10.4 Wireless Sensor Networks

Q.1. *Write note on Wireless Sensor Networks (WSNs).* **[May 11, Dec. 11] (7 M)**

- Wireless sensor networks combine sensing, computation and communication into a single tiny device.
- The power of wireless sensor networks lies in the ability to deploy large number of nodes that can dynamically configure and adapt themselves to any environment.
- Adaptation mechanisms can respond to changes in network topologies or can decide the most efficient mode of operation as per the changes in the environment.
- Unlike traditional wireless devices, wireless sensor nodes need not communicate directly with the nearest high-power control tower or base station, but only with their local peers.
- Instead of relying on a pre-deployed infrastructure, each individual sensor or actuator becomes part of the overall infrastructure.
- Peer-to-peer networking protocols provide a mesh-like interconnect to shuttle data between thousands of tiny embedded devices.
- A core design challenge in wireless sensor networks is coping with the harsh resource constraints placed on individual devices.
- Embedded processors with kilobytes of memory must implement complex, distributed, ad-hoc networking protocols.
- Many constraints derive from the vision that these devices will be produced in vast quantities and must be small and inexpensive.
- The most difficult resource constraint to meet is power consumption.

10.4.1 Wireless Sensor Network Application Classes

(A) Data Collection and Periodic Reporting

- Applications in this class collect readings from a set of points in an environment over a period of time in order to detect trends and interdependencies.
- Examples include monitoring the humidity or mineral content of soil to decide the amount of water/fertilizers required.
- Environmental data collection applications typically use tree-based routing topologies where each routing tree is rooted at high-capability nodes that collect data.
- Once the network is configured, each node periodically samples its sensors and transmits its data up the routing tree and back to the base station.
- Rather than the data of individual nodes, the collective data is more important.
- The most important characteristics of this application class are long lifetime, precise synchronization, low data rates and relatively static topologies.

Scanned by CamScanner

(B) Event Detection /Security Monitoring

- Security monitoring networks are composed of nodes that are placed at fixed locations throughout an environment that continually monitor one or more sensors to detect an anomaly.
- A key difference between security monitoring and environmental monitoring is that security networks are not actually collecting any data.
- Each node has to frequently check the status of its sensors but it only has to transmit a data report when there is a security violation.
- Once detected, a security violation must be communicated to the base station/sink immediately.
- The network must be configured such that nodes are responsible for confirming the status of each other. If a node were to be disabled or fail, it would represent a security violation that should be reported.
- The immediate and reliable communication of alarm messages is the primary system requirement.

(C) Tracking Based Applications

- There are many situations where one would like to track the location of valuable assets or personnel.
- Examples include tracking of livestock, birds or tracking a shipment of goods or vehicles and so on.
- Objects can be tracked by simply tagging them with a small sensor node.
- The sensor node will be tracked as it moves through a field of sensor nodes that are deployed in the environment at known locations.
- Unlike sensing or security networks, node tracking applications will continually have topology changes as nodes move through the network.
- While the connectivity between the nodes at fixed locations will remain relatively stable, the connectivity to mobile nodes will be continually changing.
- Additionally the set of nodes being tracked will continually change as objects enter and leave the system.
- It is essential that the network be able to efficiently detect the presence of new nodes that enter the network.

(D) Sink Initiated Querying

- Unlike the above mentioned applications, in this class of applications the base station can query a set of sensors for data.
- This allows the sink to get data 'on demand' from different parts of the network.
- E.g. in a logistics handling system, the sink could query different sensors for the current/last known location of an asset.

(E) Hybrid Networks

- Complete application scenarios may contain aspects of all the above categories.

Scanned by CamScanner

- E.g. in a network designed to monitor traffic and track vehicles that pass through it, the network may switch between being an alarm monitoring network and a data collection network.
- During the long periods of inactivity when no vehicles are present, the network will simply perform an alarm monitoring function. Each node will monitor its sensors waiting to detect a vehicle.
- Once an alarm event is detected, all or part of the network will switch into a data collection network and periodically report sensor readings up to a base station that tracks the vehicles progress.
- Then again it may raise an alarm for specified conditions such as if the vehicle is above the speed limit.

10.5 Personal Area Networks (PAN)

- A *Personal Area Network (PAN)* is a computer network used for communication among various devices such as telephones, laptops, printers and PDAs, in close proximity to an individual.
- PANs can be used to transfer files including email and calendar appointments, digital photos and music.
- Range of PANs is usually limited to about 10 meters.
- Personal Area Networks can be wired or wireless.
  - USB and FireWire technologies often link together a wired PAN.
  - Wireless PANs typically use technologies such as IrDA, Bluetooth, *Ultra-wideband (UWB)* and ZigBee.
- Each technology is optimized for specific usage, applications, or domains.
- However, Bluetooth is the most widely used technology for WPAN communication.
- IEEE 802.15 Working Groups is the organization to define WPAN technologies.
- It includes seven task groups, the most relevant of them are listed below.

(1) Task Group 1 (IEEE 802.15.1)

- Based on the Bluetooth v1.1 specifications.
- It includes a media access control and physical layer specification.
- An updated version of this standard, based upon the additions incorporated into Bluetooth v1.2, was published as IEEE 802.15.1-2005.

(2) Task Group 3 (IEEE 802.15.3)

- This is a high rate WPAN system also known as Ultra-wideband or UWB.
- UWB supports data speeds ranging from 20 Mbps to 1 Gbps, for multimedia applications.

(3) Task Group 4 (IEEE 802.15.4)

- This is a low rate WPAN system also known as ZigBee.
- Provides data speeds of 20 kbps or 250 kbps, for home control type of low power and low cost solution

Scanned by CamScanner