical contact.
- RFID: contactless (transfer of data and power)

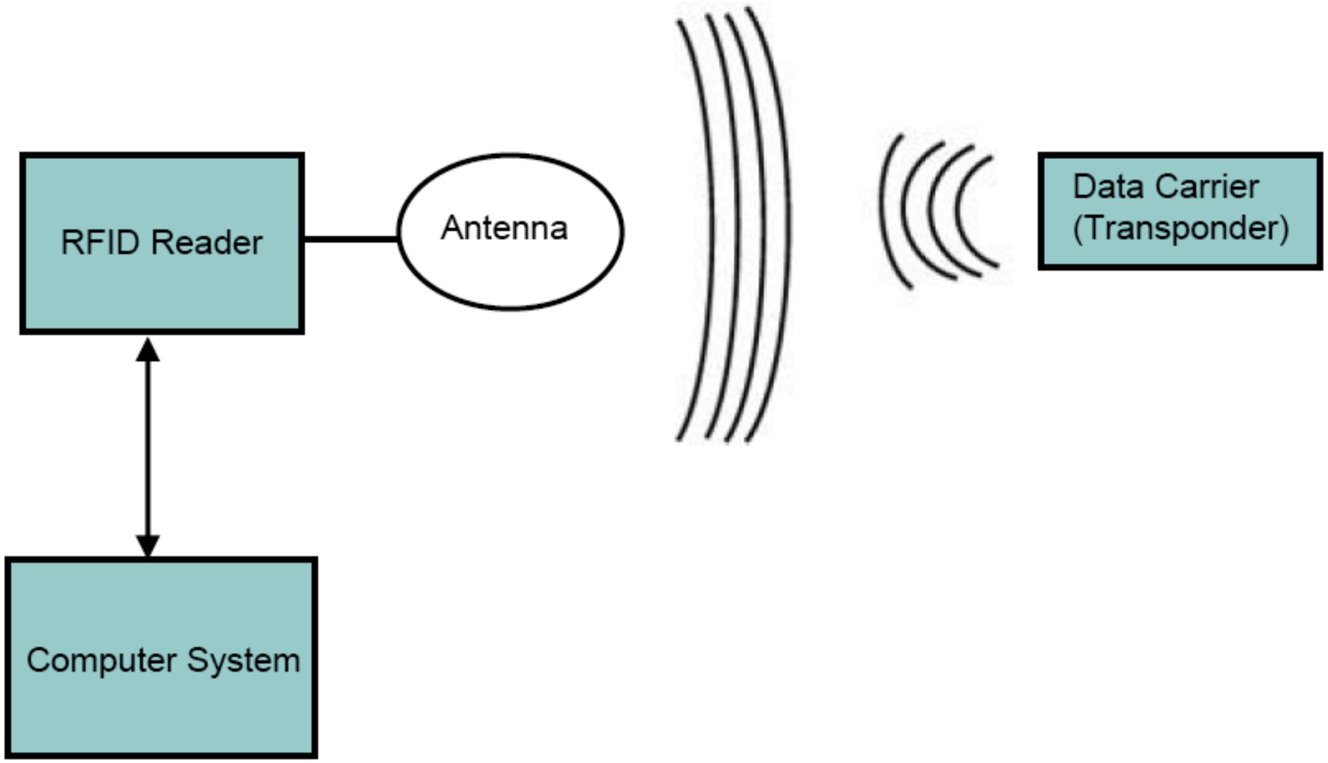
RFIDs (“Smart Labels”)



- Identify objects from distance
  - small IC with RF-transponder
- Wireless energy supply
  - ~1m
- Cost ~$0.1 ... $1
  - consumable and disposable
- Flexible tags
  - laminated with paper

Chip (without antenna): ~ 2 mm x 2 mm x 10 μm (fits into 80 μm thick paper!)

RFID System


RFID Reader
Antenna
Data Carrier
(Transponder)
Computer System

RFID

- An RFID system is always made up of two components:
- the **transponder**, which is located on the object to be identified
- the **detector reader**, which, depending upon design and the technology used, may be a read or write/read device

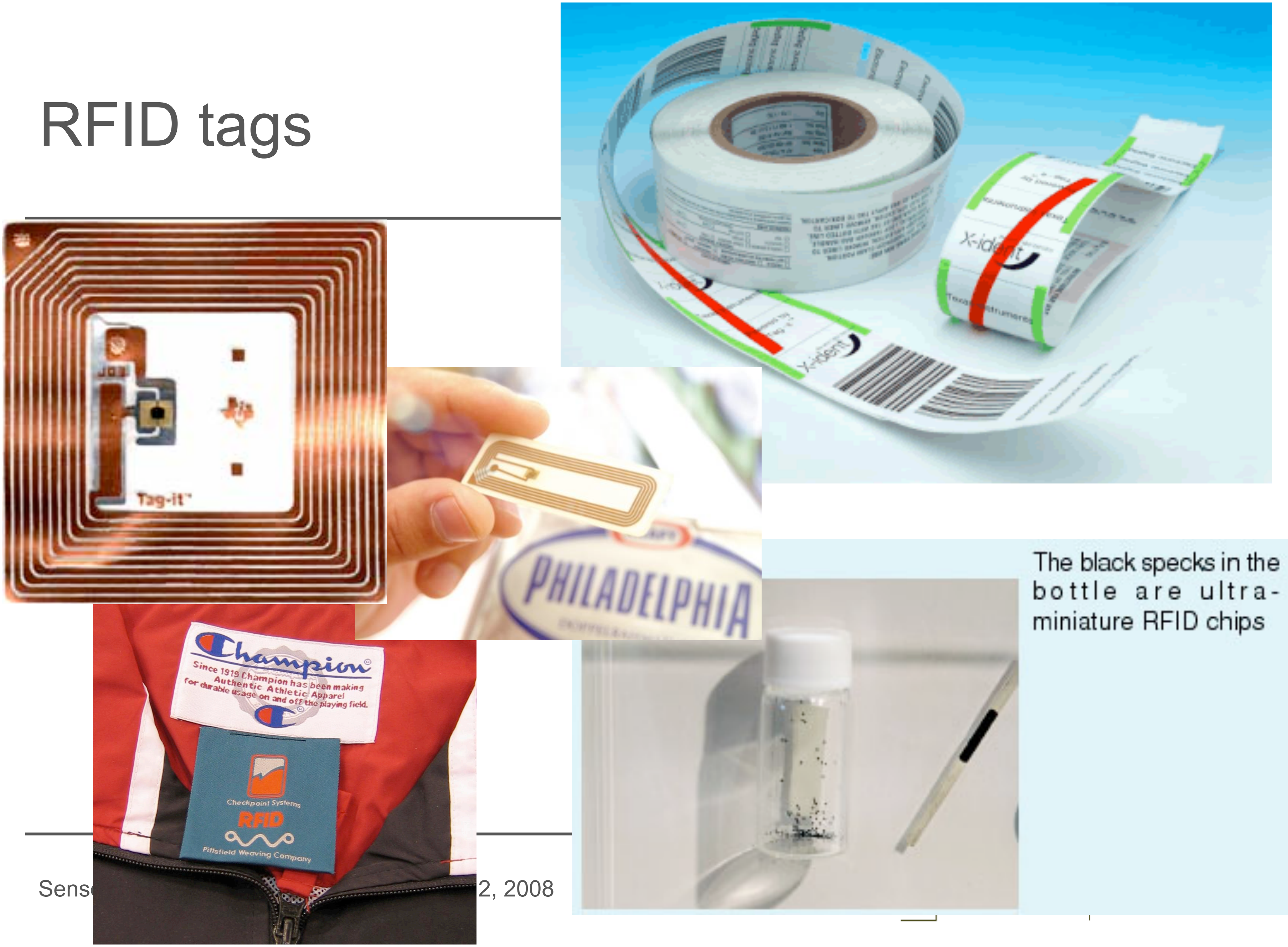
RFID

- Reader transfers energy to the transponder by emitting electromagnetic waves through the air.
- Transponder uses RF energy to charge up.
- Transponder receives command/data signal and responds.
- Reader receives transponder’s response and processes it, i.e. sends it to a computer system.

RFID tag (transponder)

- Comprised of a chip and antenna mounted onto a substrate or an enclosure.
- The chip may consists of a **processor, memory and radio transmitter.**
- The transponder communicates via radio frequency to a reader, which has its own antennas.
- Transponders are also known as smart or radio tags.
- The memory will vary, depending on the manufacturer, from just a few characters to kilobytes

RFID tags


Tag-it™
X-ident
Texas Instruments
PHILADELPHIA
Champion
Since 1919 Champion has been making Authentic Athletic Apparel for durable usage on and off the playing field.
Checkpoint Systems
RFID
Pittsfield Weaving Company

The black specks in the bottle are ultra-miniature RFID chips

Types of RFID tags

Transponders can be:

- **Read Only (R/O):**are pre-programmed with a unique identification.
- **Read Write (R/W):**for applications that require data to be stored in the transponder and can be updated dynamically.
-
- **Write Once Read Manytimes (WORM)**: will allow for an identification number to be written to the transponder once. The information is stored in the memory, it cannot be changed but the transponder can be read many times.

RFID Technologies

The two most common types of RFID technologies are:

- **Active RFID transponders: are self powered and tend to be** more expensive than passive.
    - Having power on board allows the tag to have greater communication distance and usually larger memory capacity.
- **Passive RFID transponders: which are available with chips** and without chips, they have no internal power source, therefore require external power to operate.
    - The transponder is powered by an electromagnetic signal that is transmitted from a reader. The signal received will charge an internal capacitor on the transponder, which in turn will then supply the power required to communicate with the reader.

Benefits of using RFID

- Transponders can be read from a distance and from any orientation, thus they do not require line of sight to be read.
- Transponders have read and write capabilities, which allow for data to be changed dynamically at any time.
- Multiple transponders can be read at once and in bulk very quickly.
- RF-Tags can easily be embedded into any non-metallic product. This benefit allows the tag to work in harsh environments providing permanent identification for the life of the product

Frequencies and applications

- Today, most implementations involve **passive technology.**
- There are different frequency bands which passive technology operates within:
- **Low frequency (LF) passive RFID**
- **High frequency (HF) passive RFID**
- **Ultra High frequency (UHF) passive RFID**

- One frequency does not fit all types of applications.

Frequencies and applications

- LF:
  - Range varies from a few cm to a couple of meters depending on the size of the transponders and efficiency of the meter
  - Not very affected by surrounding metals or water
  - Expensive ($ 2.00 - $17.00 CDN in 2006)
  - Only read one tag/transponder at a time
- HF
  - More affected by metals than LF
  - Faster communication
  - Read range < 1m
  - Cheap(er) ($0.70 - $0.80)
  - Reads multiple tags

RFID Frequencies cont.

- UHF
  - Longer read distance (1-10 m)
  - Does not work well with liquids (humidity)
  - Supply chain targeting
  - WalMart!!
  - Long read distance is a disadvantage in applications where security and privacy are issues
    - Banking
    - Access control

RFID deployment

- RFID systems are already in place, or soon to be installed
  - many retailers are contemplating putting tracking chips on merchandise
  - U.S. Food and Drug Administration recently decided to let hospitals inject into patients RFID chips storing medical data
- There are many issues that still need to be addressed
- Cost is still a major issue

RFID Advantages

- No line of sight required.
- Multiple items can be read with a single scan.
- Each tag can behave like a portable database.
- Hidden data source.
- Virtually unlimited lifetime
- Tags can be read from great distances.

RFID Advantages

- Can be combined with current barcode technology
- Can take many shapes and survive climactic and harsh conditions
- Data on the tag can be modified
- Unique permanent ID embedded
- No line of sight required
- Multiple tags can be read with a single scan

RFID Disadvantages

- High cost of tags
- Limited read/write range for most common types
- Current lack of worldwide standards
- Privacy and security issues of range and scope

Beyond simple sensors

The sensor is the cell of many extensive systems today

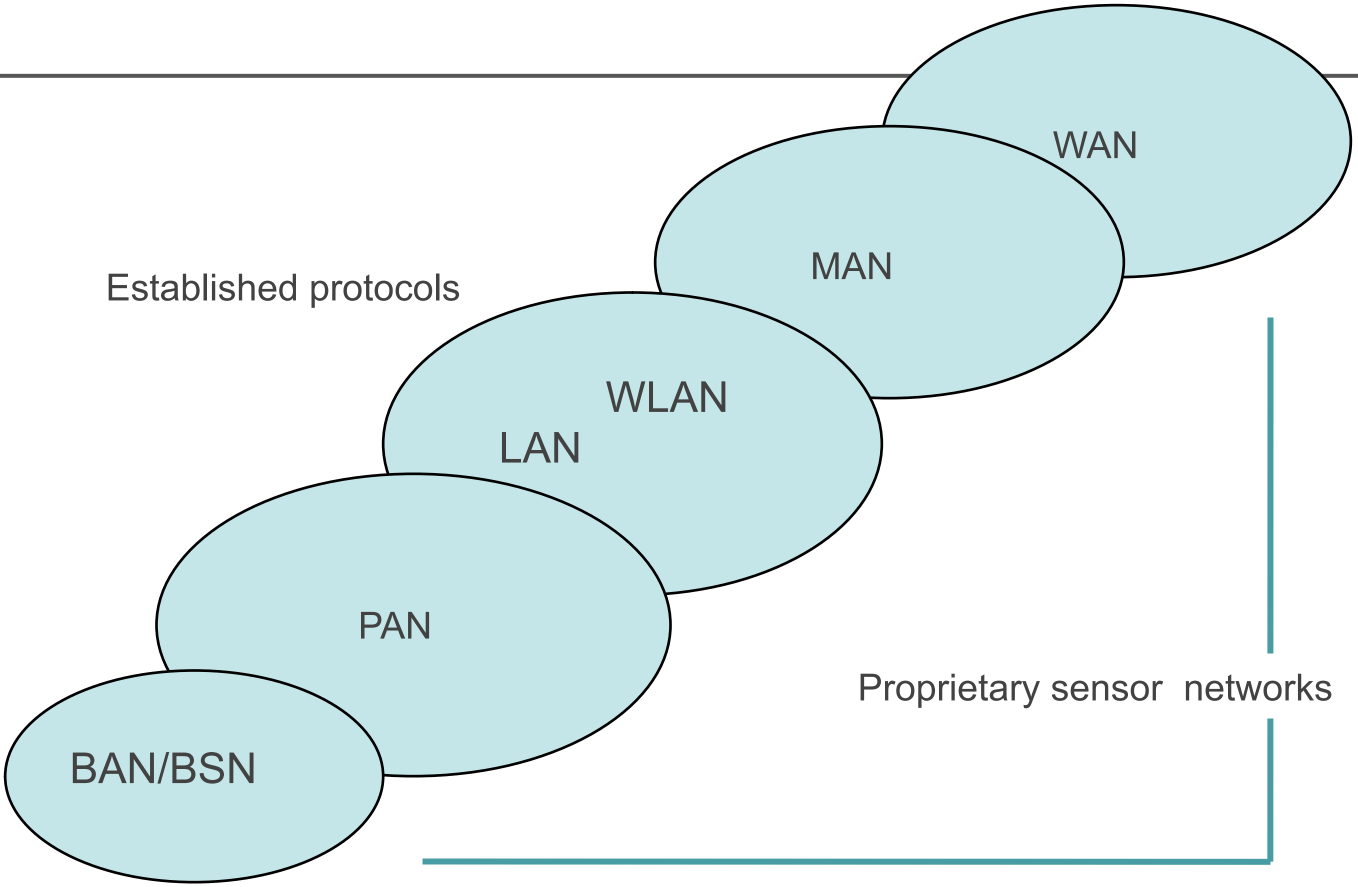
  - Supervisory control and monitoring
  - Health
  - Pervasive computing
  - Ubiquitous computing

- Sensor systems depend on:
  - Computation: the processor
  - Persistence: memory
  - Power
  - **Communication: the network**

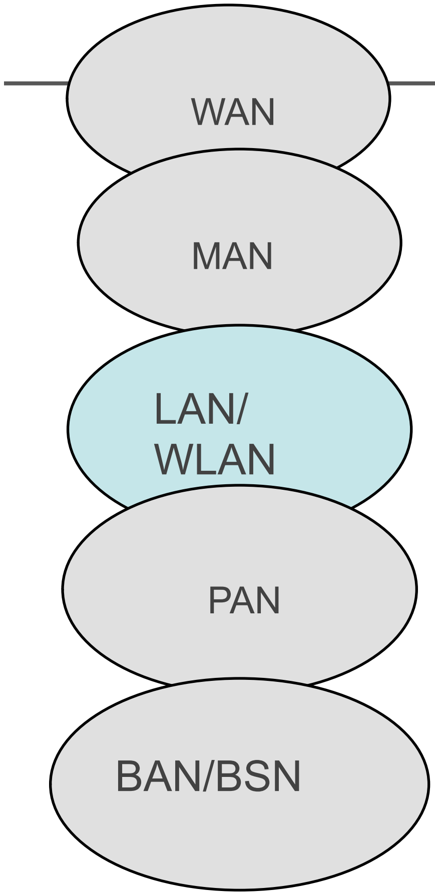
Sensor networks

- Embedded sensor networks
  - monitoring and control
- Dynamic sensor networks
  - Vehicle tracking
  - Emergency services
- Ubiquitous computing networks
  - Smart homes
  - Context-sensitive adaptive services
- Interactive individual networks
  - Body sense networks

The scope of activity



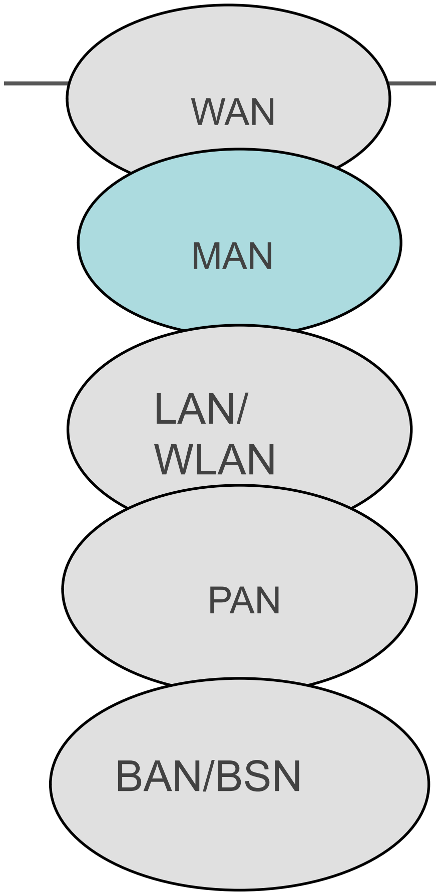
LANs



The term LAN stands for Local Area Network.

- The term ‘local area’ in the world of networking usually refers to a geographically contiguous area in which the inter-computer distance is lesser than or equal to one kilometer.
    - In practice, far smaller span
- Owned and managed by one entity
- While LANs are no longer strictly wired, they are always “grounded” on some wired backbone.
- TCP/IP (Ethernet)

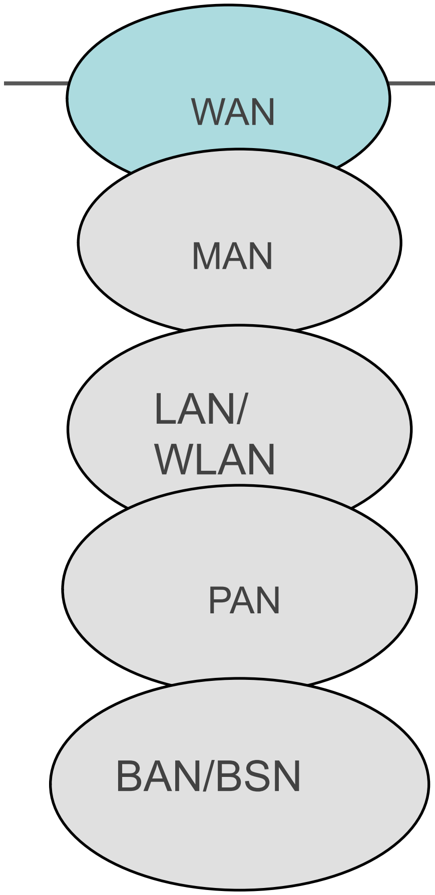
MANs



The term MAN stands for Metropolitan Area Network.

- A computer network that is not usually owned by a single organization / entity and that is spread over a metropolitan city area is called a Metropolitan Area Network.
- Normally, in a MAN, the inter-node distance does not exceed ten kilometers. This, however, is not a hard-and-fast rule.
- MANs = network of collaborating owners
- Typically internet (http, ftp)

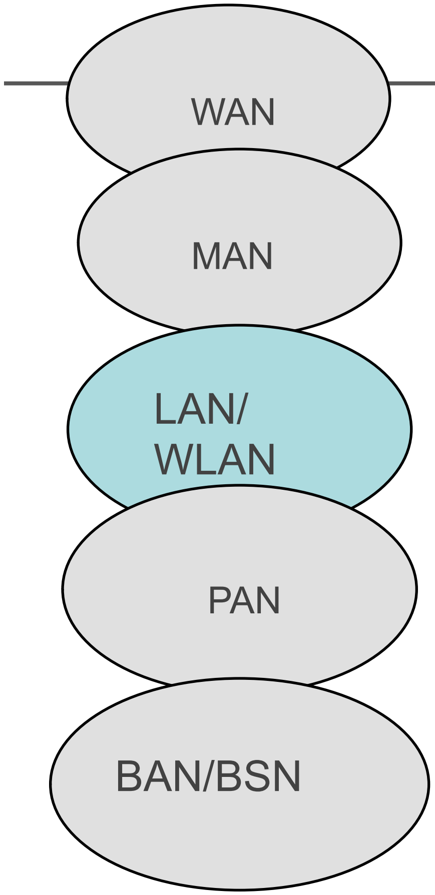
WANs



The term WAN stands for Wide Area Network.

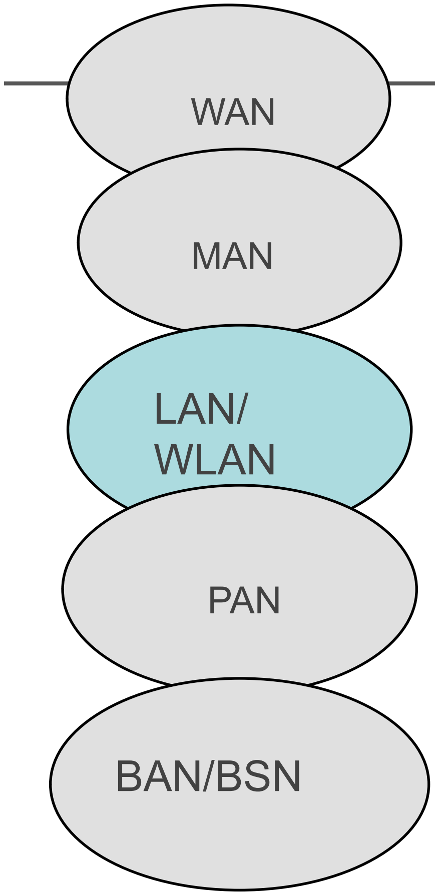
- A WAN spreads over a large geographic area.
- While the “official” designation of a WAN is a computer network that is not usually owned by one entity and is bigger than a MAN, in practice WAN has come to mean any large such service
- The most ubiquitous WANs are the cellular networks
    - Voice, some data

Wireless LAN (WLAN)



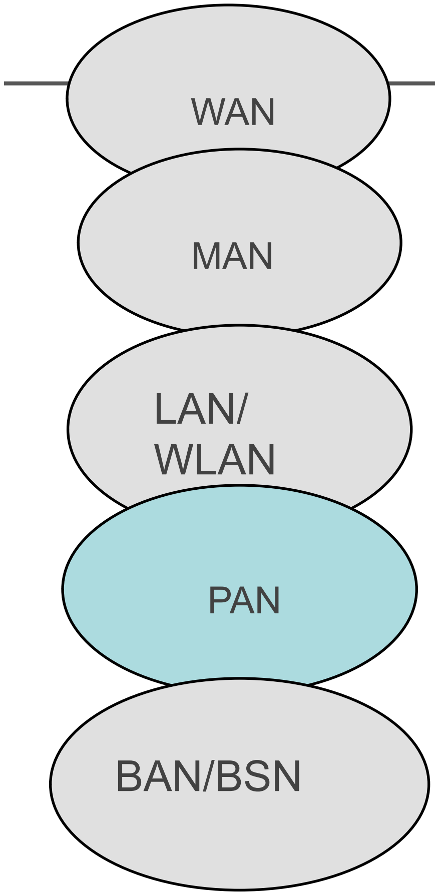
- IEEE 802.11 standard was finalized in July 1997.
  - WiFi
- Requires a receiver (computer) and a *hotspot* (wireless access point)
- Relatively small range (100-m)
  - 802.11a can transmit up to 54 Mbps within 30 meters; 802.11b can transmit up to 11 Mbps within 30-50 meters; 802.11g – 54 Mbps, 50 meters.
- Benefits are low cost and simple Internet access.

Wireless LAN (WLAN)



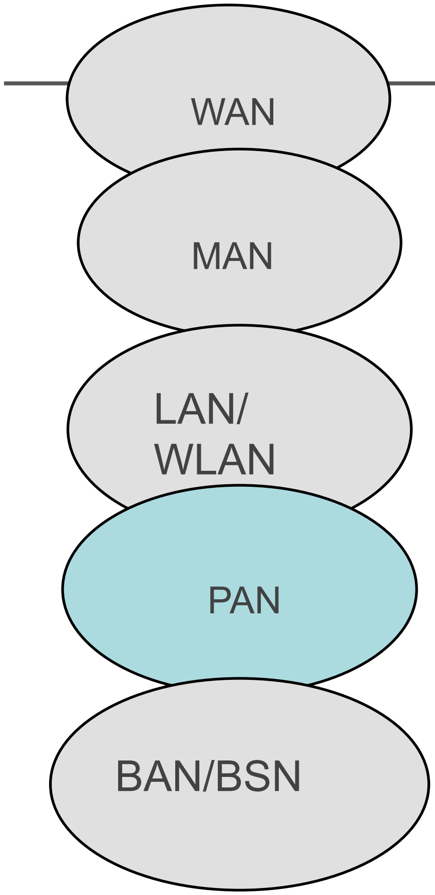
- Roaming – users cannot roam from hotspot to hotspot if the hotspots use different Wi-Fi network services.
- Security – because Wi-Fi uses radio waves, it is difficult to protect.
- Cost – commercial Wi-Fi services are low cost but not free and each service has its own fees and separate accounts for users to logon.
- Power - Devices are relatively power hungry

PAN : Bluetooth



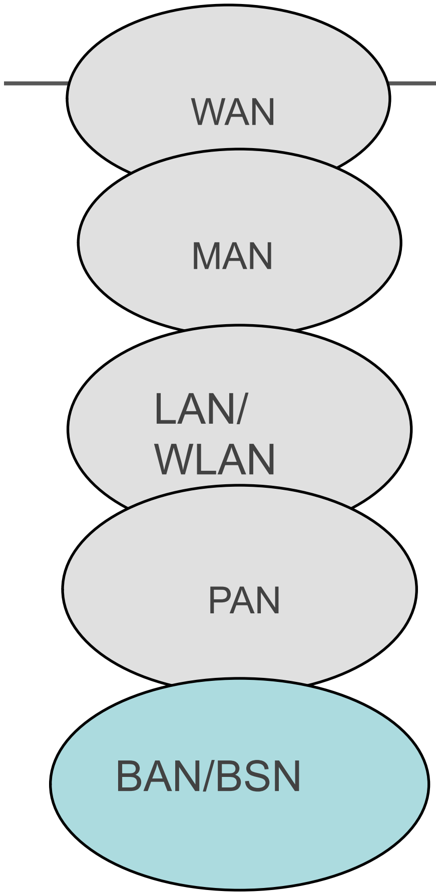
- Personal area network (PAN) is a computer network used for communication among computer devices (e.g., telephones, PDAs, smart phones) close to one person.
- Bluetooth is used to create small PANs:
  - can link up to 8 devices within a 10-meter area;
  - uses low-power, radio-based communications;
  - can transmit up to 1 Mbps.
  - Designed as a “cable replacement” technology
  - Many cell phones support Bluetooth
  - Interoperability / bridge

PAN : ZigBee



- IEEE 802.15 (Zigbee) targets applications that need low data transmission rates and low power consumption:
  - moves data only one-fourth as fast as Bluetooth;
  - Can handle hundreds of devices at once;
  - most promising application is meter reading.
- Current focus is to wirelessly link sensors that are embedded into industrial controls, medical devices, smoke and intruder alarms and building and home automaton.

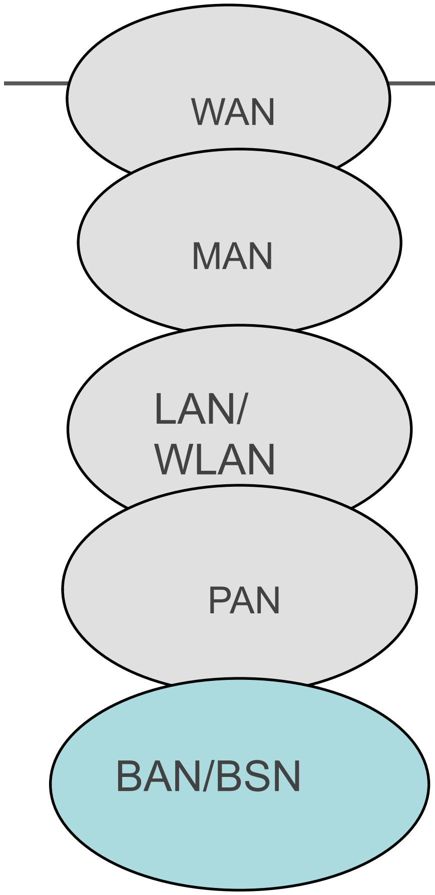
BAN : Body Area Network



- Subgroup of PANs
- Domain: HealthCare
- Compact & Mobile
- Sensors inserted inside the body coordinate
- Enable transfer of vital parameters
- Medical Communication

- GPRS and UTMS as emerging protocols

BAN Wearable computing

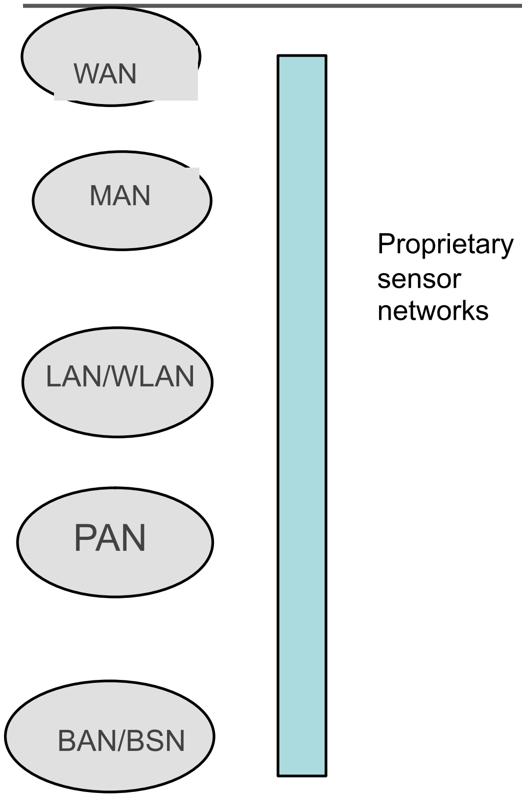


- Sensors embedded in clothing
- Smart badges

Challenges:

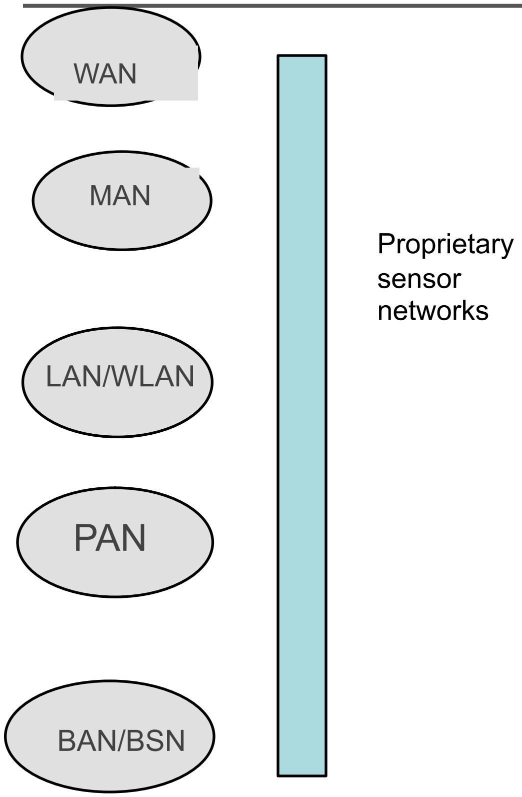
- Miniaturisation of pervasive devices
- Weight minimisation of pervasive devices
- Type/nature of device location on /in the human body
- The development of safe, secure, and effective data communication media
- Providing different forms of engagement with wearable devices that are hands-free

Telemetry: Sensor networks



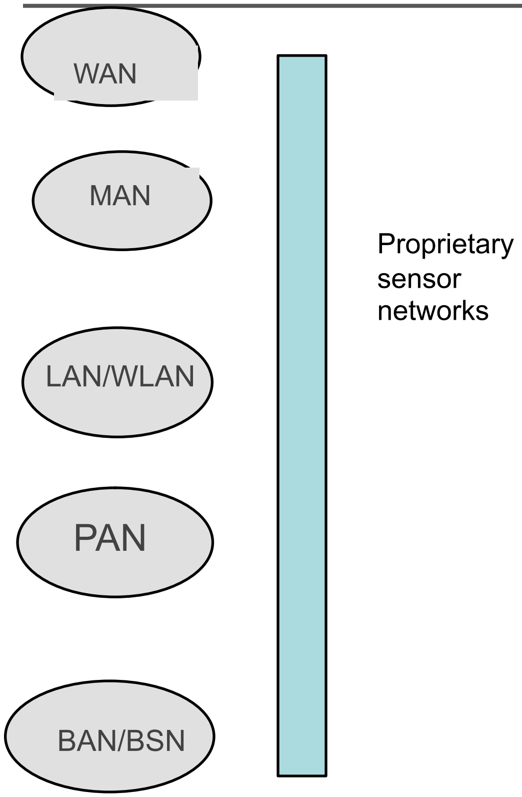
- Telemetry is the wireless transmission and receipt of data gathered from remote sensors.
- Technicians can use telemetry to identify maintenance problems in equipment;
- Doctors can monitor patients and control medical equipment from a distance;
- Car manufacturers use telemetry for remote vehicle diagnosis and preventive maintenance.

Telemetry: wireless Sensor networks



- Wireless Sensor Networks are networks of interconnected, battery-powered, wireless sensors called *motes* that are placed into the physical environment.
- Motes collect data from many points over an extended space.
- Each mote contains processing, storage, and radio frequency sensors and antennae.
- Motes provide information that enables a central computer to integrate reports of the same activity from different angles within the network.

Structure: wireless Sensor networks



WAN

MAN

LAN/WLAN

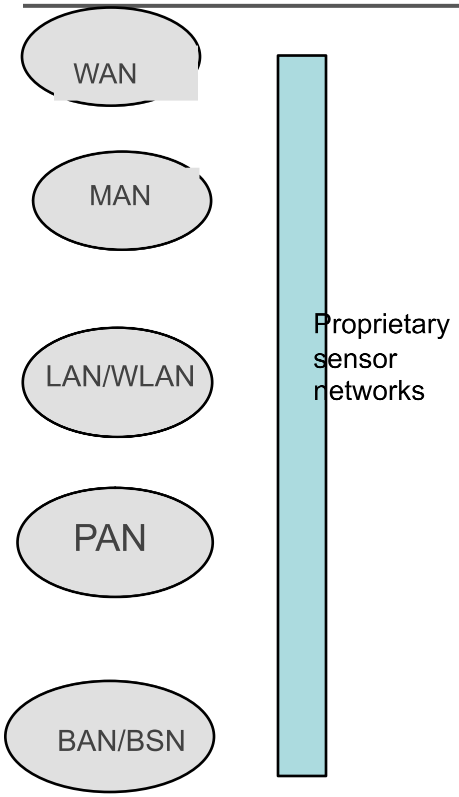
PAN

BAN/BSN

Proprietary sensor networks

- A *Mesh Network* is composed of motes, where each mote wakes up for a fraction of a second when it has data to transmit and then relays that data to its nearest neighbor.
- An advantage is if one mote fails, another one can pick up the data.
- Very efficient and reliable.
  - Self healing and reporting
- many spatially distributed low-cost sensing nodes that collaborate with each other but operate autonomously
- information routed to whichever (computational) node can best use the information

Wireless Sensor networks: classification



WAN

MAN

LAN/WLAN

PAN

BAN/BSN

Proprietary sensor networks

- Sensor position
  - Static (Habitat, CORIE, Biomedical)
  - Mobile (Smart Dust, Biomedical)
- Goal-driven
  - Monitoring: Real-time/Not-real-time (Habitat, Smart Dust)
  - Forecasting
  - Function substitution (Biomedical)
- Communication medium
  - Radio Frequency (Habitat, Biomedical)
  - Light (Smart Dust)

Smart Dust (UC Berkeley)

- network of tiny wireless microelectromechanical systems (MEMS) sensors, robots, or devices, installed with wireless communications, that can detect anything from light and temperature, to vibrations, etc
- devices=motes: each device would contain sensors, computing circuits, bidirectional wireless communications technology and a power supply
- motes would gather data, run computations and communicate using two-way-band radio with other motes at distances approaching 1,000 feet

Challenges

- Limited computation and data storage
- Low power consumption
- Wireless communication
- Data-related issues
- Continuous operation
- Inaccessibility – network adjustment and retasking
- Robustness and fault tolerance

Potential Applications

- high-rise buildings self-detect structural faults
- schools detect airborn toxins at low concentrations
- buoys alert swimmers to dangerous bacterial levels
- earthquake-rubbled building infiltrated with robots and sensors: locate survivors, evaluate structural damage
- ecosystems infused with chemical, physical, acoustic, image sensors to track global change parameters
- battlefield sprinkled with sensors that identify track friendly/foe air, ground vehicles, personnel

Design Issues

- Self configuring systems that adapt to unpredictable environment
  - dynamic, hard to model, environments preclude pre-configured behavior
- data processing inside the network
  - exploit computation near data to reduce communication
  - collaborative signal processing
  - achieve desired global behavior with localized algorithms (distributed control)
- long-lived, unattended, low duty cycle systems
  - energy a central concern
  - communication primary consumer of scarce energy resource