SRI MUTHUKUMARAN INSTITUTE OF TECHNOLOGY

(Approved by AICTE, Accredited by NBA and Affiliated to Anna University, Chennai)
Chikkarayapuram (Near Mangadu), Chennai- 600 069.

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

CEC365 – WIRELESS SENSOR NETWORK DESIGN
(REGULATION – 2021)

YEAR: III **SEM: V**

UNIT I - INTRODUCTION

PART- A

1. Define Wireless Sensor Networks.

Wireless sensor network (WSN) is a distributed, infrastructure less wireless network that contains a set of connected tiny sensors nodes, which communicate with each other and exchange information and data. These nodes obtain information on the environment such as temperature, pressure, humidity or pollutant and send this information to a base station or sink where the data can be observed and analysed.

2. Give the Characteristics of Wireless Sensor Network.

- Power consumption constraints for nodes using batteries or energy harvesting
- Chance to cope with node failures
- Mobility of nodes
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Capability to withstand harsh environmental conditions
- Simplicity of use
- Cross layer design

3. Give the advantages of WSN.

- Network setups can be carried out without fixed infrastructure.
- Suitable for the non – reachable places such as over the sea, mountains, rural areas or deep forests.
- Flexible if there is random situation when additional workstation is needed.
- Implementation pricing is cheap
- It avoids plenty of wiring.
- It might accommodate new devices at any time.
- It’s flexible to undergo physical partitions.
- It can be accessed by using a centralized monitor.

4. Define Life Time of a Sensor Node.

The time until the first node fails is the network lifetime or the time until the network is disconnected into two or more partitions, or the time until 50% of nodes have failed, or the time when for the first time a point in the observed region is no longer covered by atleast a single sensor node.

5. Define Data Centric and Address Centric Networks.

Address-Centric: Transfer of data between two specific devices, each with one network address as in traditional communication networks.

Data Centric: In WSN, where nodes are deployed redundantly to protect against node failures the identity of the node supplying data is not important. Importance is given only to the data. Hence a data centric paradigm is necessary in designing WSN.

6. Write the fundamental technologies needed for Wireless Sensor Network.

- Miniaturization of hardware
- Processing and communication
- Sensing equipment

7. What are the Deployment options of Wireless Sensor Network?

Fixed deployment: Well planned deployment of sensor network.

Random deployment: By dropping a large number of nodes from an aircraft over a forest fire.

8. How WSN is used in intelligent buildings?

Buildings waste vast amounts of energy by inefficient Humidity, Ventilation, Air Conditioning. A better real-time monitoring of temperature, airflow, humidity and other physical parameters in a building by means of a WSN can considerably increase the comfort level of inhabitants and reduce the energy consumption.

9. Give few examples of Facility management application of WSN.

- Keyless entry applications where people wear badges that allow a WSN to check which person is allowed to enter which areas of a larger company site.
- Detection of intruders to company sites.
- A wide area WSN could track a Vehicle's position and alert security personnel.
- A WSN could be used in a chemical plant to scan for leaking chemicals.
- These applications require large number of sensors and they should be able to operate a long time on batteries.

10. What are the Hardware components of a Single Node in WSN?

- Controller
- Memory
- Sensors and Actuators
- Communication Devices
- Power Supply Unit

11. What are the characteristics of a transceiver to be taken into account for using in WSN?

The most important characteristics of a transceivers are: Service to upper layer, power consumption and energy efficient state change times and energy, Data rates, Modulations, Transmission power control etc.

12. What is a Sensor? Give its categories.

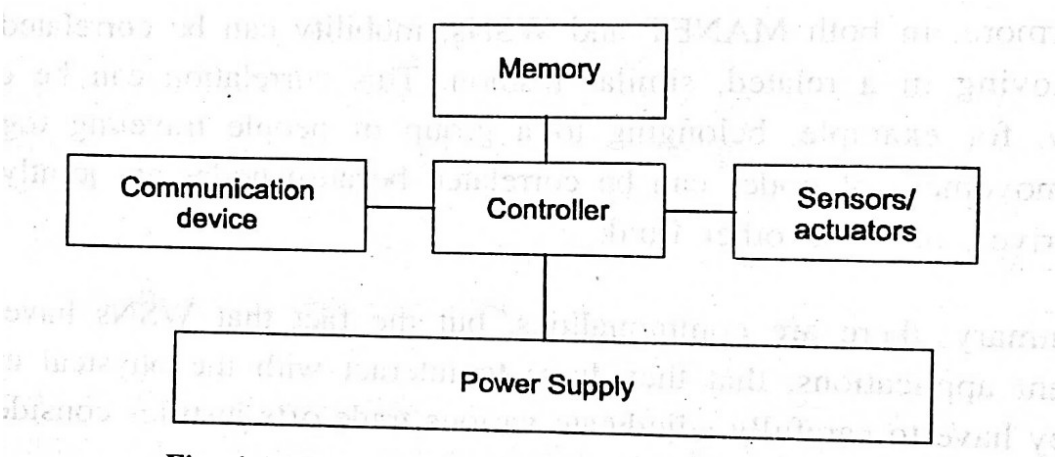
Sensors are tiny nodes used to obtain information on the environment such as temperature, pressure, humidity or pollutant. Sensors can be roughly categorized into three categories:

- Passive, Omni directional sensors
- Passive, narrow-beam sensors
- Active sensors.

13. List the components of WSN involved in energy consumption.

- Operation states with different power consumption
- Microcontroller Energy consumption
- Memory Energy consumption
- Radio Transceivers Energy consumption
- Power consumption of Sensor and Actuators

14. Draw the overview of Sensor Node Components.



15. What are the three types of mobility?

In Wireless senor networks, mobility can appear in three main forms:

Node mobility: The wireless sensor nodes themselves can be mobile. The meaning of such mobility is highly application dependent.

Sink mobility: Information sinks can be mobile. While this can be a special case of node mobility, the important aspect is the mobility of an information sink that is not part of the sensor network.

Event mobility: In application like event detection and in particular in tracking applications, the cause of the events or the objects to be tracked can be mobile

16. What is Network lifetime?

The time for which the network is operational or, put another way, the time during which it is able to fulfil its tasks (starting from a given amount of stored energy). It is not quite clear, however, when this time ends.

17. What do you mean by Scalability in wireless sensor network?

The ability to maintain performance characteristics irrespective of the size of the network is referred to as scalability.

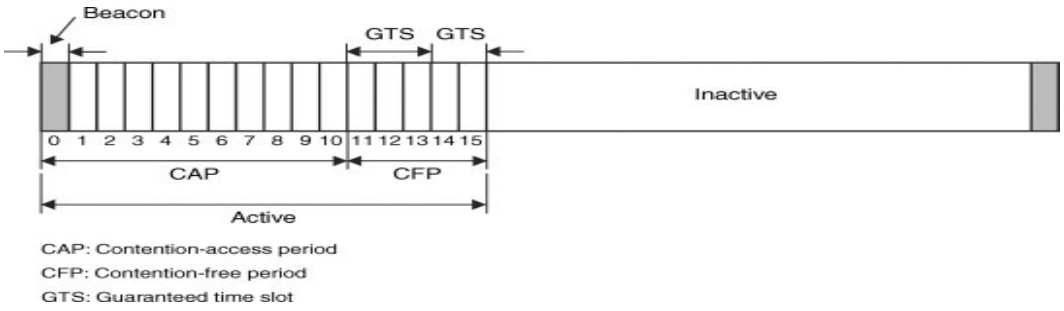
18. What is GTSDesc Persistence Time?

In GTS management, after receiving the acknowledgment packet, the device is required to track the coordinator's beacons for some specified time called GTSDesc Persistence Time.

19. What is Logical Link Control and Adaptation Protocol (L2CAP)?

This is the protocol with which most applications would interact unless a host controller is used. L2CAP supports protocol multiplexing to give the abstraction to each of the several applications running in the higher layers as if it alone is being run. Since the data packets defined by the baseband protocol are limited in size, L2CAP also segments large packets from higher layers such as RFCOMM or SDP into multiple smaller packets prior to their transmission over the channel.

20. Draw the Super Frame Structure of IEEE 802.15.4.



21. What is Noise Figure?

The noise figure NF of an element is defined as the ratio of the Signal-to-Noise Ratio (SNR) ratio SNRI at the input of the element to the SNR ratio SNRO at the element's output:

$$NF = SNRI / SNRO$$

It describes the degradation of SNR due to the element's operation and is typically given in dB: NF dB= SNRI dB − SNRO dB.

22. What is event & Sink?

The node that generates data is called source and the information to be reported is called an event. A node which interested in an event is called sink.

23. What is Receiver sensitivity?

The receiver sensitivity (given in dBm) specifies the minimum signal power at the receiver needed to achieve a prescribed Eb /N0 or a prescribed bit/packet error rate.

24. Define transceivers in WSN.

The essential task is to convert a bit stream coming from a microcontroller (or a sequence of bytes or frames) and convert them to and from radio waves. It is usually convenient to use a device that combines these two tasks in a single entity. Such combined devices are called **transceivers**.

25. Write short notes on memory devices in WSN.

There is a need for Random Access Memory (RAM) to store intermediate sensor readings, packets from other nodes, and so on. While RAM is fast, its main disadvantage is that it loses its content if power supply is interrupted. ROM, PROM, EPROM, EEPROM can be used to store the data.

26. Differentiate adhoc networks and wireless sensor networks.

Features	Wireless Sensor Networks	Ad hoc Networks
Number of Sensor Nodes	Large in Quantity	Medium in quantity
Deployment Type	Very much dense	Scattered
Rate of failure	More	Very rare
Battery	Not Rechargeable / Hard to recharge	Rechargeable
Redundancy	High	Low
Data rate	Low	High
Change in network topology	Frequency	Rare

27. What do you mean by energy scavenging in a senor node?

Depending on application, high capacity batteries that last for long times, that is, have only a negligible self-discharge rat, and that can efficiently provide small amounts of current. Ideally, a sensor node also has a device for energy scavenging, recharging the battery with energy gathered from the environment – solar cells or vibration-based power generation are conceivable options.

PART - B

1. Illustrate the challenges and the required mechanisms of a Wireless Sensor network.

Characteristic requirements

In order to perform many applications in WSN, the following characteristics must be taken into consideration.

Type of service

- The service type rendered by a conventional communication network is evident – it moves bits from one place to another. For a WSN, moving bits is only a means to an end, but not the actual purpose.
- Additionally, concepts like *scoping* of interactions to specific geographic regions or to time intervals will become important.
- Hence, new paradigms of using such a network are required, along with new interfaces and new ways of thinking about the service of a network.

Quality of Service

- Traditional quality of service requirements
  – usually coming from multimedia-type applications
  – like bounded delay or minimum bandwidth are irrelevant when applications are tolerant to latency or the bandwidth of the transmitted data is very small in the first place.
- In some cases, only occasional delivery of a packet can be more than enough; in other cases, very high reliability requirements exist.
- In yet other cases, delay *is* important when actuators are to be controlled in a real-time fashion by the sensor network.

Fault tolerance

- Nodes may run out of energy or might be damaged, or since the wireless communication between two nodes can be permanently interrupted.
- It is important that the WSN as a whole is able to tolerate such faults.

Lifetime

- In many scenarios, nodes will have to rely on a limited supply of energy (using batteries).
- Replacing these energy sources in the field is usually not practicable, and simultaneously, a WSN must operate at least for a given mission time or as long as possible.
- Hence, the **lifetime** of a WSN becomes a very important figure of merit.
- Evidently, an energy-efficient way of operation of the WSN is necessary.
- The lifetime of a network also has direct trade-offs against quality of service: investing more energy can increase quality but decrease lifetime.
- The precise *definition of lifetime* depends on the application at hand. A simple option is to use the time until the first node fails (or runs out of energy) as the network lifetime.
- Other options include the time until the network is disconnected in two or more partitions.

Scalability

- Since a WSN might include a large number of nodes, the employed architectures and protocols must be able scale to these numbers.

Wide range of densities

- In a WSN, the number of nodes per unit area – the *density* of the network – can vary considerably. Different applications will have very different node densities.
- The network should adapt to such variations.

Programmability

- Nodes should be programmable, and their programming must be changeable during operation when new tasks become important.
- A fixed way of information processing is insufficient.

Maintainability

- As both the environment of a WSN and the WSN itself change (depleted batteries, failing nodes, new tasks), the system has to adapt.
- It has to monitor its own health and status to change operational parameters or to choose different trade-offs (e.g. to provide lower quality when energy resource become scarce).

Required mechanisms

- To realize these requirements, innovative mechanisms for a communication network have to be found, as well as new architectures, and protocol concepts.
- A particular challenge here is the need to find mechanisms that are sufficiently specific to the given application to support the specific quality of service, lifetime, and maintainability requirements .
- Some of the mechanisms that will form typical parts of WSNs are:

Multihop wireless communication

- In particular communication over long distances is only possible using prohibitively high transmission power.
- The use of intermediate nodes as relays can reduce the total required power.
- Hence *multihop communication* will be a necessary ingredient.

Energy-efficient operation

- To support long lifetimes, energy-efficient operation is a key technique.
- Energy-efficient data transport between two nodes (measured in J/bit) based on energy-efficient determination of requested information.

Auto-configuration

- A WSN will have to configure most of its operational parameters autonomously, independent of external configuration.
- The total number of nodes and simplified deployment will require that capability in most applications.

Collaboration and in-network processing

- In some applications, a single sensor is not able to decide whether an event has happened.
- But several sensors have to collaborate to detect an event and only the joint data of many sensors provides enough information.

- Information is processed in the network itself in various forms to achieve this collaboration, as opposed to having every node transmit all data to an external network and process it "at the edge" of the network.

Data centric

- In traditional communication networks the transfer of data between two specific devices, each equipped with (at least) one network address – the operation of such networks is thus **address-centric**.
- In **data-centric routing,** the sink which is responsible for gathering data and sending to the base station, issues a query for finding target data stored in the other nodes of WSN.

Locality

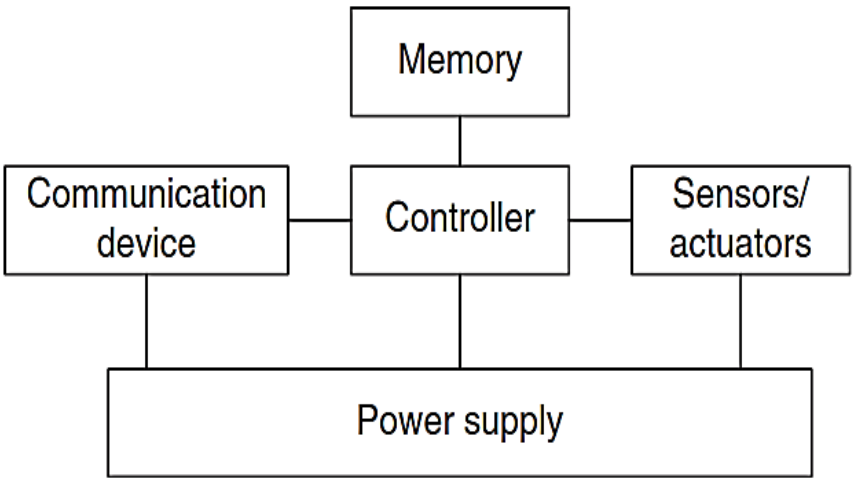
- Nodes, which are very limited in resources like memory, should attempt to limit the state that they accumulate during protocol processing to only information about their direct neighbors.

Exploit trade-offs

- WSNs will have to rely to a large degree on exploiting various inherent trade-offs between mutually contradictory goals, both during system/protocol design and at runtime.

2. Explain about the hardware components of sensor nodes.

- Building a wireless sensor network first of all requires the constituting nodes to be developed and available.
- These nodes have to meet the requirements that come from the specific requirements of a given application:
- They might have to be small, cheap, or energy efficient, they have to be equipped with the right sensors, the necessary computation and memory resources, and they need adequate communication facilities.



CONTROLLER

- The controller is the core of a wireless sensor node.
- It collects data from the sensors, processes this data, decides when and where to send it, receives data from other sensor nodes, and decides on the actuator's behavior.
- It is the Central Processing Unit (CPU) of the node.it is representing trade-offs between flexibility, performance, energy efficiency, and costs.

Microcontroller:

- Flexibility suited to embedded systems.
- Instruction set amenable to time-critical signal processing
- Low power consumption
- Have memory built in
- Freely programmable

Digital Signal Processors (DSPs)

- Specialized processor
- Special architecture and their instruction set, for processing large amounts of vectorial data.
- It is used to process data coming from a simple analog, wireless communication device to extract a digital data stream.
- Another option for the controller is Field-Programmable Gate Arrays (FPGAs) or Application-Specific Integrated Circuits (ASICs).
- *FPGA*- Time and energy consumption for reprogrammable.
- *ASIC*- Less flexibility, costly hardware.
- In WSN application, the duties of the sensor nodes do not change over lifetime and where the number of nodes is big enough to warrant the investment in ASIC development is the superior solution.

MEMORY

- There is a need for Random Access Memory (RAM) to store intermediate sensor readings, packets from other nodes, and so on. While RAM is fast, its main disadvantage is that it loses its content if power supply is interrupted.
- ROM, PROM, EPROM, EEPROM can be used to store the data.
- Correctly dimensioning memory sizes, especially RAM, can be crucial with respect to manufacturing costs and power consumption.

COMMUNICATION DEVICE

- The communication device is used to exchange data between individual nodes.
- Radio Frequency (RF)-based communication provides relatively long range and high data rates, acceptable error rates at reasonable energy expenditure, and does not require line of sight between sender and receiver.

Transceivers:

- The essential task is to convert a bit stream coming from a microcontroller (or a sequence of bytes or frames) and convert them to and from radio waves.
- It is usually convenient to use a device that combines these two tasks in a single entity. Such combined devices are called **transceivers**.
- A range of low-cost transceivers is commercially available that incorporate all the circuitry required for transmitting and receiving – modulation, demodulation, amplifiers, filters, mixers, and so on.

Transceiver tasks and characteristics

- To select appropriate transceivers, a number of characteristics should be taken into account.

Service to upper layer

- Most notably to the Medium Access Control (MAC) layer. Sometimes, this service is **packet oriented**; sometimes, a transceiver only provides a **byte interface** or even only a **bit interface** to the microcontroller.

Power consumption and energy efficiency

- Energy efficiency is the energy required to transmit and receive a single bit.
- Transceivers should be switchable between different states, for example, active and sleeping.
- The idle power consumption in each of these states and during switching between them is very important.

Carrier frequency and multiple channels

- Transceivers are available for different carrier frequencies; evidently, it must match application requirements and regulatory restrictions.
- It is often useful if the transceiver provides several carrier frequencies to choose from, helping to alleviate some congestion problems in dense networks.
- Such as FDMA or multichannel CSMA/ ALOHA techniques.

Data rates

- Carrier frequency and used bandwidth together with modulation and coding determine the gross data rate. Typical values are a few tens of kilobits per second.

Modulations -Several of on/off-keying, ASK, FSK, or similar modulations.

Noise figure

- The **noise figure** is defined as the ratio of the Signal-to-Noise Ratio (SNR) ratio SNR*I at* the input of the element to the SNR ratio SNR*O at* the element's output.

$$NF = SNRi/SNRo$$

Receiver sensitivity

- The receiver sensitivity (given in dBm) specifies the minimum signal power at the receiver needed to achieve a prescribed Eb /N0 or a prescribed bit/packet error rate.

Blocking performance

- The blocking performance of a receiver is its achieved bit error rate in the presence of an interferer.

Frequency stability

- The **frequency stability** denotes the degree of variation from nominal center frequencies when environmental conditions of oscillators like temperature or pressure change.

Transceiver operational states

- Many transceivers can distinguish four operational states

Transmit -In the **transmit state**, the transmit part of the transceiver is active and the antenna radiates energy.

Receive -In the **receive state** the receive part is active.

Idle

- A transceiver that is ready to receive but is not currently receiving anything is said to be in an **idle state**.

- In this idle state, many parts of the receive circuitry are active, and others can be switched off.

Sleep

- In the **sleep state**, significant parts of the transceiver are switched off.
- These sleep states differ in the amount of circuitry switched off and in the associated **recovery times** and **startup energy.**

Wakeup Receivers

- To keep this specialized receiver simple, it suffices for it to raise an event to notify other components of an incoming packet; upon such an event, the main receiver can be turned on and perform the actual reception of the packet.
- Such receiver concepts are called wakeup **receivers.**

SENSORS

- **Passive, omnidirectional sensors -**Thermometer, light sensors, vibration, microphones, humidity, mechanical stress or tension in materials
- **Passive, narrow-beam sensors -** Camera, which can "take measurements" in a given direction, but has to be rotated if need be.
- **Active sensors -** a sonar or radar sensor or some types of seismic sensors.

Each sensor node has a certain **area of coverage** for which it can reliably and accurately report the particular quantity that it is observing.

ACTUATORS

- Actuators are just about as diverse as sensors,
- This controls a motor, a light bulb, or some other physical object is not really of concern to the way communication protocols are designed.

POWER SUPPLY OF SENSOR NODES

- **Traditional batteries**
- ✓ The power source of a sensor node is a battery, either non rechargeable ("primary batteries") or rechargeable ("secondary batteries").
- **Capacity**
- ✓ They should have high capacity at a small weight, small volume, and low price. The main metric is energy per volume, J/cm3
- **Capacity under load**
- ✓ They should withstand various usage patterns as a sensor node can consume quite different levels of power over time and actually draw high current in certain operation modes.
- **Self-discharge**
- ✓ Their self-discharge should be low; they might also have to last for a long time
- **Efficient recharging**
- ✓ Recharging should be efficient even at low and intermittently available recharge power;
- **Energy scavenging**
- ✓ Energy from a node's environment must be tapped into and made available to the node – **energy scavenging** should take place.
- **Photovoltaic -**The well-known solar cells can be used to power sensor nodes.
- **Vibrations-** One almost pervasive form of mechanical energy is vibrations.

3. Explain the physical layer and transceiver design considerations in WSNs.

Some of the most crucial points influencing PHY design in WSNs are:

- Low power consumption;
  - ✓ Consequence 1: small transmit power and thus a small transmission range;
  - ✓ Consequence 2: low duty cycle; most hardware should be switched off or operated in a low power standby mode most of the time;
- Low data rates (tens to hundreds kb/s);
- Low implementation complexity and costs;
- Low degree of mobility;
- A small form factor for the overall node;
- Low cost;

Energy usage profile:

- The radiated energy is small but the overall transceiver consumes much more energy than is actually radiated; for ex. for the Mica motes, 21 mW are consumed in transmit mode and 15 mW in received mode for a radiated power of 1 mW;
- For small transmit powers the transmit and receive modes consume more or less the same power; therefore it is important to put the transceiver into sleep state instead of idle state;
- This rises the problem of startup energy/ startup time which a transceiver has to spend upon waking up from sleep mode, for example, to ramp up phase – locked loops or voltage – controlled oscillators; during this startup time, no transfer of data is possible; for example, the μAMPS-1 transceiver needs 466 μs and a power dissipation of 58 mW; therefore, going into sleep mode is unfavourable when the next wakeup comes fast;
- Computation is cheaper than communication: the ratio is hundreds to thousands of instructions/ 1 transmitted bit;

Choice of modulation scheme:

- The choice of modulation scheme depends on several aspects, including technological factors, packet size, target error rate and channel error model;
- The power consumption of a modulation scheme depends much more on the symbol rate than on the data rate; it leads to desire of high data rates at low symbol rates which ends to m – ary modulation schemes; trade – offs:
  - ⚠ M – ary modulation schemes require more hardware than 2 – ary schemes;
  - ⚠ M – ary modulation schemes require for increasing m an increased Eb/N0 ratio;
  - ⚠ Generally, in WSN applications most packets are short; for them, the startup time dominates overall energy consumption making the other efforts irrelevant;
- Dynamic modulation scaling is necessary;

Antenna considerations:

- The small form factor of the overall sensor restricts the size and the number of antennas;
- If the antenna is much smaller than the carrier's wavelength, it is hard to achieve good antenna efficiency and transmitted energy must increase;
- In case of multiple antennas, they should be spaced apart at least 40 – 50% of the wavelength used to achieve good effects; for ex. for 2.4 GHz, a spacing of 5 – 6 cm between the antennas is necessary, which is difficult to be accepted;
- Radio waves emitted from antennas close to the ground, typical in some applications, are faced with higher path – loss coefficients than the common value of $\alpha = 2$; a typical value, considering the obstacles too, is $\alpha = 4$;

- Nodes randomly scattered on the ground, deployed from an aircraft, will land in random orientations, with the antennas facing the ground or being otherwise obstructed; this can lead to nonisotropic propagation of the radio wave, with considerable differences in the strength of the emitted signal in different directions.

4. Explain the Sensor Network Scenarios with neat diagram.

Types of sources and sinks

- Several typical interaction patterns found in WSNs – event detection, periodic measurements, function approximation and edge detection, or tracking.
- A source is any entity in the network that can provide information, that is, typically a sensor node; it could also be an actuator node that provides feedback about an operation.
- A sink, on the other hand, is the entity where information is required.
- There are essentially three options for a sink: it could belong to the sensor network as such and be just another sensor/actuator node or it could be an entity outside this network.
- For this second case, the sink could be an actual device, for example, a handheld or PDA used to interact with the sensor network.
- It could also be merely a gateway to another larger network such as the Internet, where the actual request for the information comes from some node "far away" and only indirectly connected to such a sensor network.
- These main types of sinks are illustrated by below figure, showing sources and sinks in direct communication.

Single-hop versus Multihop networks

- The inherent power limitation of radio communication follows a limitation on the feasible distance between a sender and a receiver.

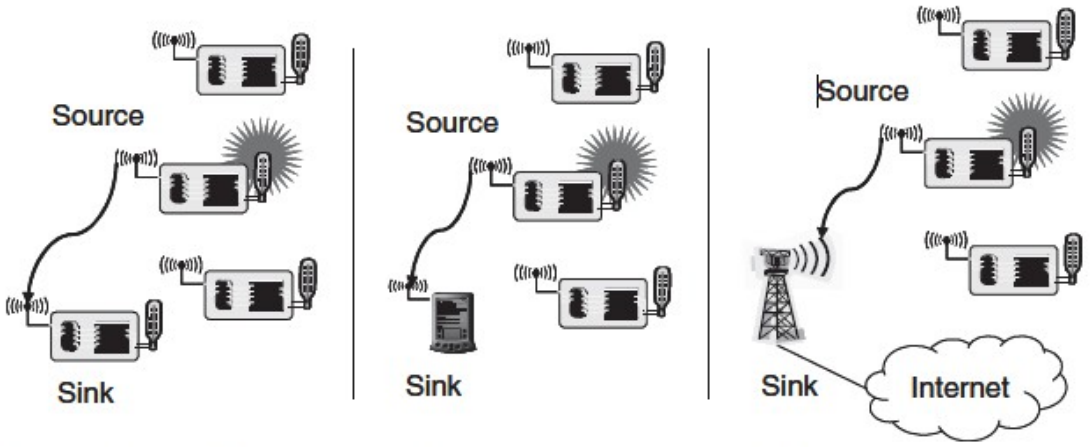


Figure 3.1 Three types of sinks in a very simple, single-hop sensor network

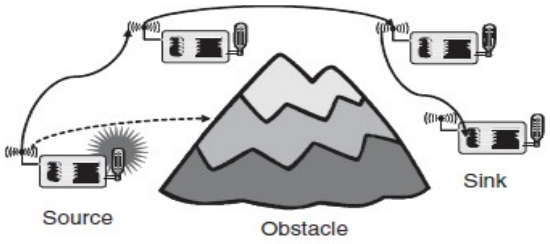


Figure 3.2 Multihop networks: As direct communication is impossible because of distance and/or obstacles, multihop communication can circumvent the problem

- Because of this limited distance, the direct communication between source and sink is not always possible, specifically in WSNs, which are intended to cover a lot of ground (e.g. in environmental or

agriculture applications) or that operate in difficult radio environments with strong attenuation (e.g. in buildings).

- To overcome such limited distances, an obvious way out is to use relay stations, with the data packets taking multi hops from the source to the sink.
- This concept of multihop networks for WSNs as the sensor nodes themselves can act as such relay nodes.
- Depending on the particular application, the likelihood of having an intermediate sensor node at the right place can actually be quite high.
- While multihopping is the solution to overcome problems with large distances or obstacles, it has been claimed to improve the energy efficiency of communication.
- The attenuation of radio signals is at least quadratic in most environments (and usually larger), it consumes less energy to use relays instead of direct communication.
- When targeting for a constant SNR at all receivers, the *radiated* energy required for direct communication over a distance d is $cd\alpha$ (c some constant, $\alpha \geq 2$ the path loss coefficient).
- Using a relay at distance $d/2$ reduces this energy to $2c(d/2)\alpha$.
- But this calculation considers only the radiated energy, not the actually *consumed* energy – in particular, the energy consumed in the intermediate relay node.
- Only for large d does the radiated energy dominate the fixed energy costs consumed in transmitter and receiver electronics.
- The concrete distance where direct and multihop communication are in balance depends on a lot of device-specific and environment-specific parameters.
- It should be pointed out that only multihop networks operating in a **store and forward** fashion. In such a network, a node has to correctly receive a packet before it can forward it somewhere.

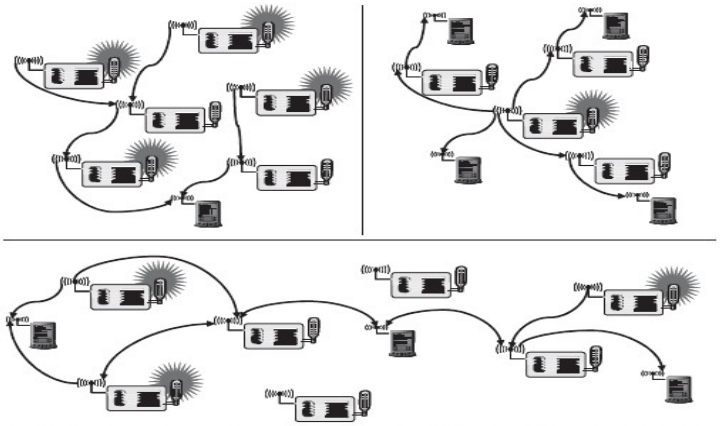


Figure 3.3 Multiple sources and/or multiple sinks. Note how in the scenario in the lower half, both sinks and active sources are used to forward data to the sinks at the left and right end of the network

Multiple sinks and sources

- In many cases, there are multiple sources and/or multiple sinks present.
- In the most challenging case, multiple sources should send information to multiple sinks, where either all or some of the information has to reach all or some of the sinks. The above figure illustrates these combinations.

Three types of mobility

- In wireless sensor networks, mobility can appear in three main forms:

Node mobility

- The wireless sensor nodes themselves can be mobile. The meaning of such mobility is highly application dependent.
- In examples like environmental control, node mobility should not happen; in livestock surveillance (sensor nodes attached to cattle, for example), it is the common rule.
- In the face of node mobility, the network has to reorganize itself frequently enough to be able to function correctly.

- It is clear that there are trade-offs between the frequency and speed of node movement on the one hand and the energy required to maintain a desired level of functionality in the network on the other hand.

Sink mobility

- The information sinks can be mobile.
- The important aspect is the mobility of an information sink that is not part of the sensor network, for example, a human user requested information via a PDA while walking in an intelligent building.
- In a simple case, such a requester can interact with the WSN at one point and complete its interactions before moving on.

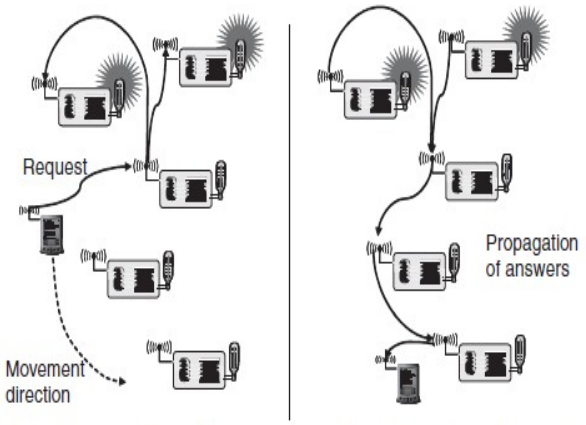


Figure 3.4 A mobile sink moves through a sensor network as information is being retrieved on its behalf

- A mobile requester is particularly interesting, however, if the requested data is not locally available but must be retrieved from some remote part of the network.
- Hence, while the requester would likely communicate only with nodes in its surrounding area, it might have moved to some other place.
- The network, possibly with the assistance of the mobile requester, must make provisions that the requested data actually follows and reaches the requester despite its movements.

Event mobility

- In applications like event detection and in particular in tracking applications, the cause of the events or the objects to be tracked can be mobile.
- In such scenarios, it is important that the observed event is covered by a sufficient number of sensors at all time.
- Hence, sensors will wake up around the object, engaged in higher activity to observe the present object, and then go back to sleep.
- As the event source moves through the network, it is accompanied by an area of activity within the network – this has been called the *frisbee* model.

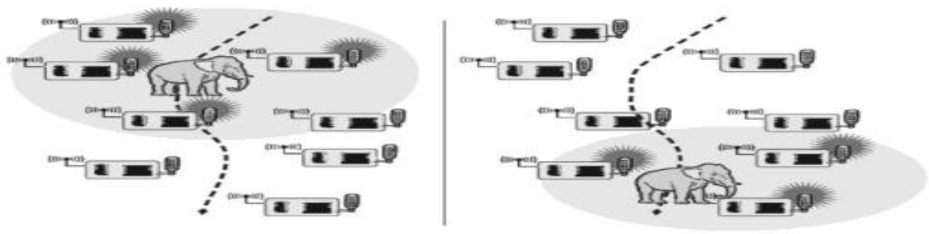


Fig.2.10 Detection of an event – an elephant that moves through the network along with the event source

5. Explain the optimization goals and figure of merit.

- For all these scenarios and application types, different forms of networking solutions can be found.
- The challenging question is how to optimize a network, how to compare these solutions, how to decide which approach better supports a given application, and how to turn relatively imprecise optimization goals into measurable figures of merit?

1. Quality of service

- WSNs differ from other conventional communication networks mainly in the type of service they offer. These networks essentially only move bits from one place to another.
- Possibly, additional requirements about the offered Quality of Service (QoS) are made, especially in the context of multimedia applications.
- Such QoS can be regarded as a low-level, networking-device-observable attribute – bandwidth, delay, jitter, packet loss rate – or as a high-level, user-observable, so-called subjective attribute like the perceived quality of a voice communication or a video transmission.
- But just like in traditional networks, high-level QoS attributes in WSN highly depend on the application. Some generic possibilities are:

Event detection/reporting probability

- What is the probability that an event that actually occurred is not detected or, more precisely, not reported to an information sink that is interested in such an event? For example, not reporting a fire alarm to a surveillance station would be a severe shortcoming.

Clearly, this probability can depend on/be traded off against the overhead spent in setting up structures in the network that support the reporting of such an event (e.g. routing tables) or against the run-time overhead (e.g. sampling frequencies).

Event classification error

- If events are not only to be detected but also to be classified, the error in classification must be small.

Event detection delay

- The delay between detecting an event and reporting it to any/all interested sinks.

Missing reports

- In applications that require periodic reporting, the probability of undelivered reports should be small.

Approximation accuracy

- For function approximation applications (e.g. approximating the temperature as a function of location for a given area), what is the average/maximum absolute or relative error with respect to the actual function? Similarly, for edge detection applications, what is the accuracy of edge descriptions; are some missed at all?

Tracking accuracy

- Tracking applications must not miss an object to be tracked, the reported position should be as close to the real position as possible, and the error should be small.

2. Energy efficiency

- Energy is a precious resource in WSN that energy efficiency should therefore make an evident optimization goal.
- It is clear that with an arbitrary amount of energy; most of the QoS metrics can be increased.
- Hence, putting the delivered QoS and the energy required to do so into perspective should give a first, reasonable understanding of the term energy efficiency.
- The most commonly considered aspects are:

Energy per correctly received bit

- How much energy, counting all sources of energy consumption at all possible intermediate hops, is spent on average to transport one bit of information (payload) from the source to the destination? This is often a useful metric for periodic monitoring applications.

Energy per reported (unique) event

- Similarly, what is the average energy spent to report one event? Since the same event is sometimes reported from various sources, it is usual to normalize this metric to only the unique events.

Delay/energy trade-offs

- Some applications can increase energy investment for a speedy reporting of such events. Here, the trade-off between delay and energy overhead is interesting.

Network lifetime

- The time for which the network is operational or, put another way, the time during which it is able to fulfill its tasks. It is not quite clear, however, when this time ends.

Time to first node death

- When does the first node in the network run out of energy or fail and stop operating?

Network half-life

- When have 50% of the nodes run out of energy and stopped operating. Any other fixed percentile is applicable as well.

Time to partition

- When the first partition of the network in two (or more) disconnected parts occur.
- This can be as early as the death of the first node or occur very late if the network topology is robust.

Time to loss of coverage

- A possible figure of merit is thus the time when for the first time any spot in the deployment region is no longer covered by any node's observations.

Time to failure of first event notification

- A network partition can be seen as irrelevant if the unreachable part of the network does not want to report any events in the first place.
- This can be due to an event not being noticed because the responsible sensor is dead or because a partition between source and sink has occurred.

3. Scalability

- The ability to maintain performance characteristics irrespective of the size of the network is referred to as scalability.

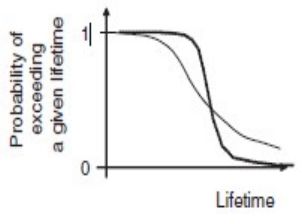


Figure 3.6 Two probability curves of a node exceeding a given lifetime – the dotted curve trades off better minimal lifetime against reduced maximum lifetime

4. Robustness

- WSN should exhibit an appropriate robustness.

They should not fail just because a limited number of nodes run out of energy, or because their environment changes, these failures have to be compensated by finding other routes.

6. Explain in detail about the applications of wireless sensor network.

(OR)

How the applications of Wireless Sensor Networks can be classified based on the interaction pattern

between sources and sinks?

Application Types

Applications of Wireless Sensor Networks can be classified based on the interaction pattern between sources and sinks. The classification is as follows:

Event detection

In this category of application, Sensor nodes should report to the sink once they have detected the occurrence of a specified event. The simplest event scan be detected locally by a single sensor node in isolation (e.g. a temperature threshold is exceeded). If several different events can occur, event classification is necessary.

Periodic measurements

In this type of applications sensors has to periodically report the measured values. The reporting period is application dependent.

Function approximation and edge detection:

Physical values like temperature which changes from one place to another can be regarded as a function of location. A WSN can be used to approximate this unknown function using a limited number of samples taken at each individual sensor node. This is function approximation.Similarly, finding edges or structures in such functions along the boundaries of patterns is called edge detection. Some applications are intended for function approximation and edge detection.

Tracking

This includes applications where the source of an event is mobile (e.g. an intruder in surveillance scenarios). The WSN can be used to report updates on the event source's position to the sink, like speed and direction.

Deployment options

- **Fixed deployment:** Well planned deployment of sensor nodes
- **Random deployment:** By dropping a large number of nodes from an aircraft over a forest fire.

Application Examples

On the basis of nodes that have different sensing facilities, in combination with computation and communication abilities, many different kinds of application scan be constructed, with very different types of nodes, even of different kinds within one application.

Disaster relief applications

One of the most important application of WSNs are disaster relief operations. A typical example is wildfire detection: Sensor nodes are equipped with thermometers and can determine their own location (relative to each other).These sensors are deployed over a wildfire, from an airplane. They collectively produce a "temperature map" of the area or determine the perimeter of areas with high temperature that can be accessed from the outside by fire fighters equipped with Personal Digital Assistants (PDAs). Similar scenarios are possible for the control of accidents in chemical factories.

Some of these disaster relief applications have similarities with military applications, where sensors should detect, enemy troops. In such an application,sensors should be cheap since a large number is necessary.

Environment control and biodiversity mapping

WSNs can be used to control the pollution in environment. A possible application is garbage dump sites. Another example is the surveillance of the marine ground floor to observe erosion processes for the construction of off shorewind farms.

WSNs are also used to find the number of plant and animal species that live in a given habitat (biodiversity mapping). The main advantages of WSNs here are the long-term, unattended, wirefree operation of sensors close to the object sand they never disturb the observed animals and plants.

Intelligent buildings

Buildings waste vast amounts of energy by inefficient Humidity, ventilation, Air Conditioning. A better real-time monitoring of temperature, airflow,humidity, and other physical parameters in a building by means of a WSN can considerably increase the comfort level of inhabitants and reduce the energy consumption.

In addition, sensor nodes can also be used to monitor mechanical stress levels of buildings and decide whether it is still safe to enter a given building after an earthquake. Similar systems can be applied to bridges. Other types of sensors can be used to detect people enclosed in a collapsed building and communicate with team.

Depending on the application, sensors can be fitted into existing buildings or have to be incorporated into the building already under construction

Facility management

In the management of facilities larger than a single building, WSNs also have a wide range of possible applications.

Simple examples include

- Keyless entry applications where people wear badges that allow a WSN to check which person is allowed to enter which areas of a larger company site.
- Detection of intruders, to company sites.
- A wide area WSN could track a vehicle's position and alert security personnel.

- A WSN could be used in a chemical plant to scan for leaking chemicals.
- These applications require large number of sensors and they should be able to operate a long time on batteries.

Machine surveillance and preventive maintenance

One idea is to fix sensor nodes to difficult to reach areas of machinery where they can detect vibration patterns that indicate the need for maintenance. Examples for such machinery could be robotics or the axles of trains.

The main advantage of WSNs here is the cable free operation, avoiding a maintenance problem in itself and allowing a cheap, often retrofitted installation of such sensors.

Precision Agriculture

Applying WSN to agriculture allows precise irrigation and fertilizing by placing humidity/soil composition sensors into the fields. A relatively small number of sensors are sufficient (one sensor per 100 m × 100 m area). Similarly, pest control can profit from a high-resolution surveillance of farm land. Also, live stock breeding can benefit from attaching a sensor to each pig or cow, which controls the health status of the animal (by checking body temperature, step counting, or similar means) and raises alarms if given thresholds are exceeded.

Medicine and health care

Health care applications of WSNs range from postoperative monitoring to long-term surveillance of (typically elderly) patients and automatic drug administration (embedding sensors into drug packaging, raising alarms when applied to the wrong patient). Also, patient and doctor tracking systems within hospitals can be literally life saving.

Telematics

Partially related to logistics applications are applications for the telematics context, where sensors embedded in the streets or road sides can gather information about traffic conditions at a much finer grained resolution. Such a so called "intelligent roadside" could also interact with the cars to exchange danger warnings about road conditions or traffic jams ahead.

Logistics

In logistics applications, goods equipped with simple sensors allow a simple tracking of these objects during transportation or facilitate inventory tracking in stores or warehouses.

In these applications, there is often no need for a sensor node to actively communicate; passive readout of data is often sufficient, for example, when a suit case is moved around on conveyor belts in an airport and passes certain check points. Such passive readout is much simpler and cheaper than the active communication and information processing it is realized by so-called Radio Frequency Identifier (RF ID) tags.

On the other hand, a simple RFID tag cannot support more advanced applications. It is very difficult to imagine how a passive system can be used to locate an item in a warehouse.

7. Explain in detail about the design principles for wireless sensor networks.

Design principles for WSNs

Appropriate QoS support, energy efficiency, and salability are important design and optimization goals for wireless sensor networks. But these goals themselves do not provide many hints on how to structure a network such that they are achieved. A few basic principles have emerged, which can be useful when designing networking protocols. Nonetheless, the general advice to always consider the needs of a concrete application holds here as well for each of these basic principles, there are examples where following them would result in inferior solutions.

7.1 Distributed organization

Both the salability and the robustness optimization goal, and to some degree also the other goals, make it imperative to organize the network in a distributed fashion. That means that there should be no centralized entity in charge – such an entity could, for example, control medium access or make routing decisions, similar to the tasks performed by a base station in cellular mobile networks.

The disadvantages of such a centralized approach are obvious as it introduces exposed points of failure and is difficult to implement in a radio network, where participants only have a limited communication range. Rather, the WSNs nodes should cooperatively organize the network, using distributed algorithms and protocols. Self-organization is a commonly used term for this principle.

When organizing a network in a distributed fashion, it is necessary to be aware of potential shortcomings of this approach. In many circumstances, a centralized approach can produce solutions that perform better or require less resources (in particular, energy). To combine the advantages, one possibility is to use centralized principles in a localized fashion by dynamically electing, out of the set of equal nodes, specific nodes that assume the responsibilities of a centralized agent, for example, to organize medium access. Such elections result in a hierarchy, which has to be dynamic: The election process should be repeated continuously lest the resources of the elected nodes be overtaxed, the elected node runs out of energy, and the robustness disadvantages of such – even only localized – hierarchies manifest themselves. The particular election rules and triggering conditions for reelection vary considerably, depending on the purpose for which these hierarchies are used.

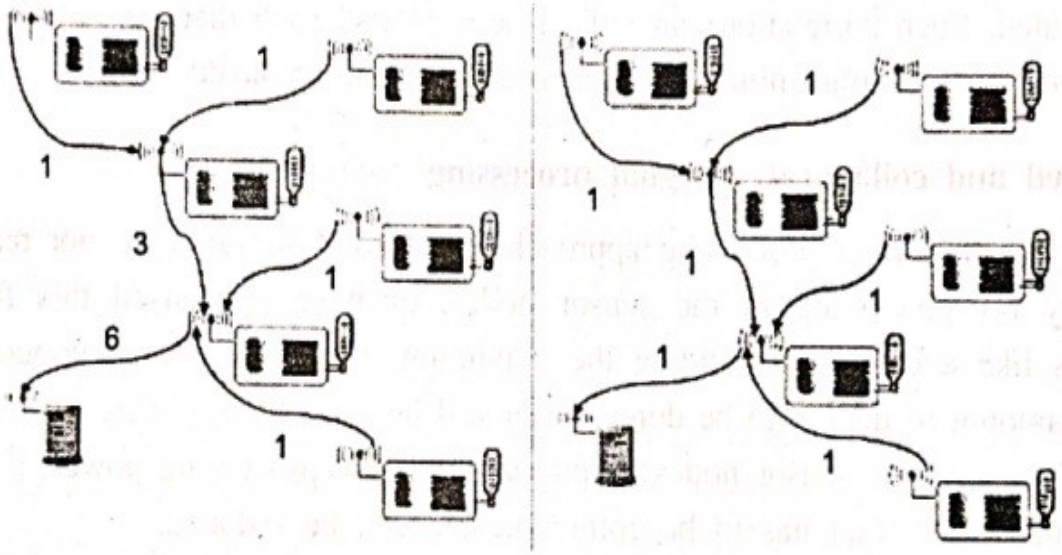
7.2 In-network processing

When organizing a network in a distributed fashion, the nodes in the network are not only passing on packets or executing application programs, they are also actively involved in taking decisions about how to operate the network. This is a specific form of information processing that happens in the network, but is limited to information about the network itself. It is possible to extend this concept by also taking the concrete data that is to be transported by the network into account in this information processing, making in-network processing a first-rank design principle.

Aggregation

Simplest in-network processing technique is aggregation. Suppose a sink is interested in obtaining periodic measurements from all sensors, but it is only relevant to check whether the average value has changed, or whether the difference between minimum and maximum value is too big. The name aggregation stems from the fact that in nodes intermediate between sources and sinks, information is aggregated into a condensed form out of information provided by nodes further away from the sink.

The aggregation function to be applied in the intermediate nodes must satisfy some conditions for the result to be meaningful; most importantly, this function should be composable. A further classification of aggregate functions distinguishes duplicate-sensitive versus insensitive, summary versus exemplary, monotone versus nonmonotone, and algebraic versus holistic. Functions like average, counting, or minimum can profit a lot from aggregation; holistic functions like the median are not amenable to aggregation at all.



Aggregation example

In the left half, a number of sensors transmit readings to a sink, using multihop communication. In total, 13 messages are required (the numbers in the figure indicate the number of messages traveling across a given link). When the highlighted nodes perform aggregation – for example, by computing average values (shown in the right half of the Fig. 1.10) – only 6 messages are necessary.

Challenges in this context include how to determine where to aggregate results from which nodes, how long to wait for such results, and determining the impact of lost packets.

Distributed source coding and distributed compression

Aggregation condenses and sacrifices information about the measured values in order not to have to transmit all bits of data from all sources to the sink. A solution is to be found in order to reduce the number of transmitted bits but still obtain the full information about all sensor readings at the sink.It is related to the coding and

compression problems known from conventional networks, where a lot of effort is invested to encode, for example, a video sequence, to reduce the required bandwidth. Information provided by several sensors are encoded, not just by a single camera; moreover, traditional coding schemes tend to put effort into the encoding, which might be too computationally complex for simple sensor nodes. Here, the information is provided by multiple sensors, hence, some implicit, joint information between two sensors is required. These sensors are embedded in a physical environment – it is quite likely that the readings of adjacent sensors are going to be quite similar; they are correlated. Such correlation can indeed be exploited such that not simply the sum of the data must be transmitted but that overhead can be saved here.

Distributed and collaborative signal processing

The in-networking processing approaches discussed so far have not really used the ability for processing in the sensor nodes, or have only used this for trivial operations like averaging or finding the maximum. When complex computations on a certain amount of data is to be done, it can still be more energy efficient to compute these functions on the sensor nodes despite their limited processing power, if in return the amount of data that has to be communicated can be reduced.

An example for this concept is the distributed computation of a Fast Fourier Transform (FFT). Depending on where the input data is located, there are different algorithms available to compute an FFT in a distributed fashion, with different trade-offs between local computation complexity and the need for communication. In principle, this is similar to algorithm design for parallel computers. However, here not only the latency of communication but also the energy consumption of communication and computation are relevant parameters to decide between various algorithms.

Such distributed computations are mostly applicable to signal processing type algorithms; typical examples are beam forming and target tracking applications.

Mobile code/Agent-based networking

With the possibility of executing programs in the network, other programming paradigms or computational models are feasible. One such model is the idea of mobile code or agent-based networking.The idea is to have a small, compact representation of program code that is small enough to be sent from node to node. This code is

then executed locally, for example, collecting measurements,and then decides where to be sent next. This idea has been used in various environments; a classic example is that of a software agent that is sent out to collect the best possible travel itinerary by hopping from one travel agent's computer to another and eventually returning to the user who has posted this inquiry.

7.3 Adaptive fidelity and accuracy

In the context of a single node, the notion of making the fidelity of computation results contingent upon the amount of energy available for that particular computation. This notion can and should be extended from a single node to an entire network As an example, consider a function approximation application. Clearly, when more sensors participate in the approximation, the function is sampled at more points and the approximation is better. But in return for this, more energy has to be invested. Similar examples hold for event detection and tracking applications and in general for WSNs.

Hence, it is up to an application to somehow define the degree of accuracy of the results (assuming that it can live with imprecise, approximated results) and it is the task of the communication protocols to try to achieve at least this accuracy as energy efficiently as possible. Moreover, the application should be able to adapt its requirements to the current status of the network – how many nodes have already failed, how much energy could be scavenged from the environment, what are the operational conditions (have critical events happened recently), and so forth. Therefore, the application needs feedback from the network about its status to make such decisions.

7.4 Data centricity

In traditional communication networks, the focus of a communication relationship is usually the pair of communicating peers – the sender and the receiver of data. In a wireless sensor network, on the other hand, the interest of an application is not so much in the identity of a particular sensor node, it is much rather in the actual information reported about the physical environment. This is especially the case when a WSN is redundantly deployed such that any given event could be reported by multiple nodes – it is of no concern to the application precisely which of these nodes is providing data. This fact that not the identity of nodes but the data are at the center of attention is called data-centric networking. For an application, this essentially means that an interface is exposed by the network where data, not nodes, is addressed

in requests. The set of nodes that is involved in such a data-centric address is implicitly defined by the property that a node can contribute data to such an address.

Data-centric networking allows very different networking architectures compared to traditional, identity-centric networks. For one, it is the ultimate justification for some in-network processing techniques like data fusion and aggregation. Data-centric addressing also enables simple expressions of communication relationships – it is no longer necessary to distinguish between one-to-one, one-to-many, many-to-one, or many-to-many relationships as the set of participating nodes is only implicitly defined. In addition to this decoupling of identities, data-centric addressing also supports a decoupling in time as a request to provide data does not have to specify when the answer should happen – a property that is useful for event-detection applications, for example.

Apart from providing a more natural way for an application to express its requirements, data-centric networking and addressing is also claimed to improve performance and especially energy efficiency of a WSN. One reason is the hope that data-centric solutions scale better by being implementable using purely local information about direct neighbors. Another reason could be the easier integration of a notion of adaptive accuracy into a data-centric framework as the data as well as its desired accuracy can be explicitly expressed

7.5 Exploit location information

Another useful technique is to exploit location information in the communication protocols whenever such information is present. Since the location of an event is a crucial information for many applications, there have to be mechanisms that determine the location of sensor nodes.

7.6 Exploit activity patterns

Activity patterns in a wireless sensor network tend to be quite different from traditional networks. While it is true that the data rate averaged over a long time can be very small when there is only very rarely an event to report, this can change dramatically when something does happen. Once an event has happened, it can be detected by a larger number of sensors, breaking into a frenzy of activity, causing a well-known event shower effect. Hence, the protocol design should be able to handle

such bursts of traffic by being able to switch between modes of quiescence and of high activity.

7.7 Exploit heterogeneity

Related to the exploitation of activity patterns is the exploitation of heterogeneity in the network.Sensor nodes can be heterogenous by constructions, that is, some nodes have larger batteries, farther-reaching communication devices, or more processing power. They can also be heterogenous by evolution, that is, all nodes started from an equal state, but because some nodes had to perform more tasks during the operation of the network, they have depleted their energy resources or other nodes had better opportunities to scavenge energy from the environment (e.g. nodes in shade are at a disadvantage when solar cells are used).

Whether by construction or by evolution, heterogeneity in the network is both a burden and an opportunity. The opportunity is in an asymmetric assignment of tasks, giving nodes with more resources or more capabilities the more demanding tasks. For example, nodes with more memory or faster processors can be better suited for aggregation, nodes with more energy reserves for hierarchical coordination, or nodes with a farther-reaching radio device should invest their energy mostly for long-distance communication, whereas, shorter-distance communication can be undertaken by the other nodes. The burden is that these asymmetric task assignments cannot usually be static but have to be reevaluated as time passes and the node/network state evolves. Task reassignment in turn is an activity that requires resources and has to be balanced against the potential benefits.

7.8 Component-based protocol stacks and cross-layer optimization

Finally, a consideration about the implementation aspects of communication protocols in WSNs is necessary.All wireless sensor networks will require some – even if only simple – form of physical, MAC and link layer protocols; there will be wireless sensor networks that require routing and transport layer functionalities. Moreover, "helper modules" like time synchronization, topology control, or localization can be useful.

On top of these "basic" components, more abstract functionalities can then be built. As a consequence, the set of components that is active on a sensor node can be complex, and will change from application to application.

Protocol components will also interact with each other in essentially two different ways. One is the simple exchange of data packets as they are passed from one component to another as it is processed by different protocols. The other interaction type is the exchange of cross-layer information.

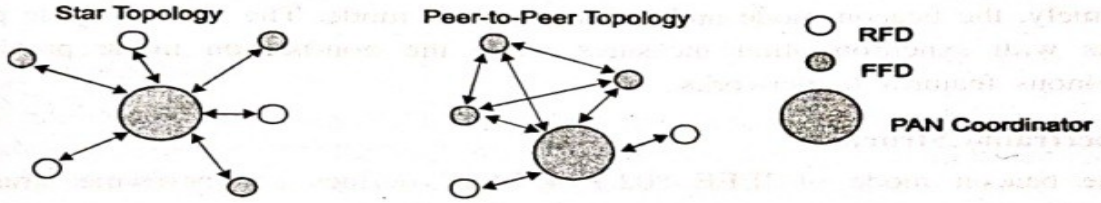
This possibility for cross-layer information exchange holds great promise for protocol optimization, but is also not without danger. For example, argue that imprudent use of cross-layer designs can lead to feedback loops, endangering both functionality and performance of the entire system.

8. Explain in detail about the IEEE 802.15.4 protocol in Wireless Sensor Networks.

The Institute of Electrical and Electronics Engineers (IEEE) released the 802.15.4 MAC standard for wireless personal area networks (WPANs) equipped with a duty cycle mechanism where the size of active and inactive parts can be adjustable during the PAN formation.

8.1 Network Architecture and Types/Roles of Nodes

The IEEE 802.15.4 MAC combines both the schedule-based and contention-based protocols and supports two network topologies, star and peer-to-peer as shown in Figure below



Topology configurations supported by IEEE 802 15.4 standard

Source: Protocol and Architecture for Wireless Sensor Networks by Holger Karl, Andreas willig

Applications of IEEE 802.15.4

- Wireless sensor networks
- Home Automation
- Home Networking
- Connecting Devices to a PC
- Home security, etc.

There are two special types of peer-to-peer topology. The first type is known as a cluster-tree network which has been used extensively in ZigBee. The other type is known as a mesh network which has been used extensively in IEEE 802.15 WPAN Task Group 5 (TG5).

The standard defines two types of nodes namely the Full Function Device (FFD) and Reduced Function Device (RFD). The FFD node can operate with three different roles as a PAN coordinator, a coordinator and a device while RFD can operate only as a device.

The devices must be associated with a coordinator in all network conditions. The multiple coordinators can either operate in a peer-to-peer topology or star topology with a coordinator becoming the PAN coordinator.

The star topology is more suitable for delay critical applications and small network coverage while the peer-to-peer topology is more applicable for large networks with multi-hop requirements at the cost of higher network latency.

Furthermore, the standard defines two modes on how data exchanges should be done,namely, the beacon mode and the non-beacon mode. The beacon mode provides networks with synchronisation measures while the non-beacon mode provides the asynchronous features to networks.

8.2 Superframe Structure

The beacon mode of IEEE 802.15.4 MAC defines a superframe structure to organise the channel access and data exchanges. The superframe structure is shown in Figure 1 with two main periods; the active period and inactive period. The active period is divided into 16 time slots. Typically the beacon frame is transmitted in the first time slot and it is followed by two other parts, Contention Access Period (CAP) and Contention-Free Period (CFP) which utilise the remaining time slots. The CFP part is also known as Guaranteed Time Slots (GTS) and can utilise up to 7 time slots.

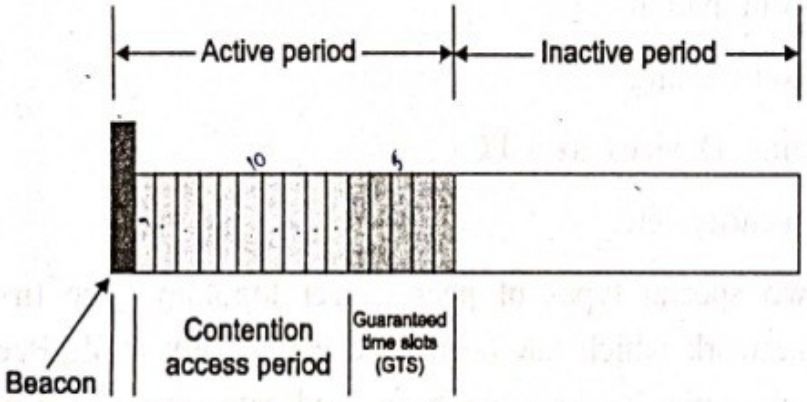


Fig. 1 Superframe structure of IEEE 802.15.4

Source: *Protocol and Architecture for Wireless Sensor Networks by Holger Karl, Andreas willig*

The length of the active and inactive periods as well as the length of a single time slot are configurable and traffic dependant.Data transmissions can occur either in CAP or GTS. In CAP, data communication is achieved by using slotted CSMA-CA while in GTS nodes are allocated fixed time slots for data communication.

The strategy to achieve energy efficient operations in IEEE 802.15.4 MAC is by putting the nodes to sleep during the inactive period and when there is neither data to be transmitted nor any data to be fetched from the coordinator.However, the burden of energy cost is put on the coordinator where the coordinator has to be active during the entire active period.

8.3 GTS Management

The coordinator allocates GTS to devices only when the latter send appropriate request packets during the CAP. One flag in the request indicates whether the requested time slot is a transmit slot or a receive slot.In a transmit slot, the device transmits packets to the coordinator and in a receive slot the data flows in the reverse direction. Another field in the request specifies the desired number of contiguous time slots in the GTS phase.

The coordinator answers the request packet in two steps: An immediate acknowledgment packet confirms that the coordinator has received the request packet properly but contains no information about success or failure of the request.

After receiving the acknowledgment packet, the device is required to track the coordinator's beacons for some specified time (called a GTS DescPersistence Time). When the coordinator has sufficient resources to allocate a GTS to the node, it inserts an appropriate GTS descriptor into one of the next beacon frames. This GTS descriptor specifies the short address of the requesting node and the number and position of the time slots within the GTS phase of the superframe.

A device can use its allocated slots each time they are announced by the coordinator in the GTS descriptor. If the coordinator has insufficient resources, it generates a GTS descriptor for (invalid) time slot zero, indicating the available resources in the descriptors length field. Upon receiving such a descriptor, the device may consider renegotiation.

If the device receives no GTS descriptor within a GTSDesc Persistence Time time after sending the request, it concludes that the allocation request has failed. A GTS is allocated to a device on a regular basis until it is explicitly deallocated. The deallocation can be requested by the device by means of a special control frame.

After sending this frame, the device shall not use the allocated slots any further. The coordinator can also trigger deallocation based on certain criteria. Specifically, the coordinator monitors the usage of the time slot: If the slot is not used at least once within a certain number of superframes, the slot is deallocated. The coordinator signals deallocation to the device by generating a GTS descriptor with start slot zero.

8.4 Data Transfer

Assume that a device wants to transmit a data packet to the coordinator. If the device has an allocated transmit GTS, it wakes up just before the time slot starts and sends it spacket immediately without running any carrier-sense or other collision-avoiding operations.

However, the device can do so only when the full transaction consisting of the data packet and an immediate acknowledgment sent by the coordinator as well as appropriate InterFrame Spaces (IFSs) fit into the allocated time slots.

If this is not the case or when the device does not have any allocated slots, it sends its data packet during the CAP using a slotted CSMA protocol. The coordinator sends an immediate acknowledgment for the data packet.

Now, assume the coordinator wants to send a data packet to the device. If the device has allocated a receive GTS and when the packet/acknowledgment/IFS cycle fits into these, the coordinator simply transmits the packet in the allocated time slot without further coordination. The device has to acknowledge the data packet. The handshake between device and coordinator is sketched in Figure 1.17. The coordinator announces a buffered packet to a device by including the devices address into the pending address field of the beacon frame.

When the device finds its address in the pending address field, it sends a special data request packet during the CAP.The coordinator answers this packet with an acknowledgment packet and continues with sending the data packet.

The device knows upon receiving the acknowledgment packet that it shall leave its transceiver on and prepares for the incoming data packet, which in turn is acknowledged. Otherwise, the device tries again to send the data request packet during one of the following superframes and optionally switches off its transceiver until the next beacon.

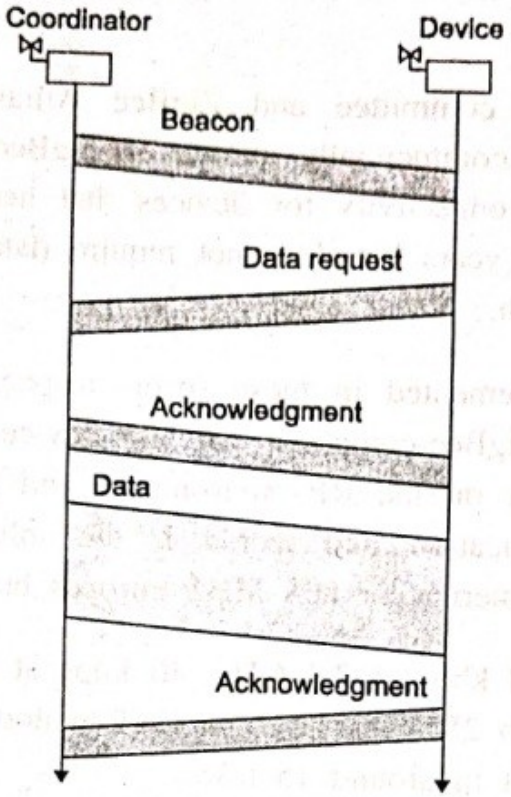


Fig. 1.17 Handshake between coordinator and device when the device retrieves a packet

Source: Protocol and Architecture for Wireless Sensor Networks by Holger Karl, Andreas willig

8.5 Slotted CSMA-CA Protocol

When nodes have to send data or management/control packets during the CAP, they use a slotted CSMA protocol. The protocol contains no provisions against hidden-terminal situations.

For example, there is no RTS/CTS handshake. To reduce the probability of collisions,the protocol uses random delays; it is thus a CSMA-CA protocol (CSMA with Collision Avoidance).

The time slots making up the CAP are subdivided into smaller time slots, called back off periods. One backoff period has a length corresponding to 20 channel symboltimes and the slots considered by the slotted CSMA-CA protocol are just these backoff periods.

9. Explain in detail about the gateway concepts in wireless senor networks. (OR)
How the wireless sensor network establish its communication with outside world or with other wireless sensor network.

9.1 The need for gateways

For practical deployment, a sensor network only concerned with itself is insufficient. The network rather has to be able to interact with other information devices, for example, a user equipped with a PDA moving in the coverage area of the network or with a remote user, trying to interact with the sensor network via the Internet (the standard example is to read the temperature sensors in one's home while traveling and accessing the Internet via a wireless connection). Figure 1.12 shows this networking scenario.

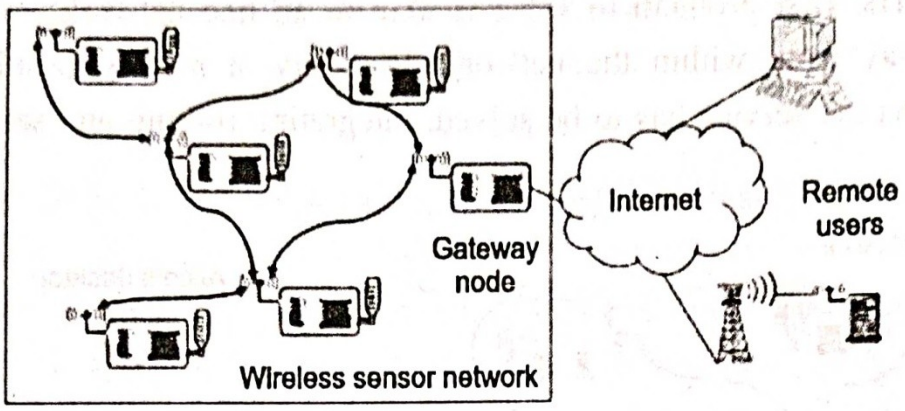


Fig. 1.12 A wireless sensor network with gateway node, enabling access to remote clients via the Internet

To this end, the WSN first of all has to be able to exchange data with such a mobile device or with some sort of gateway, which provides the physical connection to the Internet. This is relatively straightforward on the physical, MAC, and link layer – either the mobile device/the gateway is equipped with a radio transceiver as used in the WSN, or some (probably not all) nodes in the WSN support standard wireless communication technologies such as IEEE 802.11. Either option can be advantageous, depending on the application and the typical use case. Possible trade-offs include the percentage of multitechnology sensor nodes that would be required to serve mobile users in comparison with the overhead and inconvenience to fit WSN transceivers to mobile devices like PDAs.

The design of gateways becomes much more challenging when considering their logical design. One option to ponder is to regard a gateway as a simple router between Internet and sensor network. This would entail the use of Internet protocols within the sensor network. While this option has been considered as well and should not be disregarded lightly, it is the prevalent consensus that WSNs will require specific, heavily optimized protocols. Thus, a simple router will not suffice as a gateway.

The remaining possibility is therefore to design the gateway as an actual application-level gateway: on the basis of the application-level information, the gateway will have to decide its action. A rough distinction of the open problems can be made according to from where the communication is initiated.

9.2 WSN to Internet communication

Assume that the initiator of a WSN–Internet communication resides in the WSN (Fig. 1.13) – for example, a sensor node wants to deliver an alarm message to some

Internet host. The first problem to solve is akin to ad hoc networks, namely, how to find the gateway from within the network. Basically, a routing problem to a node that offers a specific service has to be solved, integrating routing and service discovery.

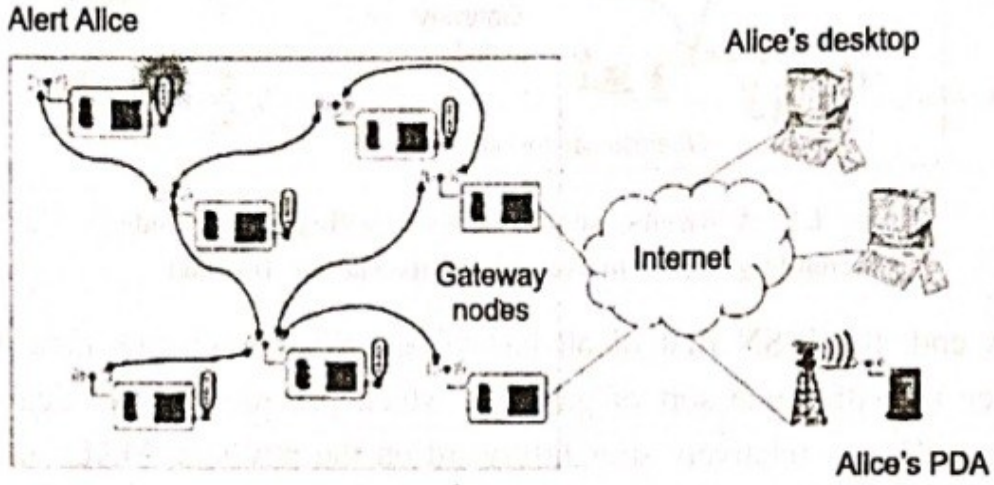


Fig. 1.13 An event notification to "Alice" needs decisions about, among others, gateway choice, mapping "Alice" to a concrete IP address, and translating an intra-WSN event notification message to an Internet application message

If several such gateways are available, choosing between them will be the next task. In particular, if not all Internet hosts are reachable via each gateway or at least if some gateway should be preferred fora given destination host? How to handle several gateways, each capable of IP networking, and the communication among them? One option is to build an IP overlay network on top of the sensor network.

How does a sensor node know to which Internet host to address such a message? Or even worse,how to map a semantic notion ("Alert Alice") to a concrete IP address? Even if the sensor node does not need to be able to process the IP protocol, it has to include sufficient information (IP address and port number, for example) in its own packets; the gateway then has to extract this information and translate it into IP packets. An ensuing question is which source address to use here – the gateway in a sense has to perform tasks similar to that of a Network Address Translation (NAT) device.

9.3 Internet to WSN communication

The case of an Internet-based entity trying to access services of a WSN is even more challenging (Fig. 1.13). This is fairly simple if this requesting terminal is able to directly communicate with the WSN, for example, a mobile requester equipped

with a WSN transceiver, and also has all the necessary protocol components at its disposal. In this case, the requesting terminal can be a direct part of the WSN and no particular treatment is necessary.

The more general case is, however, a terminal "far away" requesting the service, not immediately able to communicate with any sensor node and thus requiring the assistance of a gateway node.First of all, again the question of service discovery presents itself – how to find out that the reactually is a sensor network in the desired location, and how to find out about the existence of a gateway node?

Once the requesting terminal has obtained this information, how to access the actual services? Clearly, addressing an individual sensor (like addressing a communication peer in a traditional Internet application) both goes against the grain of the sensor network philosophy where an individual sensor node is irrelevant compared to the data that it provides and is impossible if a sensornode does not even have an IP address.

The requesting terminal can instead send a properly formatted request to this gateway, which acts as an application-level gateway or a proxy for the individual/set of sensor nodes that can answer this request; the gateway translates this request into the proper intrasensor network protocol interactions. This assumes that there is an application-level protocol that a remote requester and gateway can use and that is more suitable for communication over the Internet than the actual sensor network protocols and that is more convenient for the remote terminal to use. The gateway can then mask, for example, a data-centric data exchange within the network behind an identity-centric exchange used in the Internet.

It is by no means clear that such an application-level protocol exists that represents an actual simplification over just extending the actual sensor network protocols to the remote terminal, but there are some indications in this direction. For example, it is not necessary for the remote terminal to be concerned with maintaining multihop routes in the network nor should it be considered as "just another hop" as the characteristics of the Internet connection are quite different from a wireless hop.

In addition, there are some clear parallels for such an application-level protocol with so-called Web Service Protocols, which can explicitly describe services and the way they can be accessed. The Web Service Description Language (WSDL), in

particular, can be a promising starting point for extension with the required attributes for WSN service access – for example, required accuracy,energy trade-offs, or data-centric service descriptions.

9.4 WSN tunnelling

In addition to these scenarios describing actual interactions between a WSN and Internet terminals,the gateways can also act as simple extensions of one WSN to another WSN. The idea is to build a larger, "virtual" WSN out of separate parts, transparently "tunneling" all protocol messages between these two networks and simply using the Internet as a transport network Fig. 1.14. This can be attractive, but care has to be taken not to confuse the virtual link between two gateway nodes with a real link; otherwise, protocols that rely on physical properties of a communication link can get quite confused (e.g. time synchronization or localization protocols).

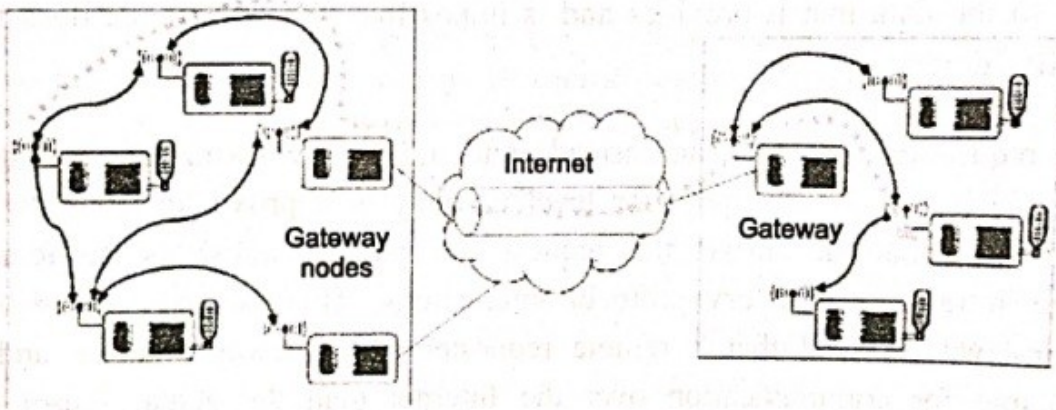


Fig. 1.14 Connecting two WSNs with a tunnel over the Internet

Such tunnels need not necessarily be in the form of fixed network connections; even mobile nodes carried by people can be considered as means for intermediate interconnection of WSNs.

10. Explain in detail about the Bluetooth and its specifications. And also explain the protocol stack of Bluetooth.

WLAN technology enables device connectivity to infrastructure-based services through a wireless carrier provider. However, the need for personal devices to communicate wirelessly with one another, without an established infrastructure, has led to the emergence of personal area networks (PANs). The first attempt to define a standard for PANs dates back to Ericsson's Bluetooth project in 1994 to enable communication between mobile phones using low-power and low-cost radio interfaces. In May 1998, several companies such as Intel, IBM, Nokia, and Toshiba joined Ericsson to form the Bluetooth Special Interest Group (SIG) whose aim was to develop a de facto standard for PANs.

Recently, IEEE has approved a Bluetooth-based standard (IEEE 802.15.1) for wireless personal area networks (WPANs). The standard covers only the MAC and the physical layers while the Bluetooth specification details the whole protocol stack. Bluetooth employs radio frequency (RF) technology for communication. It makes use of frequency modulation to generate radio waves in the ISM band.

Low power consumption of Bluetooth technology and an offered range of up to ten meters has paved the way for several usage models. One can have an interactive conference by establishing an ad hoc network of laptops. Cordless computer, instant postcard |sending digital photographs instantly (a camera is cordlessly connected to

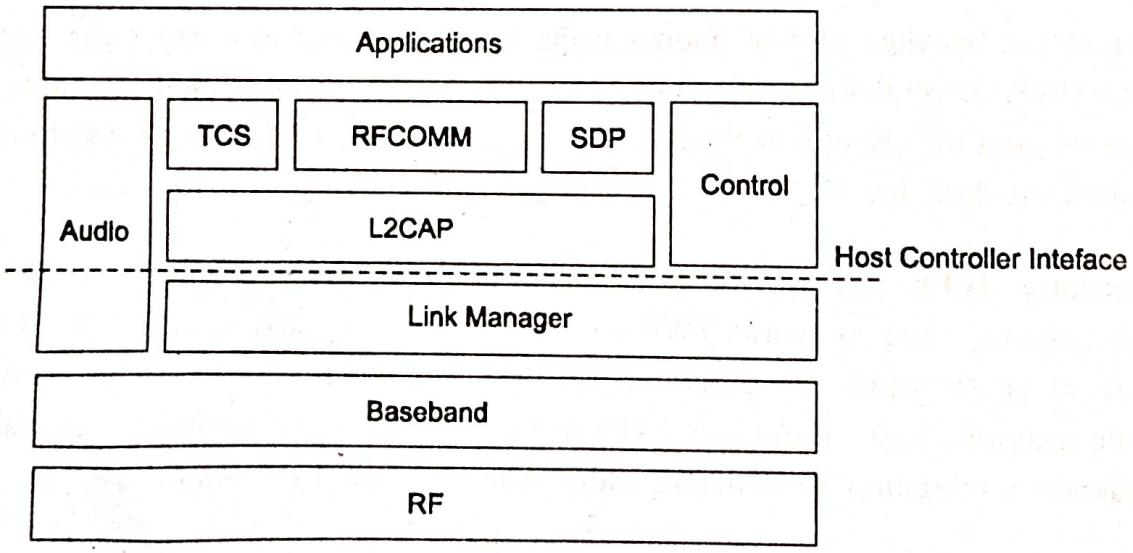


Fig. 1.19 Bluetooth protocol stack

1.7.2.2 Transport Protocol Group

This group is composed of the protocols designed to allow Bluetooth devices to locate each other and to create, configure, and manage the wireless links.Design of various protocols and techniques used in Bluetooth communications has been done with the target of low power consumption and ease of operation.This shall become evident in the design choice of FHSS and the master–slave architecture. The following sections study the various protocols in this group, their purpose, their modes of operation, and other specifications.

Radio (Physical) Layer

The radio part of the specification deals with the characteristics of the transceivers and design specifications such as frequency accuracy, channel interference, and modulation characteristics. The Bluetooth system operates in the globally available ISM frequency band and the frequency modulation is GFSK. It supports 64 Kbps voice channels and asynchronous data channels with a peak rate of 1 Mbps. The data channels are either asymmetric (in one direction) or symmetric (in both directions). The Bluetooth transceiver is a FHSS system operating over a set of m channels each of width 1 MHz. Inmost of the countries, the value of m is 79. Frequency hopping is used and hops are made at a rapid rate across the possible 79 hops in the band, starting at 2.4 GHz and stopping at 2.480 GHz. The choice of frequency hopping has been made to provide protection against interference.

The Bluetooth air interface is based on a nominal antenna power of 0 dBm (1 mW) with extensions for operating at up to 20 dBm (100 mW) worldwide. The nominal link range is from 10 centimeters to 10 meters, but can be extended to more than 100 meters by increasing the transmit power (using the 20 dBm option). It should be noted here that a WLAN cannot use an antenna power of less than 0 dBm (1 mW) and hence an 802.11 solution might not be apt for power-constrained devices.

Baseband Layer

The key functions of this layer are frequency hop selection, connection creation,and medium access control. Bluetooth communication takes place by adhoc creation of a network called a piconet. The address and the clock associated with each Bluetooth device are the two fundamental elements governing the formation of a piconet. Every device is assigned a single 48-bit address which is similar to the

addresses of IEEE 802.xx LAN devices. The address field is partitioned into three parts and the lower address part (LAP) is used in several base band operations such as piconet identification, error checking, and security checks. The remaining two parts are proprietary addresses of the manufacturing organizations. LAP is assigned internally by each organization. Every device also has a 28-bit clock (called the native clock) that ticks 3,200 times per second or once every 312.5 μ s. It should be noted that this is twice the normal hopping rate of 1,600 hops per second.

Piconet

The initiator for the formation of the network assumes the role of the master (of the piconet). All the other members are termed as slaves of the piconet. Apiconet can have up to seven active slaves at any instant. For the purpose of identification, each active slave of the piconet is assigned a locally unique active member address AM_ADDR. Other devices could also be part of the piconet by being in the parked mode (explained later). A Bluetooth device not associated with any piconet is said to be in standby mode.

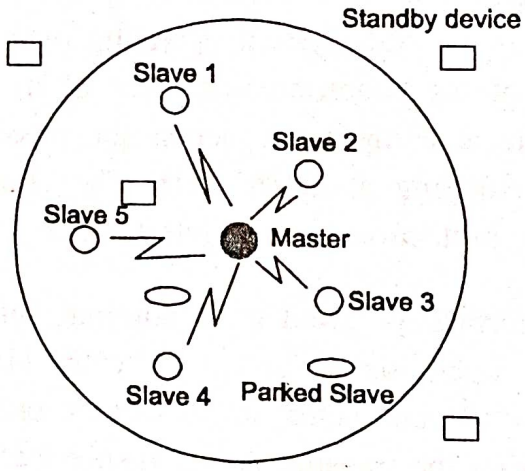


Fig. 1.20 shows a piconet with several devices

Operational States

Figure 1.21 shows the state diagram of Bluetooth communications. Initially, all the devices would be in the standby mode. Then some device (called the master)could begin the inquiry and get to know the nearby devices and, if needed, join them into its piconet. After the inquiry, the device could formally be joined by paging, which is a packet-exchange process between the master and a prospective slave to inform the slave of the master's clock. If the device was already inquired, the master could

get into the page state bypassing the inquiry state. Once the device finishes getting paged, it enters the connected state. This state has three power-conserving sub-states – hold, sniff, and park (described later in this section). A device in the connected state can participate in the data transmission.

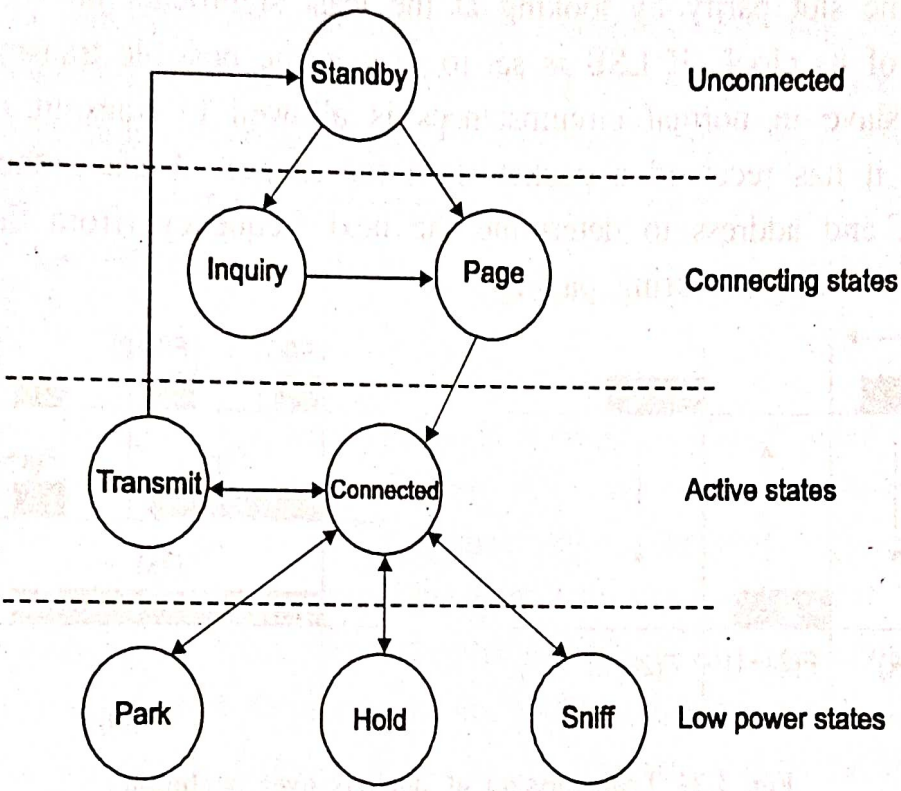


Fig. 1.21 Operational States

Frequency Hopping Sequences

It is evident (in any wireless communication) that the sender and the receiver should use the same frequency for communication to take place. A frequency selection module (FSM) is present in each device to select the next frequency to be used under various circumstances. In the connected state, the clock and the address of the device (master) completely determine the hopping sequence.Different combination of inputs (clock, address) are used depending on the operational state. During the inquiry operation, the address input to FSM is a common inquiry address. This common address is needed because at the time of inquiry no device has information about the hopping sequence being followed.The address of the paged device is fed as input to the FSM for the paging state.

Communication Channel

The channel is divided into time slots, each 625 μ s in length. The time slots a renumbered according to the Bluetooth clock of the piconet master. A time division

duplex (TDD) scheme is used where master and slave alternately transmit. The master starts its transmission in even-numbered time slots only,and the slave starts its transmission in odd-numbered time slots only. This is clearly illustrated in Figure 1.21 (a). The packet start shall be aligned with the slot start. A Bluetooth device would determine slot parity by looking at the least significant bit (LSB) in the bit representation of its clock. If LSB is set to 1, it is the possible transmission slot for the slave. A slave in normal circumstances is allowed to transmit only if in the preceding slot it has received a packet from the master. A slave should know the master's clock and address to determine the next frequency (from the FSM). This information is exchanged during paging.

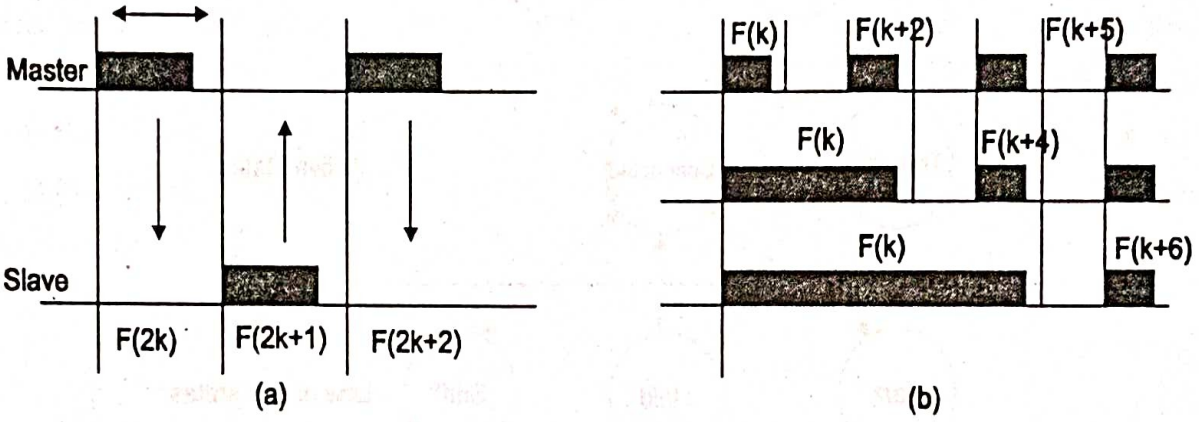


Fig. 1.21 Transmission of packets over a channel

Packet-Based Communication

Bluetooth uses packet-based communication where the data to be transmitted is fragmented into packets. Only a single packet can be transmitted in each slot. Atypical packet used in these communications has three components: access code,header, and payload. The main component of the access code is the address of the piconet master. All packets exchanged on the channel are identified by the master's identity. The packet will be accepted by the recipient only if the access code matches the access code corresponding to the piconet master. This also helps in resolving conflicts in the case where two piconets are operating currently on the same frequency. A slave receiving two packets in the same slot can identify its packet by examining the access code.

The packet header contains many fields such as a three-bit active slave address,a one-bit ACK/NACK for ARQ scheme [Automatic Repeat reQuest — any time an error is detected, a negative acknowledgment (NACK) is returned and the specified frames are retransmitted], a four-bit packet type to distinguish pay load types, and an eight-bit header error check code to detect errors in the header.

Depending on the payload size, one, three, or five slots may be used for the packet transmission. The hop frequency which is used for the first slot is used for the remainder of the packet. While transmitting packets in multiple slots, it is important that the frequencies used in the following time slots are those that are assigned to those slots, and that they do not follow the frequency sequence that should have normally applied. This is illustrated in Figure 1.21 (b). When a device uses five slots for packet transmission, the next packet transmission is allowed in $F(k+6)$ and not in $F(k+2)$. Also note that the receiving time slot be comes $F(k+5)$ as opposed to $F(k+1)$. On this slotted channel, both synchronous and asynchronous links are supported.

Between a master and a slave there is a single asynchronous connection less link (ACL) supported. This is the default link that would exist once a link is established between a master and a slave. Whenever a master would like to communicate, it would, and then the slave would respond. Optionally, a piconet may also support synchronous connection oriented (SCO) links. SCO link is symmetric between master and slave with reserved bandwidth and regular periodic exchange of data in the form of reserved slots. These links are essential and useful for high-priority and time-bound information such as audio and video.

Inquiry State

As shown in Fig. 1.19, a device which is initially in the standby state enters the inquiry state. As its name suggests, the sole purpose of this state is to collect in formation about other Bluetooth devices in its vicinity. This information includes the Bluetooth address and the clock value, as these form the crux of the communication between the devices. This state is classified into three sub-states: inquiry, inquiry scan, and inquiry response.

A potential master sends an inquiry packet in the inquiry state on the inquiry hop sequence of frequencies. This sequence is determined by feeding a common address as one of the inputs to the FSM. A device (slave) that wants to be discovered will periodically enter the inquiry scan state and listen for these inquiry packets. When an inquiry message is received in the inquiry scan state, a response packet called the frequency hopping sequence (FHS) containing the responding device address must be sent. Devices respond after a random jitter to reduce the chances of collisions.

Page State

A device enters this state to invite other devices to join its piconet. A device could invite only the devices known to itself. So normally the inquiry operation would precede this state. This state also is classified into three sub-states: page,page scan, and page response.In the page mode, the master estimates the slave's clock based on the information received during the inquiry state, to determine where in the hop sequence the slave might be listening in the page scan mode. In order to account for inaccuracies in estimation, the master also transmits the page message through frequencies immediately preceding and succeeding the estimated one.

On receiving the page message, the slave enters the slave page response sub-state. It sends back a page response consisting of its ID packet which contains its device access code (DAC). Finally, the master (after receiving the response from a slave) enters the page response state and informs the slave about its clock and address so that the slave can go ahead and participate in the piconet. The slave now calculates an offset to synchronize with the master clock, and uses that to determine the hopping sequence for communication in the piconet.

Scatternets and Issues

Piconets may overlap both spatially and temporally, that is, many piconets could operate in the same area at the same time. Each piconet is characterized by a unique master and hence the piconets hop independently, each with its own channel hopping sequence as determined by the respective master. In addition,the packets carried on the channels are preceded by different channel access codes as determined by the addresses of the master devices. As more piconets are added, the probability of collisions increases, and a degradation in performance results, as is common in FHSS systems.

In this scenario, a device can participate in two or more overlaying piconets by the process of time sharing. To participate on the proper channel, it should use the associated master device address and proper clock offset. A Bluetooth unit can act as a slave in several piconets, but as a master in only a single piconet. A group of piconets in which connections exist between different piconets is called a scatternet (Fig. 1.22).

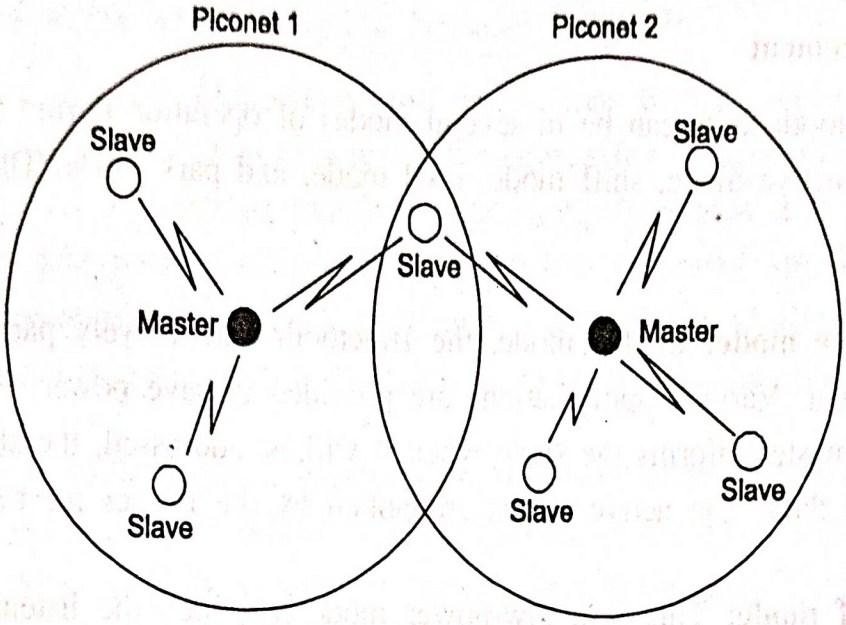


Fig. 1.22 A typical scatternet

When a device changes its role and takes part in different piconets, it is bound to lead to a situation in which some slots remain unused (for synchronization).This implies that complete utilization of the available bandwidth is not achieved. An interesting proposition at this juncture would be to unite the timings of the whole of the scatternet. But this may lead to an increase in the probability of packets colliding.

Another important issue is the timing that a device would be missing by participating in more than one piconet. A master that is missing from a piconet(by momentarily becoming a slave in another piconet) may miss polling slaves and must ensure that it does not miss beacons from its slaves. Similarly, a slave(by becoming a master or slave in another piconet) that is missing from apiconet could appear to its master to have gone out of range or to be connected through a poor-quality link.

Link Manager Protocol

Link manager protocol (LMP) is responsible for setting and maintaining the properties of the Bluetooth link. Currently, the major functionality of this layer is power management and security management. It also provides minimal QoS support by allowing control over parameters such as delay and delay jitter.Normally, a paging device is the default master of the piconet, but, depending on the usage scenario, the roles of the master and a slave could be switched and this is coordinated by exchange of LMP packets.

Power Management

The Bluetooth units can be in several modes of operation during the connection state, namely, active mode, sniff mode, hold mode, and park mode. These modes are now described.

- **Active mode:** In this mode, the Bluetooth unit actively participates in the piconet. Various optimizations are provided to save power. For instance, if the master informs the slave when it will be addressed, the slave may sleep until then. The active slaves are polled by the master for transmissions.

- **Sniff mode:** This is a low-power mode in which the listening activity of the slave is reduced. The LMP in the master issues a command to the slave to enter the sniff mode, giving it a sniff interval, and the slave listens for transmissions only at these fixed intervals.

- **Hold mode:** In this mode, the slave temporarily does not support ACL packets on the channel (possible SCO links will still be supported). In this mode,capacity is made available for performing other functions such as scanning,paging, inquiring, or attending another piconet.

- **Park mode:** This is a very low-power mode. The slave gives up its active member address and is given an eight-bit parked member address. The slave,however, stays synchronized to the channel. Any messages to be sent to a parked member are sent over the broadcast channel characterized by an active member address of all zeros. Apart from saving power, the park mode helps the master to have more than seven slaves (limited by the three-bit active member address space) in the piconet.

Bluetooth Security

In Bluetooth communications, devices may be authenticated and links may been crypted. The authentication of devices is carried out by means of a challenge-response mechanism which is based on a commonly shared secret link key generated through a user-provided personal identification number (PIN). The authentication starts with the transmission of an LMP challenge packet and end switch the verification of result returned by the claimant. Optionally, the link between them could also be encrypted.

Logical Link Control and Adaptation Protocol (L2CAP)

This is the protocol with which most applications would interact unless a host controller is used. L2CAP supports protocol multiplexing to give the abstraction to each of the several applications running in the higher layers as if it alone is being run. Since the data packets defined by the baseband protocol are limited in size, L2CAP also segments large packets from higher layers such as RFCOMM or SDP into multiple smaller packets prior to their transmission over the channel.

Similarly, multiple received baseband packets may be reassembled into a single larger L2CAP packet. This protocol provides QoS on certain parameters such a speak bandwidth, latency, and delay variation when the link is established between two Bluetooth units.

Host Controller Interface

This is the optional interface layer, provided between the higher (above LMP)and lower layers of the Bluetooth protocol stack, for accessing the Bluetooth hardware capabilities. Whenever the higher layers are implemented on the mother board of a host device, this layer is needed. Such an approach could prove beneficial as the spare capacity of the host device (say, a personal computer) could be utilized. The specification defines details such as the different packet types as seen by this layer. Command packets that are used by the host to control the device, event packets that are used by the device to inform the host of the changes, and data packets come under this category.