1.Introduction

A **wireless sensor network (WSN)** consists of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

A sensor node might vary in size from that of a shoebox down to the size of a grain of dust. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

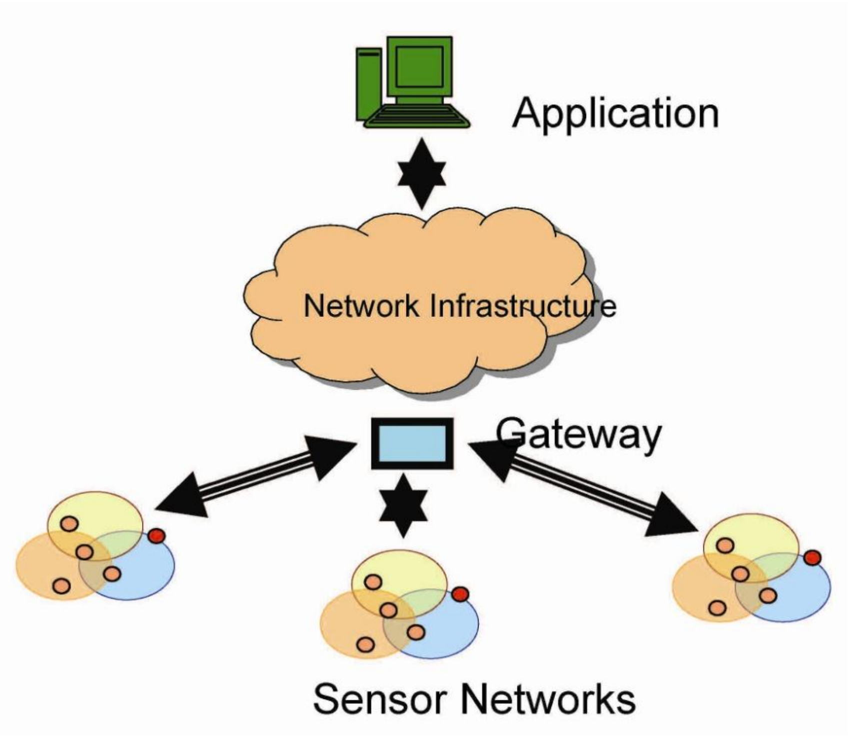


Figure:1.1 Overview of wireless sensor network

1.1 WIRELESS SENSOR NETWORK

Wireless sensor network is an infrastructure comprised of sensing (measuring), computing, and communication elements that gives a user the ability to instrument, observe, and react to events and phenomena in a specified environment.

There are four basic components in WSN:

- An assembly of distributed or localized sensors (sensing and computation nodes)
- An interconnection network,
- A central point of information gathering, and
- A set of computing resources at the central point (or beyond) to handle data correlation, event trending, status querying, and data mining.

1.2. Applications of WSN:

Area monitoring

Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors to detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines.

Environmental/Earth monitoring

The term Environmental Sensor Networks has evolved to cover many applications of WSNs to earth science research. This includes sensing volcanoes, oceans, glaciers, forests, etc. Some of the major areas are listed below.

Air quality monitoring- The degree of pollution in the air has to be measured frequently in order to safeguard people and the environment from any kind of damages due to air pollution. In dangerous surroundings, real time monitoring of harmful gases is a concerning process because the weather can change with severe consequences in an immediate manner. Fortunately, wireless sensor networks have been launched to produce specific solutions for people.

- **Interior monitoring**

Observing the gas levels at vulnerable areas needs the usage of high-end, sophisticated equipment, capable to satisfy industrial regulations. Wireless internal monitoring solutions facilitate keep tabs on large areas as well as ensure the precise gas concentration degree.

- **Exterior monitoring**

  External air quality monitoring needs the use of precise wireless sensors, rain & wind resistant solutions as well as energy reaping methods to assure extensive liberty to machine that will likely have tough access.

Air pollution monitoring

Wireless sensor networks have been deployed in several cities to monitor the concentration of dangerous gases for citizens. These can take advantage of the ad-hoc wireless links rather than wired installations, which also make them more mobile for testing readings in different areas. There are various architectures that can be used for such applications as well as different kinds of data analysis and data mining that can be conducted.

Forest fire detection

A network of Sensor Nodes can be installed in a forest to detect when a fire has started. The nodes can be equipped with sensors to measure temperature, humidity and gases which are produced by fire in the trees or vegetation. The early detection is crucial for a successful action of the firefighters; thanks to Wireless Sensor Networks, the fire brigade will be able to know when a fire is started and how it is spreading.

Landslide detection

A landslide detection system makes use of a wireless sensor network to detect the slight movements of soil and changes in various parameters that may occur before or during a landslide. Through the data gathered it may be possible to know the occurrence of landslides long before it actually happens.

Water quality monitoring

Water quality monitoring involves analyzing water properties in dams, rivers, lakes & oceans, as well as underground water reserves. The use of many wireless distributed sensors enables the creation of a more accurate map of the water status, and allows the permanent deployment of monitoring stations in locations of difficult access, without the need of manual data retrieval.

Natural disaster prevention

Wireless sensor networks can effectively act to prevent the consequences of natural disasters, like floods. Wireless nodes have successfully been deployed in rivers where changes of the water levels have to be monitored in real time.

Industrial monitoring

Machine health monitoring

Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionality. In wired systems, the installation of enough sensors is often limited by the cost of wiring. Previously inaccessible locations, rotating machinery, hazardous or restricted areas, and mobile assets can now be reached with wireless sensors.

Data logging

Wireless sensor networks are also used for the collection of data for monitoring of environmental information, this can be as simple as the monitoring of the temperature in a fridge to the level of water in overflow tanks in nuclear power plants. The statistical information can then be used to show how systems have been working. The advantage of WSNs over conventional loggers is the "live" data feed that is possible.

Water/Waste water monitoring

Monitoring the quality and level of water includes many activities such as checking the quality of underground or surface water and ensuring a country’s water infrastructure for the benefit of both human and animal. The area of water quality monitoring utilizes wireless sensor networks and many manufacturers have launched fresh and advanced applications for the purpose.

- **Observation of water quality**

The whole process includes examining water properties in rivers, dams, oceans, lakes and also in underground water resources. Wireless distributed sensors let users to make a precise map of the water condition as well as making permanent distribution of observing stations in areas of difficult access with no manual data recovery.

- **Water distribution network management**

Manufacturers of water distribution network sensors concentrate on observing the water management structures such as valve and pipes and also making remote access to water meter readings.

- **Preventing natural disaster**

The consequences of natural perils like floods can be effectively prevented with wireless sensor networks. Wireless nodes are distributed in rivers so that changes of the water level can be effectively monitored.

Agriculture

Using wireless sensor networks within the agricultural industry is increasingly common; using a wireless network frees the farmer from the maintenance of wiring in a difficult environment. Gravity feed water systems can be monitored using pressure transmitters to monitor water tank levels, pumps can be controlled using wireless I/O devices and water use can be measured and wirelessly transmitted back to a central control center for billing. Irrigation automation enables more efficient water use and reduces waste.

- **Accurate agriculture**

Wireless sensor networks let users to make precise monitoring of the crop at the time of its growth. Hence, farmers can immediately know the state of the item at all its stages which will ease the decision process regarding the time of harvest.

- **Irrigation management**

When real time data is delivered, farmers are able to achieve intelligent irrigation. Data regarding the fields such as temperature level and soil moisture are delivered to farmers through wireless sensor networks. When each plant is joined with a personal irrigation system, farmers can pour the precise amount of water each plant needs and hence, reduce the cost and improve the quality of the end product. The networks can be employed to manage various actuators in the systems using no wired infrastructure.

- **Greenhouses**

Wireless sensor networks are also used to control the temperature and humidity levels inside commercial greenhouses. When the temperature and humidity drops below specific levels, the greenhouse manager must be notified via e-mail or cell phone text message, or host systems can trigger misting systems, open vents, turn on fans, or control a wide variety of system responses.

Passive localization and tracking

The application of WSN to the passive localization and tracking of non-cooperative targets (i.e., people not wearing any tag) has been proposed by exploiting the pervasive and low-cost nature of such technology and the properties of the wireless links which are established in a meshed WSN infrastructure.

Smart home monitoring

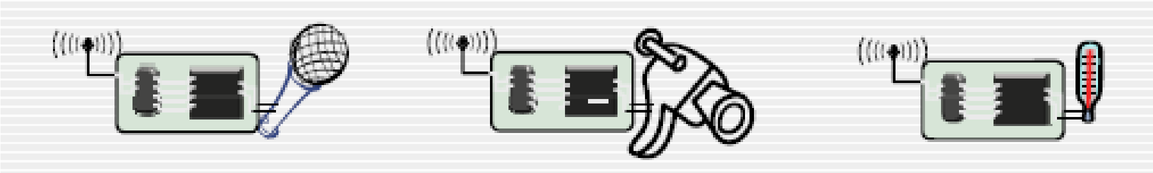
Monitoring the activities performed in a smart home is achieved using wireless sensors embedded within everyday objects forming a WSN. A state change to objects based on human manipulation is captured by the wireless sensors network enabling activity-support services.

While most of these applications are, in some form or another, possible even with today’s technologies and without wireless sensor networks, all current solutions are “sensor starved”.

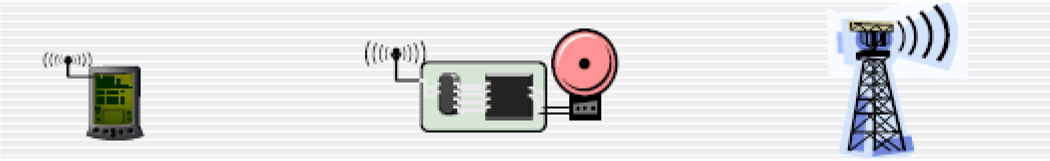
1.3.Participants in WSN:

Many of these applications share some basic characteristics. The major participants in WSN are Source, Sink and actuator.

Source of data: It measures and report data to "somewhere". In WSN it is usually equipped with different kind of sensor based on required application.



Sinks of data: It is interested in receiving data and it may be external or internal entity in WSN



Actuator: It controls the device based on the measured data.

1.4 Interaction patterns

The **interaction patterns** between sources and sinks show some typical patterns. The most relevant ones are:

Event detection Sensor nodes should report to the sink(s) once they have detected the occurrence of a specified event. The simplest events can be detected locally by a single sensor node in isolation (e.g. a temperature threshold is exceeded); more complicated types of events require the collaboration of nearby or even remote sensors to decide whether a (composite) even this occurred (e.g. a temperature gradient becomes too steep). If several different events can occur, **event classification** might be an additional issue.

Periodic measurements Sensors can be tasked with periodically reporting measured values. Often, these reports can be triggered by a detected event and the reporting period is application dependent.

Function approximation and edge detection The way a physical value like temperature changes from one place to another can be regarded as a function of location. A WSN can be used to approximate this unknown function (to extract its spatial characteristics), using a limited number of samples taken at each individual sensor node. This approximate mapping should be made available at the sink.

Tracking The source of an event can be 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(s), potentially with estimates about speed and direction as well. To do so, typically sensor nodes have to cooperate before updates can be reported to the sin**k.**

1.5Deployment options for WSN

The sensor nodes are deployed in the environment in following manner they are

1.Random deployment

2.Regular deployment

1.5.1Random deployment:

Usually uniform random distribution for nodes over a finite area is assumed.

1.5.2 Regular deployment:

Well planned, fixed, Not necessarily a geometric structure but often a convenient assumption.

1.6Challenges for WSNs

Handling such a wide range of application types will hardly be possible with any single realization of a WSN. Nonetheless, certain common traits appear, especially with respect to the characteristics and the required mechanisms of such systems. Realizing these characteristics with new mechanisms is the major challenge of the vision of wireless sensor networks.

1.6..1Characteristic requirements

The following characteristics are shared among most of the applications.

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 Closely related to the type of a network's service is the quality of that 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.
The packet delivery ratio is an insufficient metric; what is relevant is the amount and quality of information that can be extracted at given sinks about the observed objects or area. Therefore, adapted quality concepts like reliable detection of events or the approximation quality of a, say, temperature map is important.

Fault tolerance Since 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. To tolerate node failure, redundant deployment is necessary, using more nodes than would be strictly necessary if all nodes functioned correctly.

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.

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. Even within a given application, density can vary over time and space because nodes fail or move; the density also does not have to homogeneous in the entire network (because of imperfect deployment, for example) and the network should adapt to such variations.

Programmability Not only will it be necessary for the nodes to process information, but also they will have to react flexibly on changes in their tasks. These 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, the system has to adapt. It has to monitor its own health and status to change operational parameters or to choose different trade-offs. In this sense, the network has to maintain itself; it could also be able to interact with external maintenance mechanisms to ensure its extended operation at a required quality.

1.6.2 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. On the other hand, these mechanisms also have to generalize to a wider range of applications.

Some of the mechanisms that will form typical parts of WSNs are:

Multihop wireless communication While wireless communication will be a core technique, a direct communication between a sender and a receiver is faced with limitations. 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, for many forms of WSNs, so-called *multihop communication* will be a necessary ingredient.

Energy-efficient operation To support long lifetimes, energy-efficient operation is a key technique Options to look into include energy-efficient data transport between two nodes (measured in J/bit) or, more importantly, the energy-efficient determination of a requested information. Also, non homogeneous energy consumption – the forming of "hotspots" – is an issue.

Auto-configuration A WSN will have to configure most of its operational parameters autonomously, independent of external configuration the sheer number of nodes and simplified deployment will require that capability in most applications. As an example, nodes should be able to determine their geographical positions only using other nodes of the network – so called "self-location". Also, the network should be able to tolerate failing nodes or to integrate new nodes.

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.

An example is to determine the highest or the average temperature within an area and to report that value to a sink. To solve such tasks efficiently, readings from individual sensors can be *aggregated* as they propagate through the network, reducing the amount of data to be transmitted and hence improving the energy efficiency.

Data centric Traditional communication networks are typically centered around 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 a WSN, where nodes are typically deployed redundantly to protect against node failures or to compensate for the low quality of a single node's actual sensing equipment, the identity of the particular node supplying data becomes irrelevant. Hence, switching from an address-centric paradigm to a **data-centric** paradigm in designing architecture and communication protocols is promising.

Locality Rather a design guideline than a proper mechanism, the principle of locality will have to be embraced extensively to ensure, in particular, scalability. 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. The hope is that this will allow the network to scale to large numbers of nodes without having to rely on powerful processing at each single node.

Exploit trade-offs Similar to the locality principle, 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. Another important trade-off is node density: depending on application, deployment, and node failures at runtime, the density of the network can change considerably – the protocols will have to handle very different situations, possibly present at different places of a single network.

1.7 **Mobile ad hoc networks and wireless sensor networks**

An ad hoc network is a network that is setup, literally, for a specific purpose, to meet a quickly appearing communication need. The simplest example of an ad hoc network is perhaps a set of computers connected together via cables to form a small network, like a few laptops in a meeting room. In this example, the aspect of *self-configuration* is crucial – the network is expected to work without manual management or configuration. Usually, however, the notion of a MANET is associated with wireless communication and specifically *wireless* multihop communication; also, the name indicates the mobility of participating nodes as a typical ingredient. Examples for such networks are disaster relief operations – firefighters communicate with each other – or networks in difficult locations like large construction sites, where the deployment of wireless infrastructure (access points etc.), let alone cables, is not a feasible option. In such networks, the individual nodes together form a network that relays packets between nodes to extend the reach of a single node, allowing the network to span larger geographical areas than would be possible with direct sender – receiver communication. The two basic challenges in a MANET are the reorganization of the network as nodes move about and handling the problems of the limited reach of wireless communication. These general problems are shared between MANETs and WSNs. Nonetheless, there are some principal differences between the two concepts, warranting a distinction between them and regarding separate research efforts for each one.

Applications and equipment MANETs are associated with somewhat different applications as well as different user equipment than WSNs: in a MANET, the terminal can be fairly powerful (a laptop or a PDA) with a comparably large battery. This equipment is needed because in the typical MANET applications, there is usually a human in the loop: the MANET is used for voice communication between two distant peers, or it is used for access to a remote infrastructure like a Web server. Therefore, the equipment has to be powerful enough to support these applications.

Application specific Owing to the large number of conceivable combinations of sensing, computing, and communication technology, many different application scenarios for WSNs become possible. It is unlikely that there will be a "one-size-fits-all" solution for all these potentially very different possibilities. As one example, WSNs are conceivable with very different network densities, from very sparse to very dense deployments, which will require different or at least adaptive protocols. This diversity, although present, is not quite as large in MANETs.

Environment interaction Since WSNs have to interact with the environment, their traffic characteristics can be expected to be very different from other, human-driven forms of networks. A typical consequence is that WSNs are likely to exhibit very low data rates over a large timescale, but can have very bursty traffic when something happens. MANETs, on the other hand, are used to support more conventional applications (Web, voice, and so on) with their comparably well understood traffic characteristics.

Scale Potentially, WSNs have to scale to much larger numbers (thousands or perhaps hundreds of thousands) of entities than current ad hoc networks, requiring different, more scalable solutions. Endowing sensor nodes with a unique identifier is costly(either at production or at runtime) and might be an overhead that could be avoided – hence, protocols that work without such identifiers might become important in WSNs, whereas it is fair to assume such identifiers to exist in MANET nodes.

Energy In both WSNs and MANETs, energy is a scare resource. But WSNs have tighter requirements on network lifetime, and recharging or replacing WSN node batteries is much less an option than in MANETs. Owing to this, the impact of energy considerations on the entire system architecture is much deeper in WSNs than in MANETs.

Self configurability Similar to ad hoc networks, WSNs will most likely be required to self configure into connected networks, but the difference in traffic, energy trade-offs, and so forth, could require new solutions. Nevertheless, it is in this respect that MANETs and WSNs are probably most similar.

Dependability and QoS The requirements regarding dependability and QoS are quite different. In a MANET, each individual node should be fairly reliable; in a WSN, an individual node is next to irrelevant. The qualities of service issues in a MANET are dictated by traditional applications (low jitter for voice applications, for example); for WSNs, entirely new QoS concepts are required, which also take energy explicitly into account.

Data centric Redundant deployment will make data-centric protocols attractive in WSNs. This concept is alien to MANETs. Unless applications like file sharing are used in MANETs, which do bear some resemblance to data centric approaches, data-centric protocols are irrelevant to MANETs – but these applications do not represent the typically envisioned use case.

Simplicity and resource scarceness Since sensor nodes are simple and energy supply is scarce, the operating and networking software must be kept orders of magnitude simpler compared to today's desktop computers. This simplicity may also require breaking with conventional layering rules for networking software, since layering abstractions typically cost time and space. Also, resources like memory, which is relevant for comparably heavy-weight routing protocols as those used in MANETs, is not available in arbitrary quantities, requiring new, scalable, resource-efficient solutions.

Mobility The mobility problem in MANETs is caused by nodes moving around, changing multihop routes in the network that have to be handled. In a WSN, this problem can also exist if the sensor nodes are mobile in the given application. There are two additional aspects of mobility to be considered in WSNs.

1.8 Fieldbuses and wireless sensor networks

Fieldbuses are networks that are specifically designed for operation under hard real-time constraints and usually with inbuilt fault tolerance, to be used predominantly in control applications, that is, as part of a control loop. Examples include the Profibus and IEEE 802.4

Since fieldbuses also have to deal with the physical environment for which they report sensing data and which they control, they are in this sense very similar to WSNs. WSNs can be considered examples of wireless fieldbuses. Some differences do exist, however: WSNs do mostly not attempt to provide real-time guarantees in the range of (tens of) milliseconds but are rather focused on applications that can tolerate longer delays and some jitter (delay variability). Also, the adaptive trade-offs that WSNs are willing to make (accuracy against energy efficiency, for example) is a concept that is not commonly present in the fieldbus literature; specifically, fieldbuses make no attempt to conserve energy, and their protocols are not prepared to do so.

1.9 Enabling technologies for wireless sensor networks

Building such wireless sensor networks has only become possible with some fundamental advances in enabling technologies. First and foremost among these technologies is the miniaturization of hardware. Smaller feature sizes in chips have driven down the power consumption of the basic components of a sensor node to a level that the constructions of WSNs can be contemplated.

The three basic parts of a sensor node have to accompany by power supply. This requires, depending on application, high capacity batteries that last for long times, that is, have only a negligible self-discharge rate, 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. Such a concept requires the battery to be efficiently chargeable with small amounts of current, which is not a standard ability.

The counterpart to the basic hardware technologies is software. The first question to answer here is the principal division of tasks and functionalities in a single node – the architecture of the operating system or runtime environment. This environment has to support simple retasking, cross-layer information exchange, and modularity to allow for simple maintenance. This software architecture on a single node has to be extended to a network architecture, where the division of tasks between nodes, not only on a single node, becomes the relevant question – for example, how to structure interfaces for application programmers. The third part to solve then is the question of how to design appropriate communication protocols.

1.10 CONCLUSION

This chapter has introduced the Wireless Sensor Networks and its applications in detail and it gives enough information about challenges, basic requirements and enabling technologies of Wireless Sensor Networks.

SHORT QUESTIONS

1. Define Wireless Sensor Networks

Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc.

2. What is the role of participants in Wireless Sensor Networks?

The participants are Source of data, sink of data and actuators. The source of data measures data and report them somewhere, sink of data is interested in receiving data from WSN and actuators control some device based on data, usually also a sink.

3. State the various interaction patterns between source and sink.

The various interaction patterns between source and sink are event detection, Periodic measurement, Function approximation, Edge detection and Tracking.

4. List out the drawbacks of infrastructure based wireless networks.

It is too expensive/inconvenient to set up.

It takes more amount of time to install a network.

5. Define energy scavenging.

Some of the unconventional energy stores described in above fuel cells, heat engines radioactivity convert from stored, secondary form into electricity in a less direct and easy to use way than a normal battery would do. The entire supply is strode on the node itself once the fuel supply is exhausted, the node fails. To ensure truly long- lasting nodes and wireless sensor networks, such a limited energy storing is unacceptable. Rather, energy from node's environment must be tapped into and made available to the node energy scavenging.

6. State the deployment options for Wireless Sensor Networks.

The deployment options for wireless sensor networks are random deployment and regular deployment

7. What is data centric Network?

The network design mainly focused on data and not on node identifies and it is mainly done to improve efficiency of network.

8. Why mutihop wireless communication is required for Wireless Sensor Networks?

The multihop wireless communication is required for Wireless Sensor Networks because the distance between source and destination are very large. Direct communication is usually affected by distance, obstacles etc.

9. Mention the characteristics requirements of Wireless Sensor Networks.

The characteristics requirements of Wireless Sensor Networks are

i) Type of service of WSN

ii) Quality of service

iii) Fault tolerance

iv) Lifetime

v) Scalability

vi) Wide range of densities

vii) Programmability

viii) Maintainability

10.What is mobile Adhoc network?

A wireless network that transmits from computer to computer of using a central base station to which all computers must communicate, this peer-to-peer mode of operation ca greatly extend the distance of the wireless network.

11.Waht is actuator?

An actuator is a type motor for moving or controlling mechanism or system. It is operated by a source of energy, usually in the form of electric current.

12. List some applications of Wireless Sensor Networks.

The wireless sensor networks can be used in

i) Area monitoring

ii) Environmental/Earth monitoring

iii) Air quality monitoring

iv) Forest fire detection

v) Landslide detection

13.What is field bus?

Field Bus is the name of a family of industrial computer network protocols used for real time distributed control, now standardized as IEC 61158.

14. Write the goal of sensor Networks.

The fundamental goal of a sensor network is to produce globally meaningful information from raw local data obtained by individual sensor nodes.

15. What is meant by routing?

It is the process of determining a network path from a source node to destination node to deliver a packet.

16.Compare MANET and WSN.

i) Application equipment: MANETs more powerful equipment assumed, often "human in the loop"- type applications, higher data rates, more resources.

ii) Application specific: WSNs depend much energy stronger on application specific s, MANETs comparably uniform.

iii) Environment interaction: core of WSN, absent in ANET

iv) Scale: WSN might be much larger than MANETs

v) Dependability/QoS: In WSN, individual node may be dispensable, QoS different because of different applications.

vi) Data centric vs. id- centric networking

vii) Mobility: WSN have different mobility pattern.

viii) Energy: WSN tighter requirements, maintenance issues.

17. **Compare field buses and WSN**

Scale- WSN often intended for larger scale

Real time-WSN usually not intended to provide real-time guarantees as attempted by fieldbusses.

18. Write the differences between WSN and Ad hoc.

i) WSN broadcast but Ad hoc point to point.

ii) Sensor node limited in power computation capacities and memory.

iii) Sensor nodes may not have global identification

19. Why do many unique challenges arise in sensor networks?

i) Opportunity to architect security solutions into systems from the outset.

ii) Many applications are likely to involve the deployment of sensor networks. Under a single administrative domain, simplifying the threat model.

iii) It may be possible to exploit redundancy, scale and the physical characteristics of the environment in the solutions.

20. List the advantages and disadvantages of wireless sensor networks.

Advantages:

1. It avoids a lot of wiring
2. It can be accommodate new devices at any time.
3. It's flexible to go through physical partitions.
4. It can be accesses through a centralized monitor.
5. Low maintenance cost though little bit high cost of initial investment.

Disadvantages:

1. It is easy for hacker to hack it.

2. Comparatively low speed of communication
3. **More expensive**

REVIEW QUESTIONS

1. Explain the core challenges of Wireless Sensor Networks.(NOV/DEC-2012)

2. Explain in detail about the application for Wireless Sensor Networks.

3. Explain the innovative mechanism to realize the characteristics requirements of WSN.

4. Explain in detail how to enable technologies for Wireless Sensor Networks.

5. Compare MANET and WSN.

6. Explain how sensor networks employed as a bridge to the physical world.(NOV/DEC-2012)

7. Explain the various interaction patterns of Wireless Sensor Networks.