FACULTY OF EGINEERING AND TECHNOLOGY

WSN (MCS-033)

LECTURE -2

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

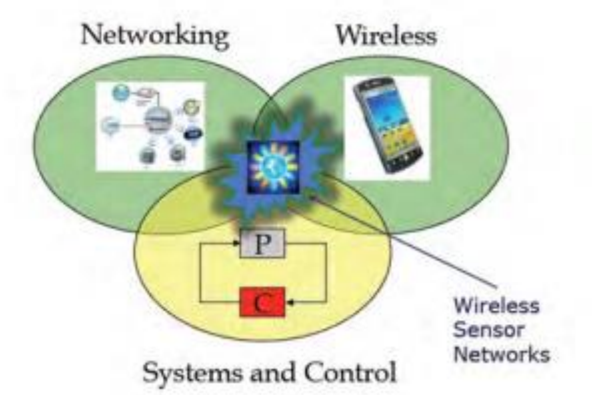
OUTLINE

- Introduction to WSN
- WSN Architecture and Protocol Stack
- Components of a node of a WSN
- Power consumption of a node to receive or transmit messages.
- WSN having a star topology
- WSN having with multihop communication.
- Challenges and Constraints
- ISO-OSI protocol stack for WSNs
- MCQ
- Reference

Introduction to WSN

Sensor nodes offer a powerful combination of distributed sensing, computing and communication. The ever-increasing capabilities of these tiny sensor nodes, which include sensing, data processing, and communicating, enable the realization of WSNs based on the collaborative effort of a number of other sensor nodes. They enable a wide range of applications and, at the same time, offer numerous challenges due to their peculiarities, primarily the stringent energy constraints to which sensing nodes are typically subjected.

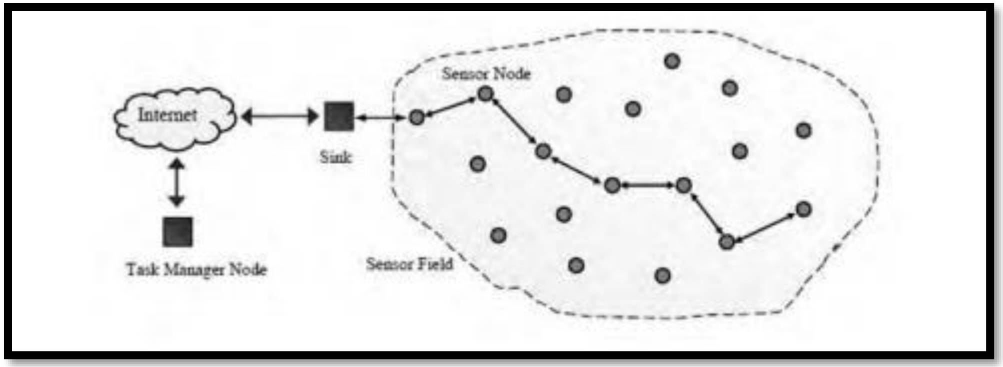
As illustrated in Figure WSNs incorporate knowledge and technologies from three different fields; Wireless communications, Networking and Systems and Control theory. In order to realize the existing and potential applications for WSNs, sophisticated and extremely efficient communication protocols are required. This chapter provides a first introduction to the WSNs, including architecture, specific characteristics and applications.



Areas of study that concur to the definition of WSNs

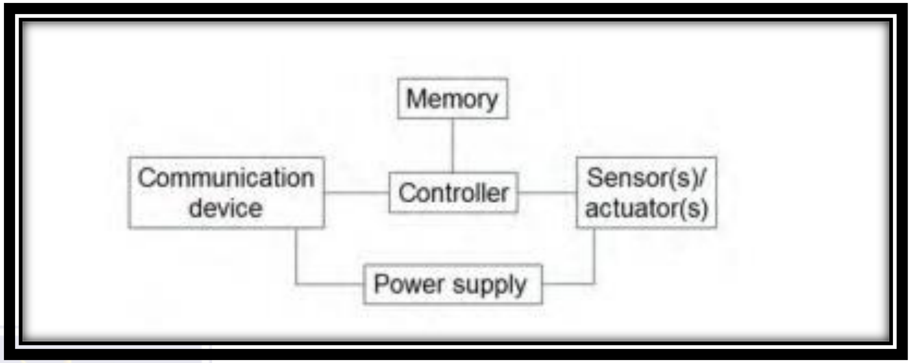
WSN Architecture and Protocol Stack

WSNs, as shown in Figure are composed of a number of sensor nodes, which are densely deployed either inside a physical phenomenon or very close to it. The sensor nodes are transceivers usually scattered in a sensor field where each of them has the capability to collect data and route data back to the sink/gateway and the end-users by a multi-hop infrastructure less architecture through the sink. They use their processing capabilities to locally carry out simple computations and transmit only the required and partially processed data. The sink may communicate with the task manager/end-user via the Internet or satellite or any type of wireless network (like Wi-Fi, mesh networks, cellular systems, WiMAX, etc.), making Internet of Things possible. However, in many cases the sink can be directly connected to the end-users. Note that there may be multiple sinks/gateways and multiple end-users in the architecture



A WSN connected to the Internet via a sink node

Components of a node of a WSN



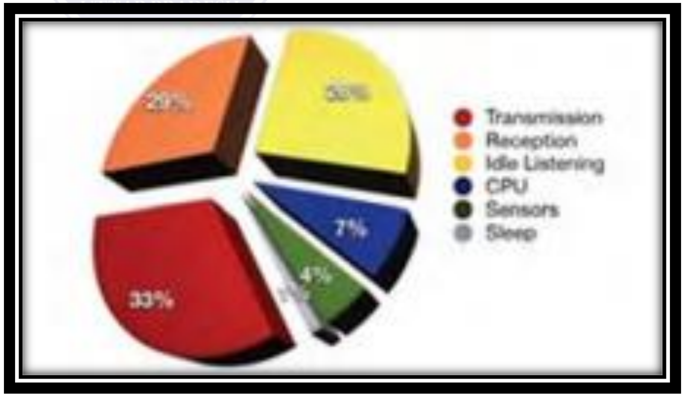
In WSNs, the sensor nodes have the dual functionality of being both data originators and data routers. Hence, communication is performed for two reasons:

• Source function: Each sensor node's primary role is to gather data from the environment through the various sensors. The data generated from sensing the environment need to be processed and transmitted to nearby sensor nodes for multi-hop delivery to the sink.

• Router function: In addition to originating data, each sensor node is responsible for relaying the information transmitted by its neighbors. The low-power communication techniques in WSNs limit the communication range of a node. In a large network, multi-hop communication is required so that nodes relay the information sent by their neighbors to the data collector, i.e., the sink. Accordingly, the sensor node is responsible for receiving the data sent by its neighbors and forwarding these data to one of its neighbors according to the routing decisions.

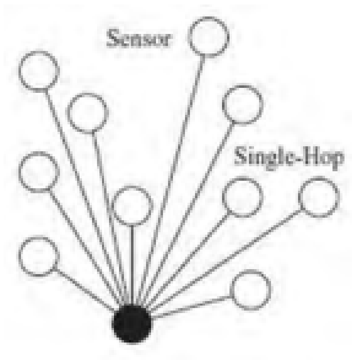
Power consumption of a node to receive or transmit messages.

Except for their transmit/receive operation state, transceivers can be put into an idle state (ready to receive, but not doing so) where some functions in hardware can be switched off, reducing energy consumption. The breakdown of the transceiver power consumption in Figure 1.4 shows that a transceiver expends a similar amount of energy for transmitting and receiving, as well as when it is idle. Moreover, a significant amount of energy can be saved by turning off the transceiver to a sleep state whenever the sensor node does not need to transmit or receive any data. In this state, significant parts of the transceiver are switched off and the nodes are not able to immediately receive something. Thus, recovery time and startup energy to leave sleep state can be significant design parameters.



INTRODUCTION TO WSN

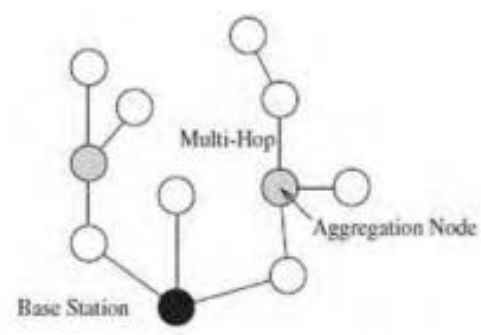
WSN having a star topology



When the transmission ranges of the radios of all sensor nodes are large enough and the sensors can transmit their data directly to the centralized base station, they can form a star topology as shown in Figure 1.5. In this topology, each sensor node communicates directly with the base station using a single hop.

WSN having with multihop communication.

However, sensor networks often cover large geographic areas and radio transmission power should be kept at a minimum in order to conserve energy; consequently, multi-hop communication is the more common case for sensor networks.



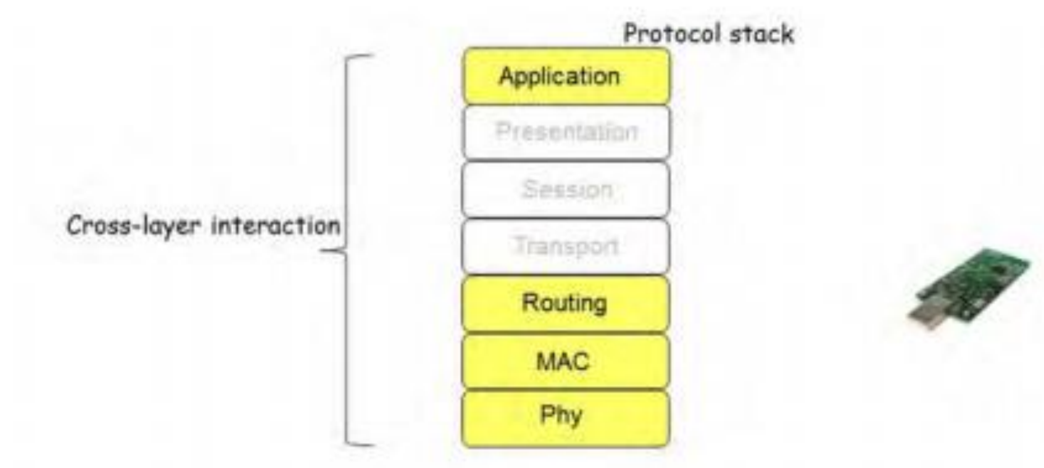
INTRODUCTION TO WSN

Challenges and Constraints

While WSNs share many similarities with other distributed systems, they are subject to a variety of unique challenges and constraints. These constraints impact the design of a WSN, leading to protocols and algorithms that differ from their counterparts in other distributed systems.

ISO-OSI protocol stack for WSNs

- ❑Energy
- ❑Node Deployment
- ❑Wireless Medium
- ❑Hardware Constraints
- ❑Security



MCQ

1. In wireless network an extended service set is a set of ________

a) connected basic service sets

b) all stations

c) all access points

d) connected access points

2. Mostly ________ is used in wireless LAN.

a) time division multiplexing

b) orthogonal frequency division multiplexing

c) space division multiplexing

d) channel division multiplexing

3. Which one of the following event is not possible in wireless LAN?

a) collision detection

b) acknowledgement of data frames

c) multi-mode data transmission

d) connection to wired networks

4. What is Wired Equivalent Privacy (WEP)?

a) security algorithm for ethernet

b) security algorithm for wireless networks

c) security algorithm for usb communication

d) security algorithm for emails

5. What is WPA?

a) wi-fi protected access

b) wired protected access

c) wired process access

d) wi-fi process access

REFERENCES

- https://www.kth.se/social/files/5431a388f276540a05ad2514/An_Introduction_WSNS_V1.8.pdf