Wireless Sensor Networks

Definitions

- a WSN is a wireless network consisting of spatially distributed autonomous devices called sensor nodes to cooperatively monitor physical or environmental conditions at different locations.
- a WSN is a computer network consisting of a number of small, intercommunicating computers equipped with one or several sensors, where each small computer represents a node of the network.

Definitions

- a WSN is a "network of devices and these nodes are commonly known as nodes, which can sense the environment and communicate the information gathered from the monitored field through wireless links.
- the data is forwarded, possibly via multiple hops, to a sink that can use it locally or is connected to other networks through a gateway.
- The nodes can be stationary or moving.
- They can be aware of their location or not.
- They can be homogeneous or not.

Definitions

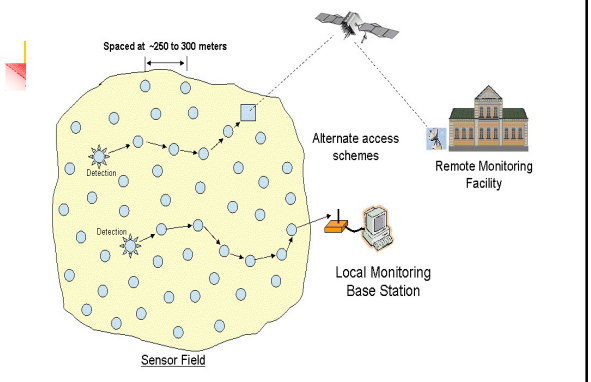
- a WSN can therefore be defined as a collection of sensors
- that are able to sense the environment
- by collecting the data about an event and then process that data,
- which is then transmitted to the workstation for interpretation and necessary action.

WSNs vs Traditional systems

- Wireless sensor networks are different from traditional sensors systems in that,
- 1) traditional sensors are positioned far from actual phenomenon being studied while as for WSN the sensor nodes are closely deployed near or inside the phenomenon,
- 2) Traditional sensors only perform the duty of sensing while nodes in WSNs perform sensing, data processing and data communication.

WSNs vs Traditional systems

- 3) The positions and topology of traditional sensors are engineered or pre determined in advance
- while for WNS the positions of nodes and topology are determined at the time of implementation.



WSNs Vs Wireless Ad hoc Networks

- WSNs are sometimes erroneously considered as a special type of wireless ad hoc networks by many people including some researchers.
- This conclusion could lead to incorrect conclusions and decisions, especially when it comes to the design of protocols and algorithms for ad hoc networks and trying to use them in WSNs.

WSNs Vs Wireless Ad hoc Networks

- Wireless ad hoc networks in their simplest form can be defined as "networks formed dynamically by an autonomous system of nodes connected via wireless links without using an existing network infrastructure or centralized administration".

WSNs Vs Wireless Ad hoc Networks

- In an ad hoc network, as the name implies, nodes or computing devices are connected through "ad hoc", "improvised", or "unplanned" topologies and
- set up and cleared according to user needs and temporary conditions.

features associated with wireless ad hoc networks

- 1) usually unplanned and highly dynamic;
- 2) nodes are "smart" terminals, for example, laptops, etc.;
- 3) typical applications include real-time or non-real-time data, multimedia, voice;

features associated with wireless ad hoc networks

- 4) every node can be either source or destination of information or both;
- 5) every node can be a router towards other nodes;
- 6) energy conservation is not the most relevant matter;
- 7) capacity is the most relevant matter.

features associated with wireless ad hoc networks

- There is a clear distinction from the above, between WSNs and wireless ad hoc networks
- apart from the very first feature "usually unplanned and highly dynamic",
- which is common to both WSNs and wireless ad hoc networks..

features associated with wireless sensor networks

- 1) nodes are normally not smart terminals, but simple and less complex devices;
- 2) the typical applications are normally not real time but require few bytes sent periodically or upon request or according to some external event;

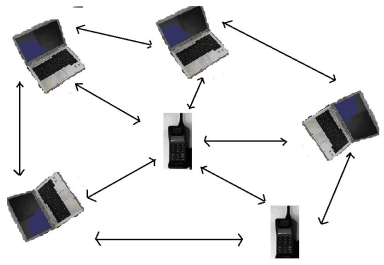
features associated with wireless ad hoc networks

- 3) every node can be either source or destination of information, not both;
- 4) some nodes do not play the role of routers;
- 5) and most importantly energy efficiency is a very relevant matter, while capacity is not for most applications.

features associated with wireless ad hoc networks

- Therefore from the above distinctions we would conclude that WSNs are not a special case of wireless ad hoc networks.
- Thus, a lot of care must be used when considering protocols and algorithms which are good for ad hoc networks, and using them in the context of WSNs.

An example of a wireless Ad hoc network



Sensor Nodes

- The major component of a WSN is a sensor node
- and the basic role of a sensor node is to sense or collect data from the environment in which it is deployed.
- Sometimes some sensor nodes may act as data sources on one hand and act as relaying stations on the other hand,
- where they are expected to receive and forward data from neighboring nodes.

Sensor Nodes

- There is also one or more particular sensor node(s) that act as base stations
- and represents the data sink in the network.
- The basic function of the base station node(s) is that of receiving and aggregating all the data generated within the network.

Sensor Nodes

- In addition, the base station establishes a communication link to a data logging unit or a remote site,
- for example, a control centre, using standard wired or wireless communication technologies like a wireless local area network (WLAN).

Sensor Nodes

- The communication between sensor nodes within the Wireless sensor network is established using radio frequency (RF) transmission techniques
- and the sensor nodes in the network may form a multi hop mesh network by establishing communication links to neighboring nodes.

Sensor Nodes

- Multi hop networks offer a number of advantages when monitoring data that has to be transmitted over long distances.
- Additionally multi hop networks are normally immune to sensor node failure and the high power efficiency make multi hop networks attractive for monitoring applications.

Sensor Nodes

- A sensor node in a WSN uses some energy in form of a signal and converts it into a reading for the purpose of information transfer.
- The sensor nodes are normally powered using an ordinary battery which requires charging and replacement as the case maybe
- and the sensor nodes' bandwidth for wireless communication is also limited.

Sensor Nodes

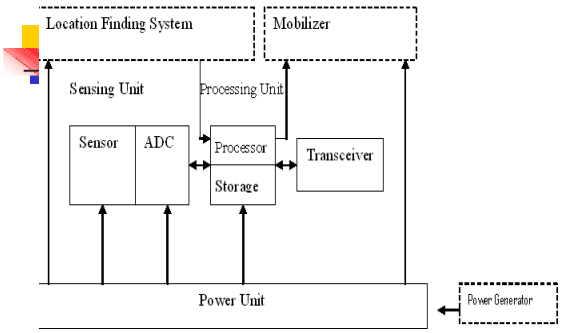
- Therefore, energy efficient Wireless sensor networks systems are needed for less consumption of the limited energy found in sensors.
- Moreover, the unattended nature of sensor nodes and the hazardous sensing environment prevents manual battery replacement and charging.

Sensor Nodes

- It is for these reasons that energy awareness or energy conservation becomes the key research challenge for sensor network protocol design

General architecture of a sensor node

- Sensor nodes in a wireless sensor network are basically equipped with a sensor, a processor, a transceiver and a power unit.
- The location finding system, the mobilizer and power generator can also be found in a sensor but they are optional.



General architecture of a sensor node

- The sensing unit is composed of a sensor and an Analogue to Digital converter, ADC
- and since the basic function of a sensor node is to obtain the characteristics of the environment in form of analogue signals,
- these signals are converted into digital data using the ADC and then the data is fed into the processing unit for processing and storage.

General architecture of a sensor node

- The processing unit is made of the processor and secondary storage.
- The transceiver is in charge of receiving data from other sensors and also in charge of transmitting data to other sensors or the base station.
- The power unit provides energy required for the sensor to perform its duty.

General architecture of a sensor node

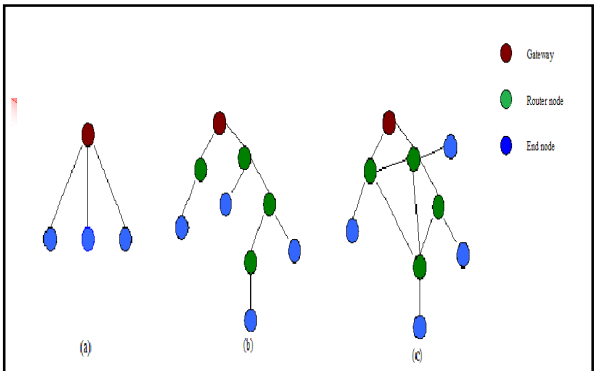
- It is normally made of an ordinary battery which can be recharged or replaced depending on the application and accessibility.
- The location finding system as the name suggests is responsible for locating the position of a particular sensor within the monitoring environment, in other words a sensor can be aware of its location using this unit.

General architecture of a sensor node

- And if the sensor does not have this unit, then it can be located by designing a localization algorithm.
- The mobilizer may be required in special cases in order to move the sensor node as and when it is needed to carry out assigned tasks and then finally
- the power generator generates power for the battery in the sensor.
- An example of a power generator can be a solar panel attached to the battery

WSN network topologies

- Several network topologies exist in WSNs to coordinate the gateway, end nodes, and router nodes.
- The router nodes in some cases are similar to the end nodes in that apart from acquiring measurement data, they can also be used to transmit along measurement data from other nodes in the network.



WSN network topologies

- The first and the most basic WSN topology is the star topology.
- In the star topology, each node in the network maintains a single and direct communication path with the gateway.
- This topology maybe simple but restricts the overall distance that the network can achieve.

WSN network topologies

- The second type of topology which can increase the distance a network can cover is a cluster, or tree topology.
- In this topology, each sensor node in the network is required to maintain one communication route to the gateway and
- at the same time can make use of other nodes to route its data along that path.

WSN network topologies

- This topology however has one big limitation,
- if a router node malfunctions, and then all the other nodes that are directly dependent on that router node automatically lose their communication paths to the gateway.

WSN network topologies

- The third type of topology which may remedy the limitation common with the tree topology is the mesh network topology.
- The mesh topology uses redundant communication paths to increase system reliability.
- In a mesh network, sensor nodes are expected to maintain a number of communication paths back to the gateway.

WSN network topologies

- this enables the network to automatically reroute the data through a different path if one router node goes down.
- The mesh topology, which can sometimes be very reliable, does suffer from an increase in network latency since the data is expected to make a number of hops before arriving at the gateway

The Open Systems Interconnection model (OSI model)

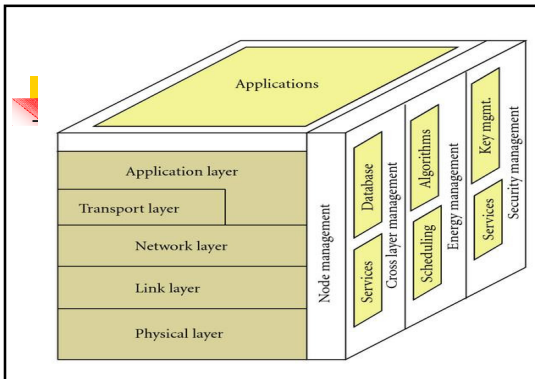
- was a product of the Open Systems Interconnection effort at the International Organization for Standardization.
- It is a way of sub-dividing a communications system into smaller parts called layers.
- Similar communication functions are grouped into logical layers.
- A layer provides services to its upper layer while receiving services from the layer below.

OSI model

- On each layer, an *instance* provides service to the instances at the layer above and requests service from the layer below.
- For example, a layer that provides error-free communications across a network provides the path needed by applications above it,
- while it calls the next lower layer to send and receive packets that make up the contents of that path.
- Two instances at one layer are connected by a horizontal connection on that layer.

WSNs protocol stack

- The protocol stack of a WSN consists of the following layers:
- the physical layer, data link layer, network layer, transport layer, application layer, power management plane, mobility management plane, and task management plane.



Physical layer

- The responsibilities of the Physical Layer are;
- selecting the frequency,
- generating the carrier frequency,
- detecting the signal, modulation, and encryption.
- Its main priority though is energy minimization and secondary concerns are the same as those of other wireless networks.

Data link layer

- The responsibilities of the Data Link Layer (DLL) are;
- data frame detection,
- multiplexing of data streams,
- medium access and error control.
- Due to the fact that the environment in which sensors maybe deployed may be noisy and since some sensor nodes maybe mobile,
- the medium access control (MAC) protocol on the DLL must be power-aware and should be able to reduce possible collisions with neighbors' broadcasts

Network layer

- The responsibility of the network layer is to take care of the routing of the data between nodes.
- It does this by handling how two sensor nodes will talk to each other,
- this layer is responsible for deciding which node to talk to.

Transport layer

- The transport layer comes into play when the system needs to communicate with the outside world.
- Communication from the sink to the user is normally problematic since communicating in Wireless Sensor Network is not based on global addressing associated with ordinary networks
- but the communication is based on attribute naming to indicate the destinations of the data packets.

Application layer

- The system administrators and programmers will interact with the Sensor Network using the Sensor Management Protocol (SMP) at the application layer.
- SMP, at the application layer is in charge of making the hardware and software of layers below in the stack transparent to the Sensor Network Management Applications.
- This layer should take into consideration the fact that WSNs use global identification and they are infrastructure less in nature.

Others layers

- A WSN architecture has an additional layer as shown in figure above,
- known as the management planes comprising a cross layer, an energy layer, a security layer and a node layer.
- The layers and planes mentioned above can be connected using well-defined interfaces.

The cross-layer management plane (CLAMP):

- This layer provides a mechanism that allows the exchange of cross-layer information in a non mandatory fashion so as to maintain what is referred to as layered Architecture modularity.
- The layer is also in charge of providing to all the modules of the Protocol stack a rich set of parameters.
- It achieves this by applying a technique known as publish-notify-update-query mechanism.

The energy management layer or plane:

- The wireless sensor is mostly characterized by its limited energy sources and the difficulty to replace batteries due to cost and geographic reasons.
- The EMP has the job of implementing certain algorithms that are used to calculate the capacity of the remaining battery.
- The EMP can also be used to implement algorithms that can reschedule different events such as updating timers, periodic listening and so on in order to save energy.

A security management plane (SMP):

- The duty of a security management plane (SMP) includes the integration of security-related issues.
- These issues include but are not limited to key management algorithms, data encryption, and data decryption and so on.

A security management plane (SMP):

- The issues are integrated into every component of the architecture,
- for example integrating TinySec into the link-layer security architecture can help detect unauthorized packets when they are first injected into the network.
- TinySec provides the basic security properties of message authentication and integrity using MAC.

Node management Layer NMP:

- The node management layer is responsible for tasks that include but are not limited to the following:
- the resetting deployed sensor nodes,
- the deployment of remote firmware, assigning node address,
- checking on the availability of the node, and so forth

Potential WSNs Applications

- Wireless sensor networks have numerous exciting applications in virtually all fields of science and engineering, including
- health care, industry, military, security, environmental science, geology, agriculture, and social studies.

Potential WSNs Applications

- In particular, the combination with macroscopic or MEMS-based actuators is intriguing because it permits manipulation of the environment in an unprecedented manner.
- Researchers and operators currently face a number of critical issues that need be resolved before these applications become reality.
- Wireless networking and distributed data processing of embedded sensing/actuating nodes under tight energy constraints demand new approaches to protocol design and hardware/software integration.