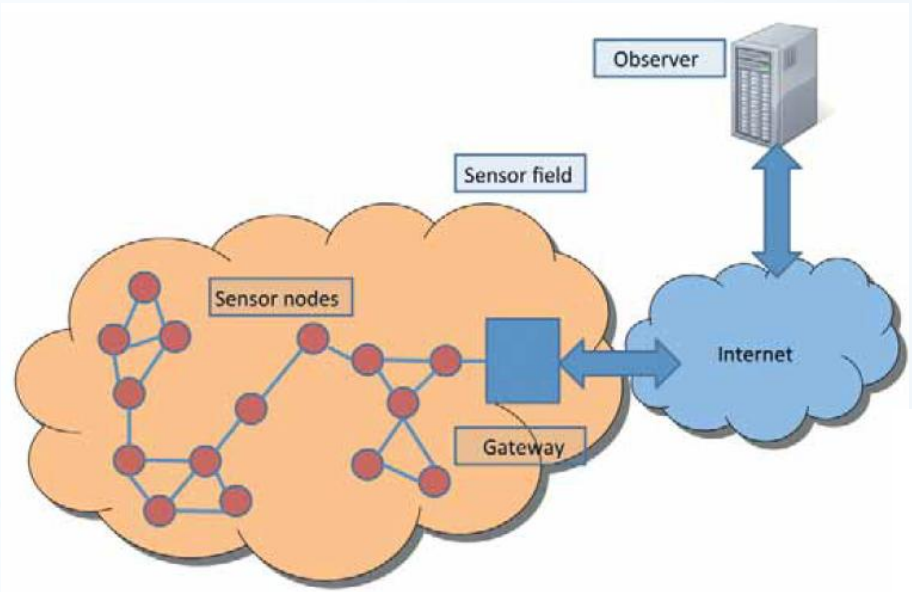
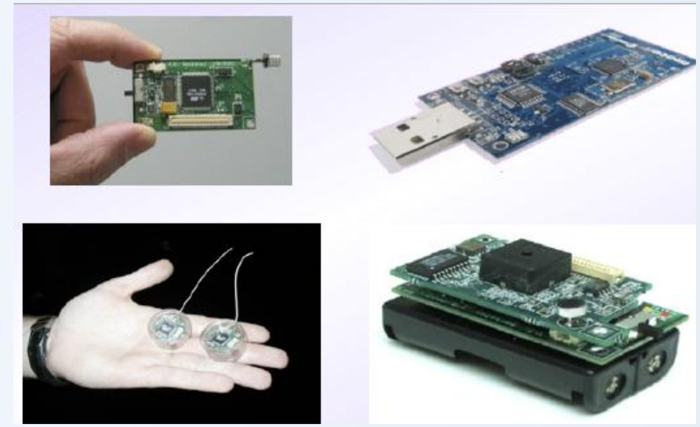
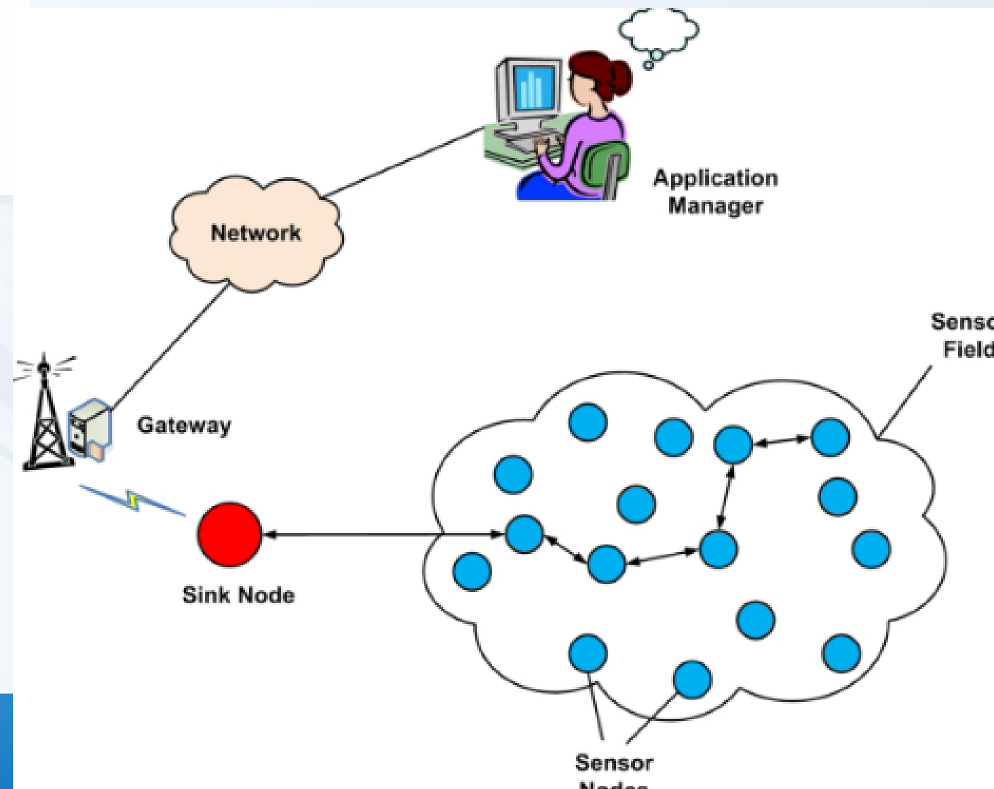
Wireless Sensor Network

Andrey Vasilyev

What is Wireless Sensor Network?







A **Wireless Sensor Network** is 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.

When and where did WSN start from?

- The development of WSNs was inspired by **military applications**, notably surveillance in conflict zones. Research on WSNs dates back to the early 1980s when the United States Defense Advanced Research Projects Agency (DARPA) carried out the distributed sensor networks (DSNs) for the US military. Drawbacks: the sensors were rather large (i.e. the size of a shoe box and bigger), and the number of potential applications was thus limited.
- The new wave of research on WSNs started around 1998. **Inspired by rapid advancement in multiple sensing technologies**:
  - **Microelectromechanical systems (MEMS)** – gyroscopes, ccelerometers, magnetometers, pressure sensors, pyroelectric effect sensors, acoustic sensors
  - **CMOS-based sensors** – temperature, humidity, capacitive proximity, chemical composition
  - **LED sensors** – ambient light sensing, proximity sensing

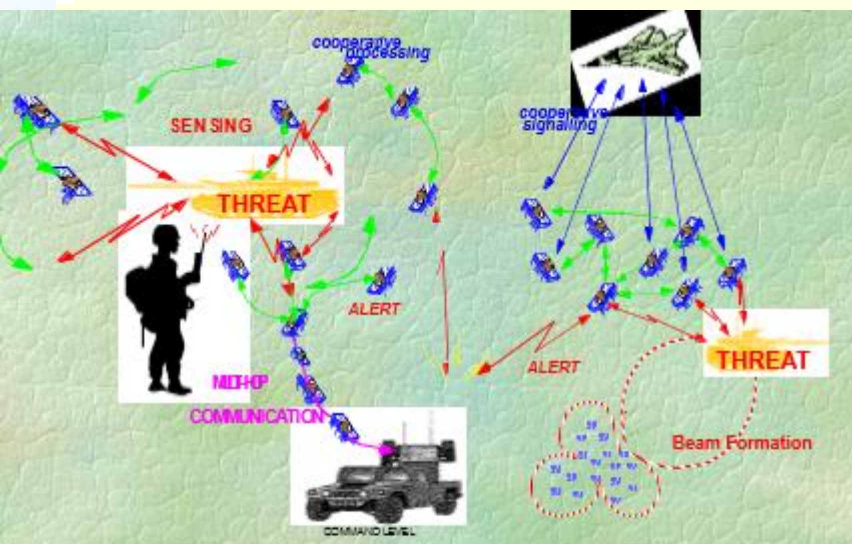
WSN Timeline

- 1980’s: Distributed wired sensor networks
- 1999-2003: DARPA SensIT project: UC Berkeley, USC, Cornell etc.
- 2001: Intel Research Lab at Berkeley focused on WSN
- 2001-2002: Emergence of sensor networks industry; startup companies including Sensoria, Crossbow, Ember Corp, SensiCast plus established ones: Intel, Bosch, Motorola, General Electric, Samsung.
- 2003-2004: IEEE 802.15.4 standard, Zigbee Alliance

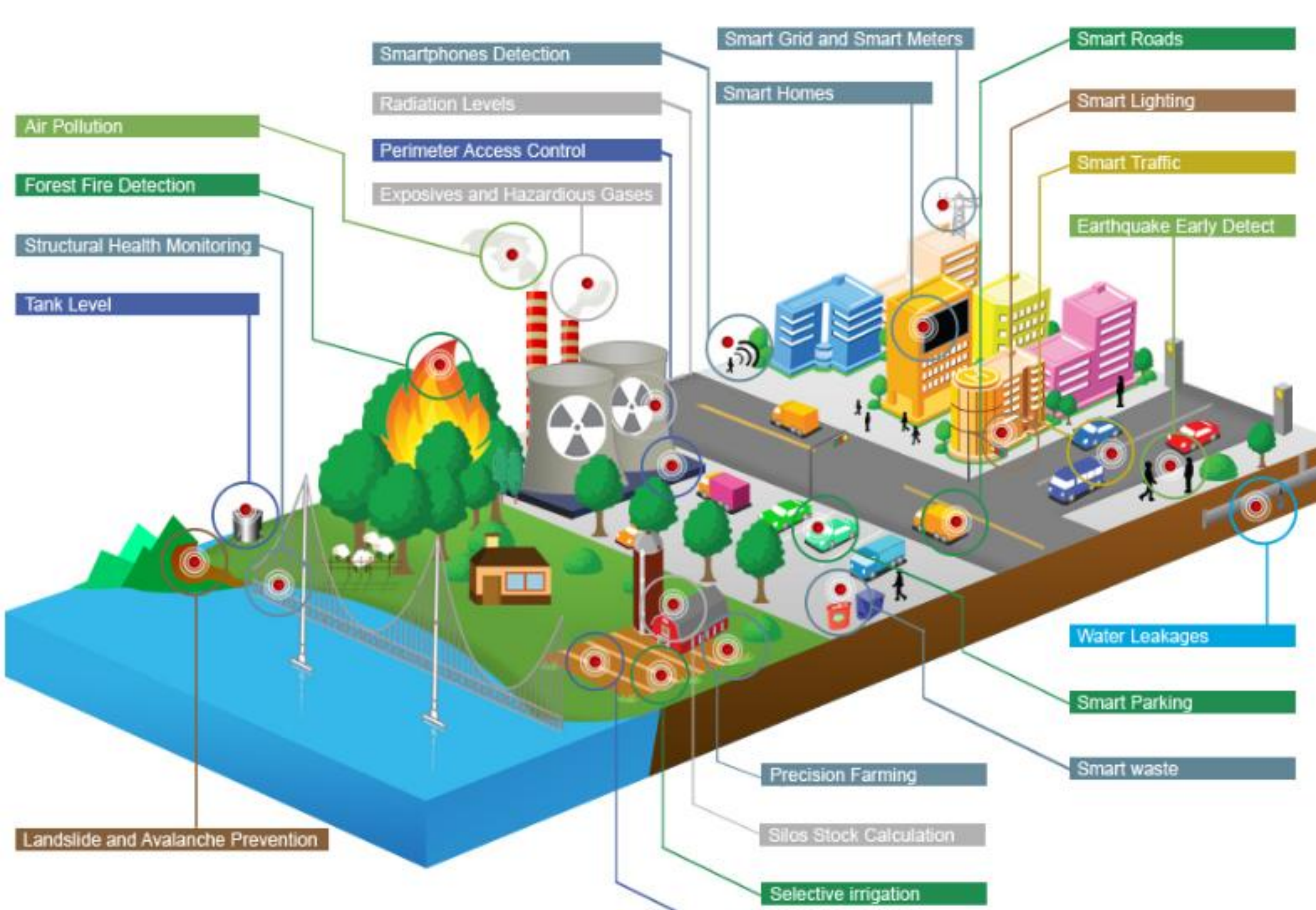
WSN Applications

Sensor Network

- **Tracking**
  - **Military** — Enemy Tracking
  - **Habitat** — Animal Tracking
  - **Business** — Human tracking
  - **Public/Industrial** — Traffic Tracking, Car/Bus Tracking
- **Monitoring**
  - **Military** — Security Detection
  - **Habitat** — Animal Monitoring (Zebra, birds, Cane toad)
  - **Business** — Inventory Monitoring
  - **Public/Industrial** — Structural Monitoring, Factory Monitoring, Inventory Monitoring, Machine Monitoring, Chemical Monitoring
  - **Health** — Patient monitoring
  - **Environment** — Environmental Monitoring (weather, temperature, pressure)

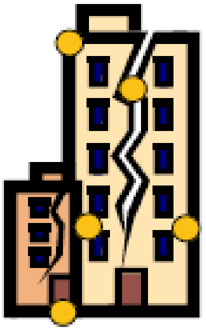


WSN examples

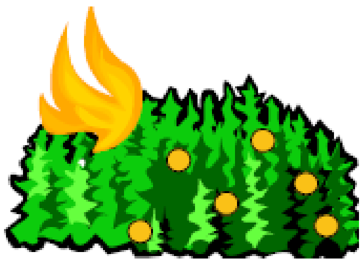


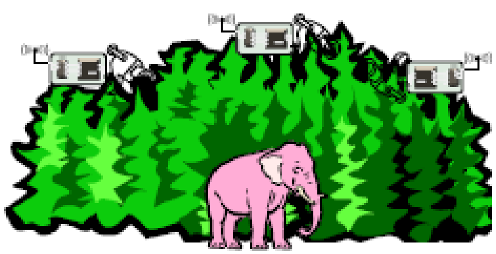
WSN Examples continued

- Intelligent buildings (or bridges)
  - Reduce energy wastage by proper humidity, ventilation, air conditioning (HVAC) control
  - Needs measurements about room occupancy, temperature, air flow, …
  - Monitor mechanical stress after earthquakes



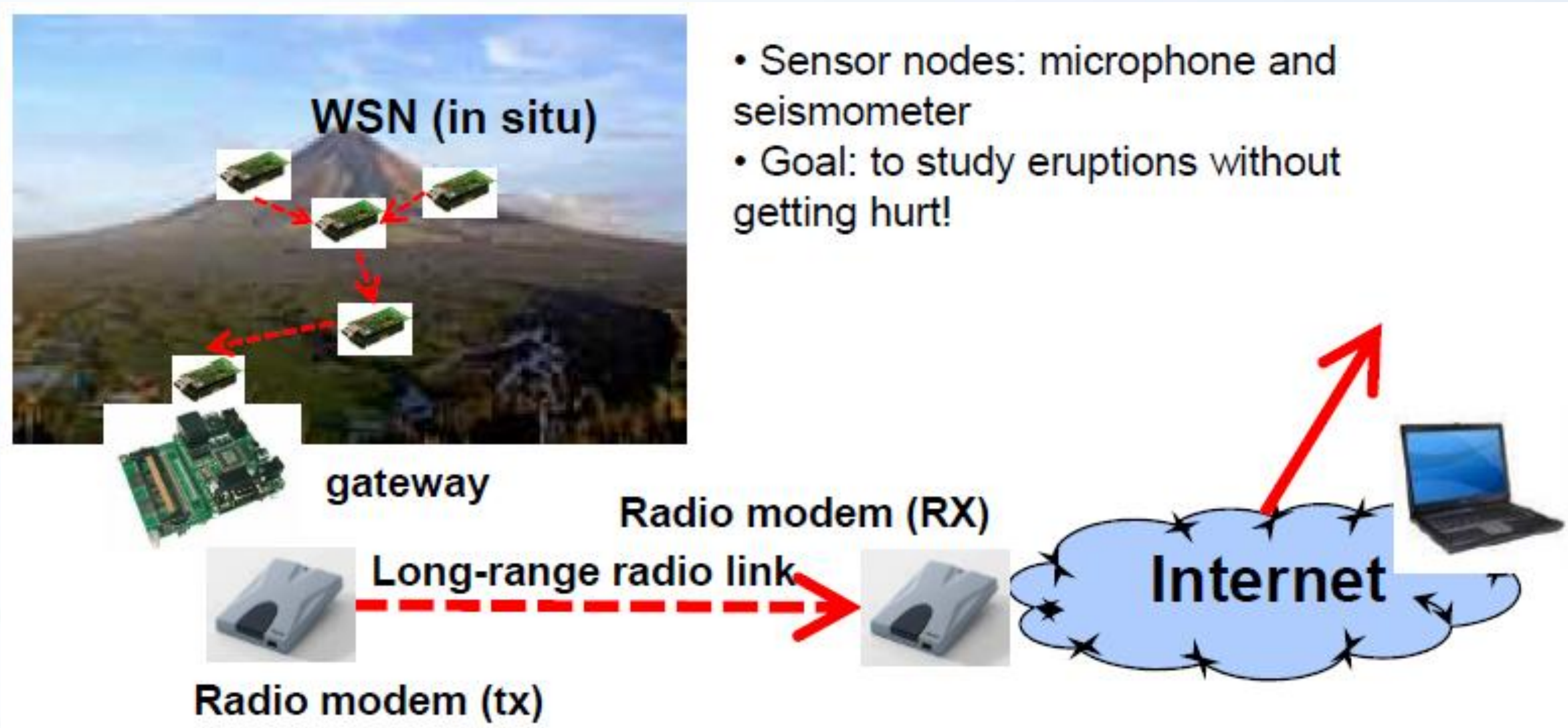
- Disaster relief operations
  - Drop sensor nodes from an aircraft over a wildfire
  - Each node measures temperature
  - Derive a "temperature map"
- Biodiversity mapping
  - Use sensor nodes to observe wildlife



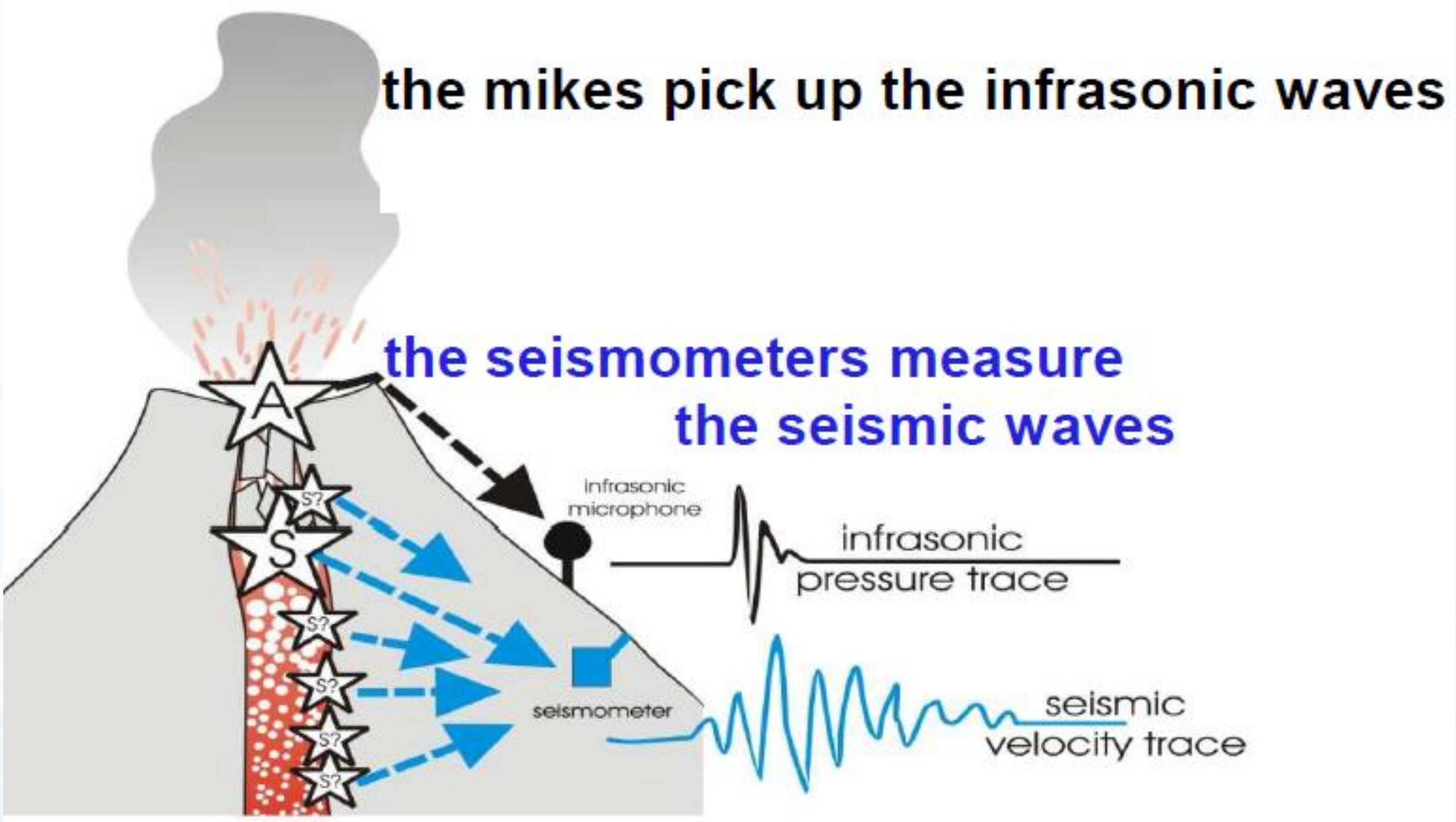


WSN Examples continued

Volcano Monitoring



WSN Examples continued
Volcano Monitoring



The main challenges of WSN

Ad hoc deployment: Most sensor nodes are deployed in regions which have no infrastructure at all. A typical way of deployment in a forest would be tossing the sensor nodes from an are plane. In such a situation, it is up to the nodes to identify its connectivity and distribution.

Unattended operation: In most cases, once deployed, sensor networks have no human intervention. Hence the nodes themselves are responsible for reconfiguration in case of any changes.

Energy: The sensor nodes are not connected to any energy source. There is only a finite source of energy, which must be optimally used for processing and communication. Thus, in order to make optimal use of energy, communication should be minimized as much as possible.

Dynamic changes: It is required that a sensor network system be adaptable to changing connectivity (for e.g., due to addition of more nodes, failure of nodes etc.) as well as changing environment

Challenges continued

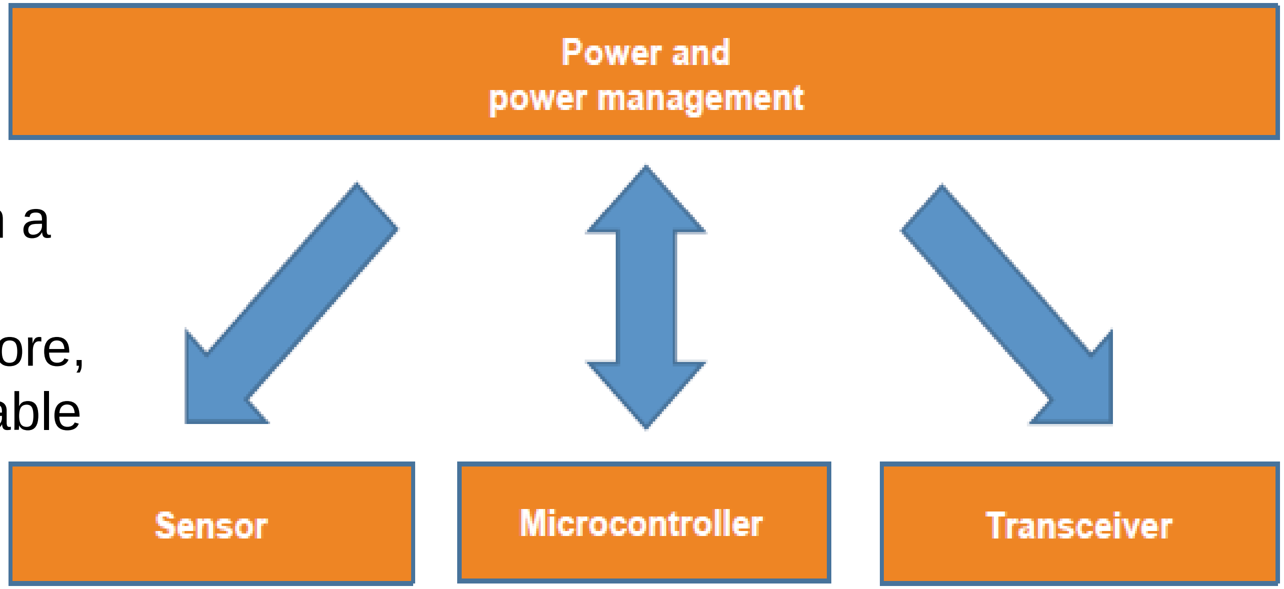
Challenges

- Limited battery power
- Limited storage and computation
- Lower bandwidth and high error rates
- Scalability to 1000s of nodes

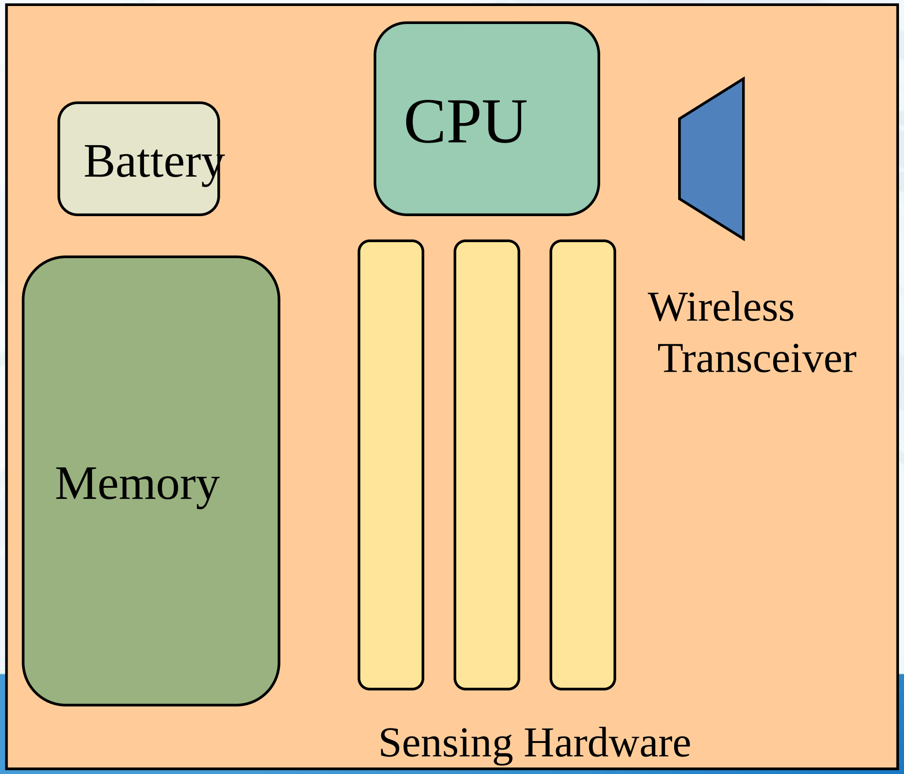
Network Protocol Design Goals

- Operate in self-configured mode (no infrastructure network support)
- Limit memory footprint of protocols
- Limit computation needs of protocols -> simple, yet efficient protocols
- Conserve battery power in all ways possible

Sensor nodes



A **microcontroller** is a small computer (SoC) on a single integrated circuit containing a processor core, memory, and programmable input/output peripherals.



UC Berkeley: Smart Dust

JPL: Sensor Webs

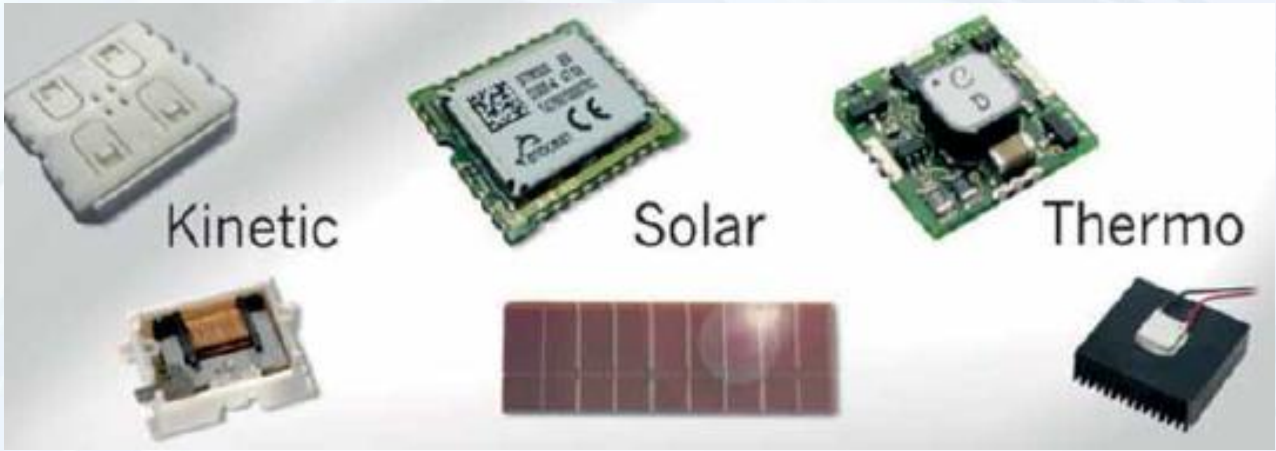
UC Berkeley: COTS Dust

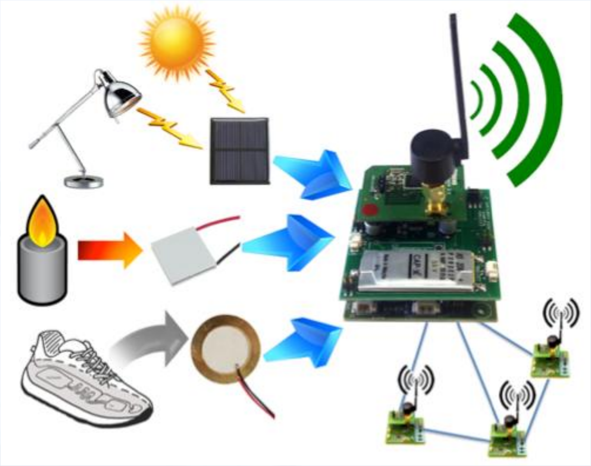
UC Berkeley: COTS Dust

Ambient Energy harvesting nodes

(ambient means surrounding)

- **Light energy harvesting devices, vibration energy harvesting devices and temperature-based** energy harvesting devices were provided for smart building lighting and air monitoring applications.
- Maintenance-free industrial wireless sensor nodes converts **mechanical vibration** into electrical energy used to perpetually power autonomous.
- For the monitoring applications of piping systems, a large number of products based on **temperature difference** energy harvesting have been developed.





Another approach to save energy and improve communication in WSN

- Implementation of protocols at different layers in the **protocol stack can significantly affect energy consumption, end-to-end delay, and system efficiency**. It is important to optimize communication and minimize energy usage.
- **Traditional networking protocols do not work well in a WSN** since they are not designed to meet these requirements. Hence, new energy-efficient protocols have been proposed.
- These protocols **employ cross-layer optimization** by supporting interactions across the protocol layers. Specifically, protocol state information at a particular layer is shared across all the layers to meet the specific requirements of the WSN.

Access Network Technologies of WSN

- The two main wireless standards used by WNS are **802.15.4 (2 layer in the OSI model)** and **Zigbee (3 layer in the OSI model).**
- They are low-power protocols
- Max distance is around 100 m (at 2.4Ghz)
- Main purpose of ZigBee is to create a **network topology (hierarchy)** to let a number of devices communicate among them and to **set extra communication features** such as authentication, encryption, association and in the upper layer application services.

- 802.11 – Wireless Local Area Networks (WiFi)
  - 802.11a, 802.11b, 80211g, 802.11n
- 802.15 – Wireless Personal Access Networks (WPAN)
  - Task Group 1 – Bluetooth (802.15.1)
  - Task Group 2 – Co-existence (802.15.2)
  - Task Group 3 – High Rate WPAN (802.15.3)
  - Task Group 4 – Low Rate WPAN (802.15.4 or 802.15 TG4)
  - Task Group 5 – Mesh Networking (802.15.5)
- 802.16 – Wireless Metropolitan Area Networks (WiMax)
- 802.20 – Mobile Broadband Wireless Access (Mobile-Fi) - Defunct
- 802.22 – Wireless Regional Access Network (WRAN)
  - Utilise free space in the allocated TV spectrum

Layer	Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Advantages of 802.15.4 standard in WSN

Why is it good **against interference:**

- Carrier Sense Multiple Access-Collision Avoidance (**CSMA-CA**): each node listen the medium prior to transmit. If the energy found is higher than a specific level, the transceiver waits for a random time (in an interval) and tries again.
- Guarantee Time Slots (**GTS**). This systems uses a centralized node (PAN coordinator) which gives slots of time to each node so that any knows when they have to transmit. There are 16 possible slots of time.

Why is it **low power:**

- It is ready to work with low-duty cycles. It means that the transceiver can be sleeping most of the time (up to 99% on average) while the receiving and sending tasks can be set to take just a small part of the devices' energy.
- This percentage depends on the kind of communication model used.

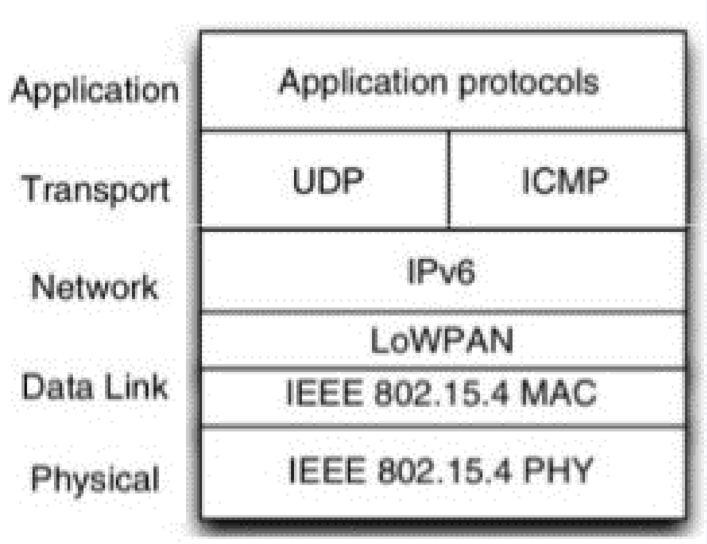
Advantages of ZigBee standard in WSN

ZigBee offers basically four kinds of different services:

- **Encryption** services (application and network keys implement extra 128b AES encryption)
- Association and **authentication** (only valid nodes can join to the network).
- **Routing** protocol: AODV, a reactive ad hoc protocol has been implemented to perform the data routing and forwarding process to any node in the network.
- **Application** Services: An abstract concept called "cluster" is introduced. Each node belongs to a predefined cluster and can take a predefined number of actions. Example: the "house light system cluster" can perform two actions: "turn the lights on", and "turn the lights off".

IPv6-based Low power Wireless Personal Area Networks **6LoWPAN** in WSN

- IPv6-based Low power Wireless Personal Area Networks **enables IPv6 packets communication over an IEEE 802.15.4** based network.
- Low power device can **communicate directly with IP devices** using IP based protocols.



- Because IPv6 packet sizes are much larger than the frame size of IEEE 802.15.4, an adaptation layer is used. The adaptation layer carries out **the functionality for header compression**. With header compression, smaller packets are created to fit into an IEEE 802.15.4 frame size.

Deployment of Sensor Nodes

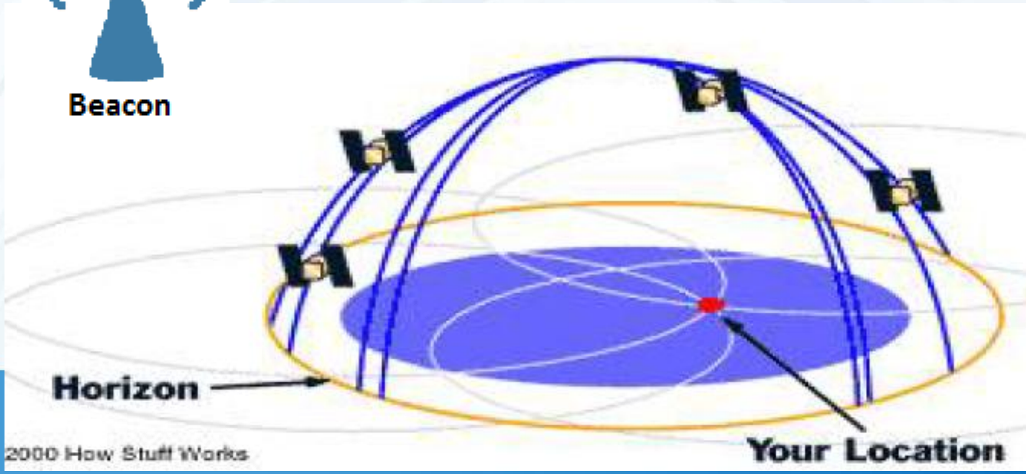
- Dropped from aircraft: ***Random deployment***
  - Usually uniform random distribution for nodes over finite area is assumed
- Well planned, fixed: ***Regular deployment***
  - E.g., in preventive maintenance or similar
  - Not necessarily geometric structure, but that is often a convenient assumption
- ***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

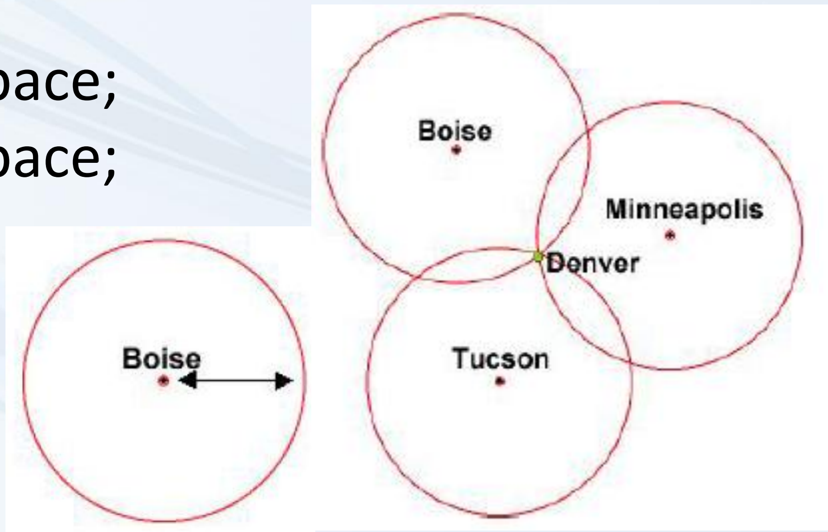
An **ad hoc deployment is preferred** over pre-planned deployment when the environment is inaccessible by humans

Localization (important for random deployment)

no *priori* knowledge of location. The problem of estimating spatial-coordinates is called **localization**

- **GPS:** (1) can work only outdoors; (2) GPS receivers are expensive and not suitable in the construction of small cheap sensor nodes; (3) cannot work in the presence of any obstruction like dense trees, leaves
- **Beacon identification:** network is organized as a hierarchy with the nodes in the upper level being more complex and already knowing their location through some technique (say, through GPS). Beacon approaches are:
  - iterative trilateration in 2D space;
  - iterative trilateration in 3D space;



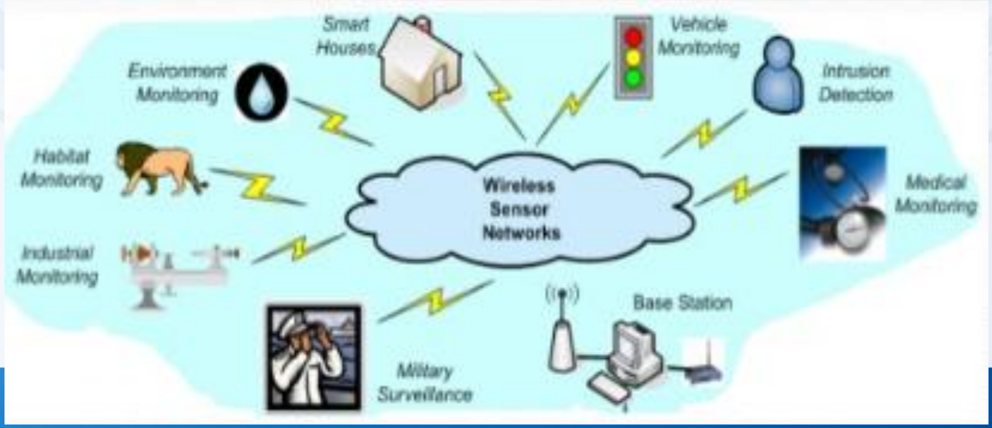


Sensing techniques

Data Diffusion Model:

- *Source*: A sensor node that generates data, based on its sensing mechanisms’ observations
- Event: Something that needs to be reported, e.g. in target detection; some abnormal activity
- Sink: A node, randomly located in the field, that is interested in events and seeks such information

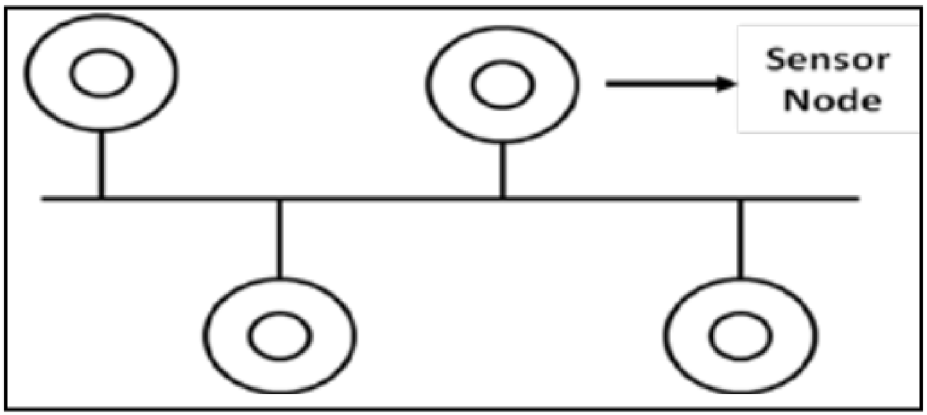
For example, consider a system which is used to measure temperature at a particular location. Then, the name [type=temperature, location=N-E, temperature=103] refers to all the sensors located at the northeast quadrant with a temperature reading of 103F.



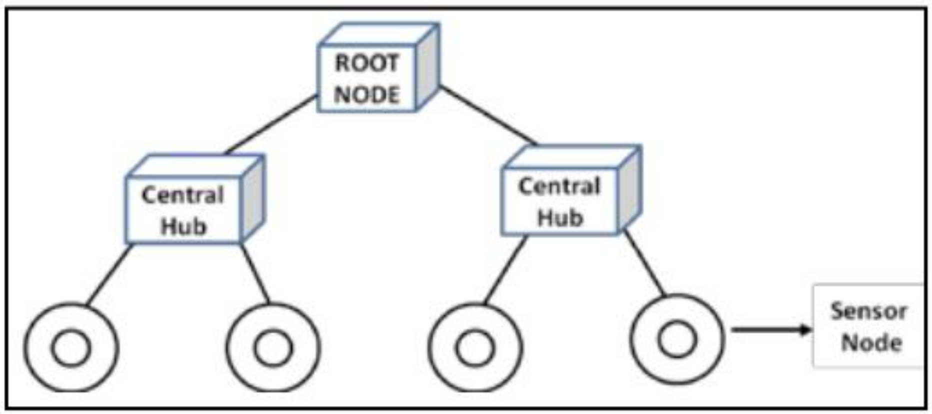
Network topologies

One-way and Bi-directional topologies

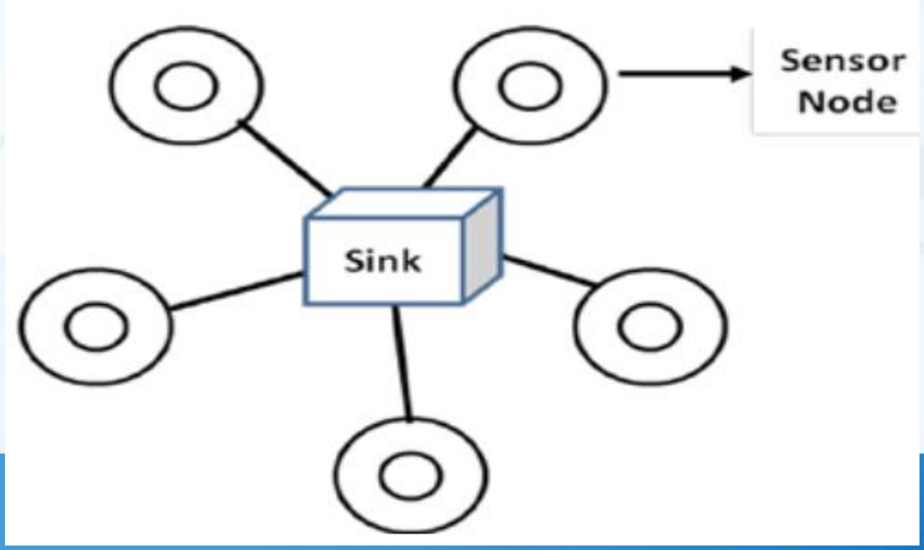
Bus Topology



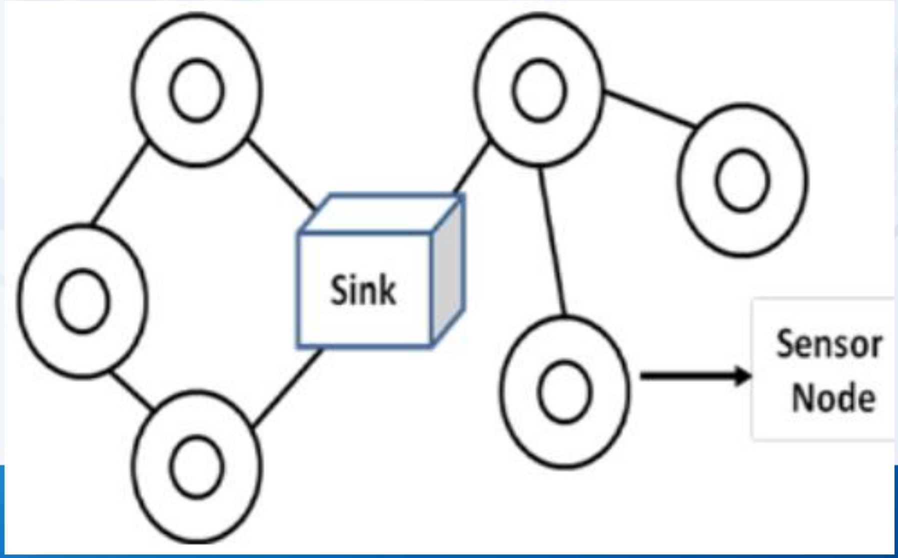
Tree Topology



Star Topology



Mesh Topology

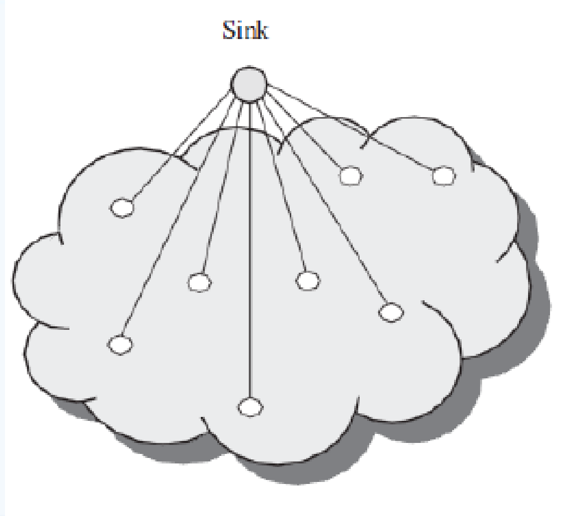


Network Architecture in WSN

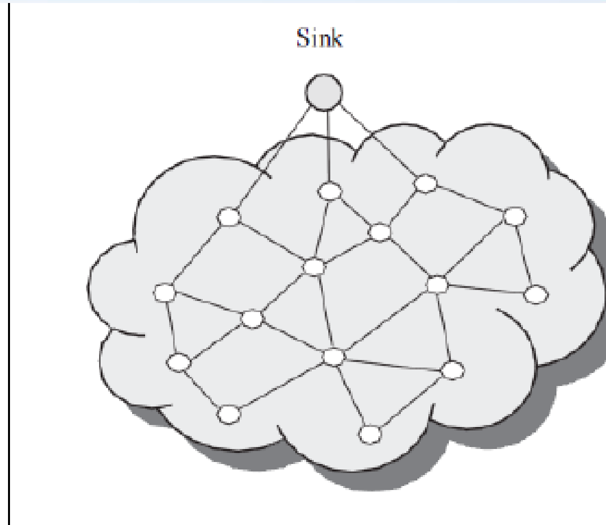
Flat Architecture – each node plays the same role in performing sensing task and all sensor nodes are peers

Hierarchical Architecture

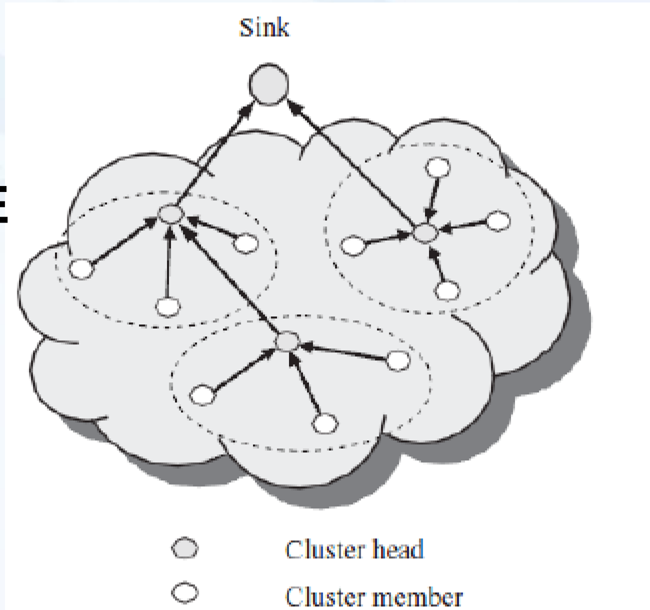
Sensor nodes are organized clusters, where the cluster members send their data to the sink.



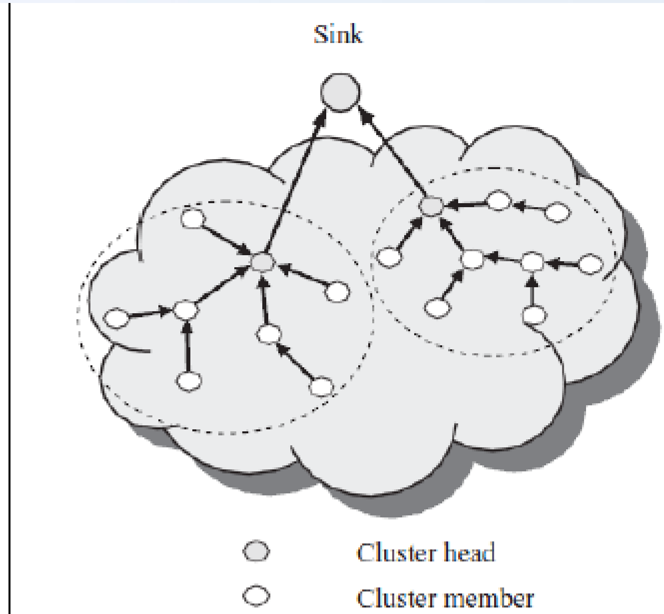
Single-hop network



Multi-hop network



Single-hop clustering architecture



Multi-hop clustering architecture

REASONS OF THESE TOPOLOGIES?!

THANK YOU