UNIT 2

Mobile Ad-hoc Networks and Wireless Sensor Networks

Syllabus

Mobile Ad-hoc Networks (MANETs) and Wireless Sensor Networks, Enabling Technologies for Wireless Sensor Networks. Issues and Challenges in Wireless Sensor Networks.

Learning Objectives

- ✓ Introduction to Personal Area Network
- ✓ Various Networking Topologies
- ✓ MANET and its Properties
- ✓ Applications of MANET
- ✓ Introduction to WANET
- ✓ Various issues in Wireless Sensor Networks
- ✓ Various Challenges involved in Wireless Sensor Networks.

Introduction

A Mobile Ad hoc Network (MANET) is a self-configuring network of mobile routers, which are connected through various wireless links forming an arbitrary topology. It is a kind of wireless ad hoc network that transmits the information from one computer to another computer. It can be considered as an autonomous network that comprises of routing nodes which can move freely. These mobile wireless nodes can create network dynamically without using any pre-existing infrastructure.

The mobile ad hoc network of smart sensors with communication, networking and computational features is referred to as wireless sensor networks. The development of WSN is possible only with advancements of various hardware technologies.

PART-B ESSAY QUESTIONS WITH SOLUTIONS

2.1 MOBILE AD-HOC NETWORKS (MANETs) AND WIRELESS SENSOR NETWORKS

Q9. Explain in detail about Personal Area Network (PAN) and MANETs. Model Paper-I, Q4(a)

Answer :

Personal Area Network (PAN)

The Personal Area Network (PAN) is a network that interconnects several computing devices to be used by an individual. These devices must be located physically together and connected for sharing the data, hardware internet connection etc. It helps to communicate and transmit data among multiple hardware devices using one computer. A computer by default will communicate with mobile computer such as PDA, mobile phone and electronic equipment such as camera, scanner, printer etc. All the hardware components in a PAN can be connected through wire or wireless method.

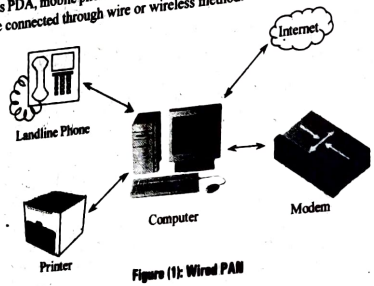

Figure (1): Wired PAN

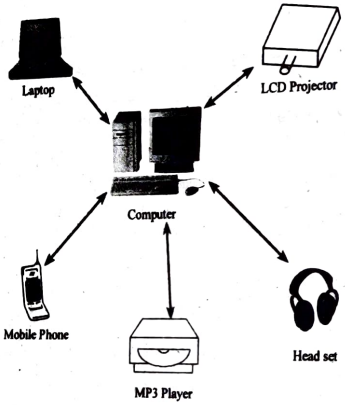

Figure (2): Wireless PAN

In wireless PAN the devices need to be in the radio vicinity of each other in order to create a communication medium among them. The bluetooth protocols allow them to form a network only when they are in the vicinity of each other. A device can then find out the services offered by other devices and then obtains them.

MANETs

For answer refer Unit-II, Q13.

Q10. Explain in brief about hidden node and exposed node problems.

Answer :

Hidden Node Problem

A set of nodes which are unreachable to other nodes in a wireless network are called hidden nodes. Consider a physical star topology that has an access point along with the nodes enclosing it in circular fashion. That is, all the nodes are within the range of access point, but are unable to interact with each other, since they are not connected physically. A node which is at the far edge of the range of access point, called P, in a wireless network can view the access point. But, it cannot see the node 'R' which is at the opposite end of the access point range. Such nodes are referred as hidden nodes. When both of these nodes start sending packets simultaneously to another node Q, the problem occurs. The carrier sensing multiple access without collisions will not work because P and R are unable to sense the carrier. Therefore, collisions occur because of which the data gets corrupted at the access point.

This problem can be overcome by handshaking along with CSMA/CA scheme.

Exposed Node Problem

An exposed terminal problem occurs when a node gets blocked due to its incapability of transmitting node (nearby node) to transmit data to the other node. It reduces the throughput of the network when the traffic load increases.

For example, when node 2 and node 3 wishes to transmit data to node 1 and some other terminal respectively, node 3 stops its transmission as it is exposed to node 2.

Q11. What are different networking topologies for wireless sensors? Explain.

Answer : Model Paper-II, Q4(a)

The different networking topologies for wireless sensor networks are as follows,

1. Bus topology
2. Star topology
3. Tree topology
4. Ring topology
5. Mesh topology.

1. Bus Topology

In bus topology, all the computers are connected to a long cable called a bus. A node that wants to send data puts the data on the bus which carries it to the destination node. In this topology, any computer can send data over the bus at anytime. Since, the bus is shared among all the computers. When two or more computers want to send data at the same time, an arbitration mechanism is needed to prevent simultaneous access to the bus.

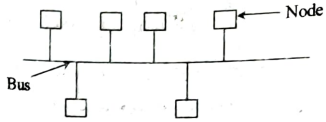

Figure (1): Bus Topology

A bus topology is easy to install, but is not flexible i.e., it is difficult to add a new node to a bus. In addition to this, the bus stops functioning even if a portion of the bus breaks down. It is also very difficult to isolate fault.

2. Star Topology

In star topology, all the nodes are connected to a central node called a hub. A node, that wants to send data to some other node on the network, send data to the hub which in turn sends it to the destination node. The hub plays a major role in such networks.

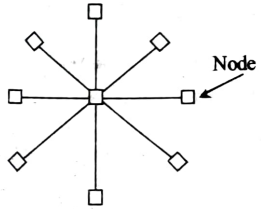

Figure (2): Star Topology

Star topology is easy to install and reconfigure. If a link fails, then it separates the node connected to link from the network and the network continues to function. However, if the hub goes down, the entire network collapses.

3. Tree Topology

Tree topology is a hierarchy of various hubs. All the nodes are connected to one hub or the other. There is a central hub to which, only a few nodes are connected directly.

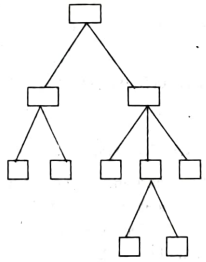

Figure (3): Tree Topology

The central hub is also called as active hub which looks at the incoming bits and regenerates them so that, they can traverse over longer distances. The secondary hubs in a tree topology may be active hubs or passive hubs. The failure of a transmission line separates a node from the network.

4. Ring Topology

In ring topology, the computers are connected in the form of a ring. Each node has exactly two adjacent neighbours. To send data to a distant node on a ring, it passes through many intermediate nodes to reach to its ultimate destination.

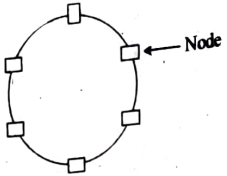

Figure (4): Ring Topology

A ring topology is easy to install and reconfigure. In this topology, fault isolation is easy because, a signal that circulates all the time in a ring helps in identifying a faulty node.

The data transmission takes place in only one direction. When a node fails in a ring, it breaks down the whole ring. To overcome this drawback some ring topologies use dual rings. The topology is not useful to connect large number of computers.

5. Mesh Topology

A mesh topology is also called as complete topology. In this topology, each node is connected directly to every other node in the network. That is, if there are n nodes then there would be $n(n-1)/2$ physical links in the network.

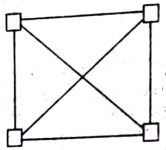

Figure (5): Mesh Topology

As there are dedicated links, the topology does not have congestion problems. Further, it does not need a special Media Access Control (MAC) protocol to prevent simultaneous access to the transmission media, since links are dedicated, not shared. The topology also provides data security. The network can continue to function even in the failure of one of the links. Fault identification is also easy.

The main disadvantage of mesh topology, is the complexity of the network and the cost associated with the cable length. The mesh topology is not useful for medium to large networks.

Q12. Explain about bluetooth based PAN.

Answer :

Personal Area Networks (PAN)

Personal Area Network (PAN) introduces a new form of communication network called bluetooth based PAN. It evolve new developments into the mobile network so as to service the user domain. It offers GPRS/UTMS services on mobile phone with which the user can connect to internet or to incorporate IP network. However in contrast to mobile phone network, the PAN networks are always fully loaded at the time of traffic congestion. This problem can easily be solved by interconnecting the bluetooth PAN's with scatternets. The below figure shows the interconnection of four PAN's.

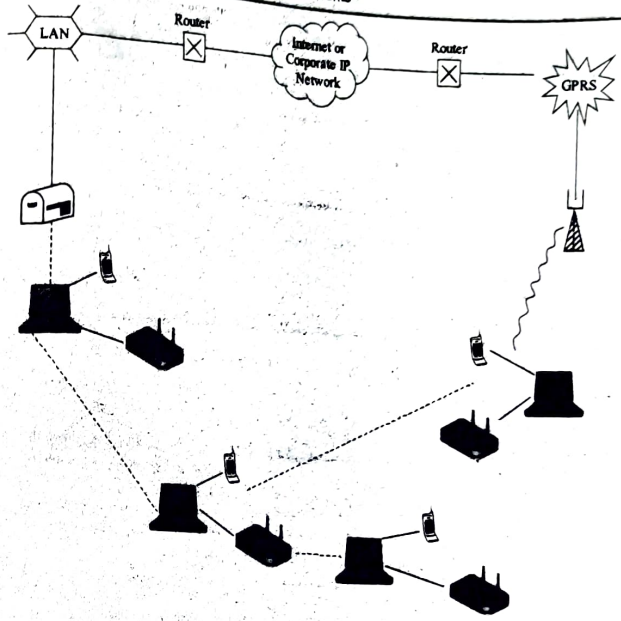

Figure: Interconnection of Four Bluetooth PANs

In the above figure, several PANs are connected along with the bluetooth links through laptop computers. A pair of these PAN's are connected to an IP backbone network among which one is connected through a GPRS/UMTS phone and the other is connected through a LAN access point. PAN supports large number of access technologies which are shared among the available devices to take advantage of the ad hoc functionality. In addition to this, it enables inclusion of new devices as well as technologies in the PAN framework.

Q13. Discuss about the topology of MANET.

Answer : **Model Paper-I, Q4(b)**

Mobile Ad hoc Network

A Mobile Ad hoc Network (MANET) is a self-configuring network of mobile routers, which are connected through various wireless links forming an arbitrary topology. It is a kind of wireless ad hoc network that transmits the information from one computer to another computer. It can be considered as an autonomous network that comprises of routing nodes which can move freely. These mobile wireless nodes can create network dynamically without using any pre-existing infrastructure.

The nodes present in MANET generates the user and application traffic and perform the network control and routing protocols. Many practical applications use ad hoc networks because it can be easily and quickly deployed.

Several problems may arise during the design of mobile adhoc networks which as follows,

(i) Wireless medium which possess the sharing nature.

(ii) Limited wireless connectivity range.

(iii) Mobility of nodes.

(iv) Energy constraints.

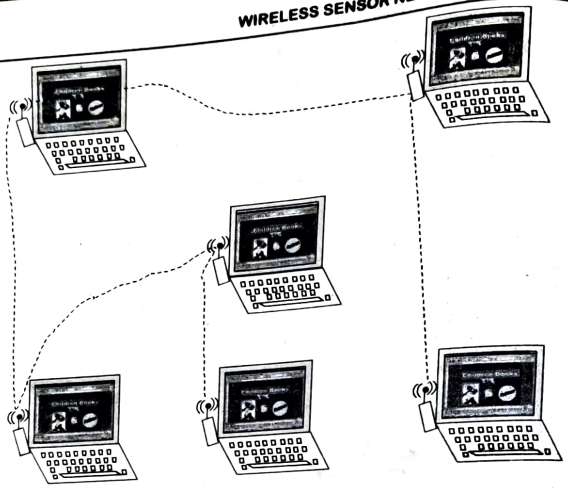

Figure: Mobile Adhoc Network (MANET)

Mobile adhoc network is decentralized wherein the mobile nodes has the routing functionality i.e., the nodes themselves perform all the network tasks like topology discovery and message delivery. The applications used for MANETs are different ranging from small static networks (that possess resource constraints) to large dynamic networks (that are large and mobile). The design of network protocols become complicated for these kind of networks. MANETs need efficient distributed algorithms so that, scheduling and routing network organizations can be determined.

In case of static networks, the shortest path from source to destination node is considered as an optimal route. But this mechanism is hardly extended in MANETs. The following are the relevant issues that arise in MANETs,

(i) Wireless link nature

(ii) Propagation path loss

(iii) Multiuser interference

(iv) Power consumed

(v) Fading

(vi) Frequent changes in topology, etc.

MANETs perform the network functionality even in the absence of fixed infrastructure. When there exists no access point in the ad hoc network, then the network facilities are provided by a popular and advance IEEE 802.11 Wi-Fi protocol. But in this situation, limited nodes are available for transmitting and receiving the information and no routing is done across the network. Mobile ad hoc networks operate independently or may be connected to a large network called Internet. The applications of MANETs include a military operation or a disaster recovery.

Q14. Explain the properties of MANETs.

Answer : Model Paper-II, Q5

The following are the properties of mobile ad hoc networks

1. MANET has the capability of establishing the networks quicker and faster. For establishing a new network, only one requirement is available and new set of nodes must be provided by MANET along with the limited wireless communication range. A node consumes only a less amount of power and has very little capability to communicate. Hence, these kind of nodes communicate only with the neighbouring nodes.
2. Mobile ad hoc networks depends upon the wireless transmission links. These links consume very less power than the wired links.
3. MANET has a dynamic topology and the periodic changes occurring in the topology are difficult to predict.
4. MANET nodes depend upon the limited power supply batteries so as to gain energy. But the energy savings are the basic criterion of a system design since, the operations performed by a node entirely depends upon the energy supply. Hence, node should be aware about the available power.
5. There exists a peer-to-peer connection between the nodes in MANET.
6. A MANET node has the ability of computing, switching (or routing), communicating independently. This provides a great potential to the users.
7. MANETs depends upon a multiple technologies instead of single technology they have the ability of capitalizing onto the various technology advances.
8. The basic property of a MANET is the neighbour discovery, that is used for both data transmission and reception. It has the capability of creating data routing paths, wherein the data can be routed from one node to its neighbouring node.
9. With the help of the service discovery protocol, a node in MANET identifies the service of a neighbouring node and explicitly makes a connection to a remote node.
10. In case of wireless network of limited connectivity range, MANET contains a network architecture that has a flexible nature and contains routing paths (that are variable) for communication purpose.
11. MANET nodes make use of various protocols like GSM, Bluetooth, IrDA, ZigBee 802.11 and TCP/IP.
12. A node in MANET can be a,
    (i) PC
    (ii) Ipod
    (iii) Smart sensors
    (iv) Smart labels
    (v) Handheld systems
    (vi) Automobile embedded systems.

Q15. What is mobile-adhoc networks and list its applications?

Answer :

Mobile Ad hoc Network

For answer refer Unit-II, Q13.

Applications of MANET

The following are the applications of mobile adhoc network.

1. **Military Applications**

Ad hoc wireless networks are used in setting up a communication between a group of soldiers, so that they can perform some strategic operations. A fixed infrastructure cannot be made for communication. Hence in this type of environments, the necessary communication mechanism is given by the ad hoc wireless networks. These wireless networks are also used in forming proper order of relationship between military objects that at high speeds like the flying of airplanes or warships. This type of application need a communication which is both quick and reliable. Here, secure communication is an important factor, because the issues such as eavesdropping or other security threats may hinder the use of communication required in strategic operations. In addition, reliable support and secure multimedia multicasting are also very important.

To maintain secure communication, all the vehicle-mounted nodes are very complex, highly developed as well as effective. Such nodes comprise of many transceivers that are of high power. These transceivers have the capability to hop among different range of frequency spectrum. In order to make such communication possible, it is necessary to have batteries with longer lifetime. However, using such batteries are economically not feasible. Communication system can employ various other services like location tracking, satellite-based services, so that efficient as well as coordinated communication is made possible.

2. **Collaborative and Distributed Computing**

Ad hoc wireless networks are useful in the collaborative computing where a temporary communication infrastructure along with least possible configuration is used for the communication between a group of people in a conference. The distributed file sharing applications doesn't need a secure communication. Instead a reliable transmission of data is required which is considered as an important factor in such applications.

Another application of ad hoc wireless network is the streaming of multimedia objects between the participating nodes. This need a soft real-time communication support. In these type of applications, economical and portable devices that have a battery source power are most probably preferable by the users. Thus, a mobile node has unidirectional links among its neighbours because of an adaptive (varying) transmission power and power drain.

3. **Emergency Operations**

The following emergency operations require ad hoc wireless networks.

(i) Search and rescue operations

(ii) Crowd control operations

(iii) Command operations.

The above tasks require the support of the following major factors of ad hoc wireless network.

(i) A self system configuration along with less overhead.

(ii) Mobility that has a free and flexible nature

(iii) Independent of fixed or centralized infrastructure.

(iv) Unavailability of conventional communication infrastructure etc.

Thus, for the coordination of rescue activities, adhoc wireless networks are mostly used.

4. **Wireless Mesh Networks**

Wireless mesh networks are a type of ad hoc wireless networks. These networks are used for the mobile or fixed nodes/ users by providing an alternate communication infrastructure. But, these networks do not use the network planning requirements of cellular networks and the spectrum reuse constraints. As wireless mesh networks has a mesh topology, there exists a quick path reconfiguration even if the node failure damages the existing path. Hence, there are many alternative paths for transferring the data between source and destination. The wireless mesh networks have some deployment designs such as residential zones, highways, business zones etc. Some advantages of these networks include,

(i) High data rate support

(i) High scalability

(iii) High availability

(iv) Quick and low cost of deployment

(v) Enhanced services

(vi) Easy extendability

(vii) Low cost per bit.

The deployment cost as well as the data transfer costs are very less when the communication is via wireless mesh networks (because of the efficient communication infrastructure). Mesh networks can accommodate a large number of nodes, because they have a very high scalability. If the mobile nodes have a very high density, then even at this level mesh networks obtain a better system throughput and a large number of users support. This is obtainable, because of the power control which is employed at mobile and relay nodes.

5. **Wireless Sensor Networks**

The nodes in the wireless sensor networks are the tiny devices that helps in,

(i) Sensing the physical parameters

(ii) Processing the data gathered

(iii) Communicating over the network to the monitoring station.

The sensor nodes present in a particular application domain are provided with a wireless communication infrastructure by the wireless sensor networks. The domain applications used for sensor networks includes health care, home security, military and environmental monitoring. Because of the following features sensor networks are considered as a special class of ad hoc wireless networks.

(i) **Nodes Mobility**

In sensor networks, it is not compulsory to have mobility support for the nodes.

(ii) **Network Size**

Sensor networks have a very large number of nodes than the ad hoc wireless networks.

(iii) **Deployment Density**

The density of nodes is dependent on the application domain i.e., as the domain of application changes the nodes density also varies.

(iv) **Power Constraints**

Even in the hard environments or geographical conditions, the nodes in the sensor networks operate with less or no maintenance and human control. This nature of the sensor nodes make the power constraints to be more severe than the constraints in the ad hoc wireless networks.

(v) **Replenishable Power Source**

In some applications of sensor networks, if the existing power source is completely depleted then that source can be substituted with the new one.

(vi) **Non-replenishable Power Source**

In certain applications, even if the existing power source is depleted, then that source cannot be replenished (substituted).

(vii) **Regenerative Power Source**

The power sources used in sensor networks can regenerate the power by using some appropriate measurement parameters.

6. **Hybrid Wireless Networks**

Ad hoc wireless networks are widely used in the hybrid wireless architectures like Integrated Cellular Ad hoc Relay (ICAR) networks and Multi-hop Cellular Networks (MCNs). The capacity or maximum throughout of the cellular networks and the equipment cost can be increased by most of the methods like cell resizing, cell sectoring and multi-tier cells. If the hybrid wireless networks contain multi-hop relaying properties and the existing fixed infrastructure support then the capacity of cellular networks can be increased. The multi-hop relaying properties and flexibility of ad hoc wireless networks are combined with the support and reliability of cellular networks base stations.

Hybrid wireless networks has the following advantages.

(i) Increased cellular network capacity.

(ii) Increased flexibility and reliability in routing.

(iii) A good connectivity and coverage in holes of a cell.

Q16. Compare MANET and WSN. **Model Paper-II, Q4(b)**

Answer :

	MANET		WSN
1.	Manet uses IEEE 802.11 standard to carryout its activities.	1.	WSN uses IEEE 802.15.4 standards to carryout its activities.
2.	It contains less number of nodes and has decentralized node movement.	2.	It contains more number of nodes and has centralized node movement.
3.	It follows point to point mode of communication.	3.	It follows broadcast mode of communication.
4.	It has high scalability.	4.	It has much higher scalability in comparison to MANET.
5.	It is deployed by several entities which are unrelated.	5.	It is deployed by single entity.
6.	It is used for distributed computing.	6.	It is used for information gathering.
7.	It is unique because it contains a unique id provided by MAC address.	7.	It does not have any unique identification.
8.	It uses pro-active, reactive, hybrid routing protocols.	8.	It uses flat routing, hierarchical, location based routing protocols.
9.	It has high data rates which is used to carry out rich multimedia data.	9.	It has low data rates.
10.	It has no data redundancy.	10.	It has data redundancy.
11.	It has less number of node failures.	11.	It has high number of node failures.
12.	It maintains interactions between humans.	12.	It maintains interaction with entire environment.
13.	It contains nodes which serves as a host and also as a router.	13.	It contains nodes which works separately.
14.	It has less memory constraints when compared to WSN.	14.	It has more memory constraints.

Q17. Write short notes on WANETs.

Answer :

Wireless Ad Hoc Network (WANET)

A WANET connects a number of mobile devices that communicate through wireless medium. They are treated as node in the network and they use radio transmitter and receiver to communicate with other devices. The communication links depend upon the wireless technologies and the structure topology of the network is built through dynamic network connectivity. It is not predefined. The common subtypes of these networks are Mobile Ad hoc Networks(MANETs), wireless sensor networks and wireless mesh networks.

WANET posses a unique feature like self organization so it does not require any base station for communication purpose. All the nodes present in the network plays the role of packet creator and router i.e., they create the packets as well as route them to their specified destination. It can extend its access offered in fixed network services by connecting to the gateways.

Hence, WANETs are multihop wireless networks inherently when compared with other networks.

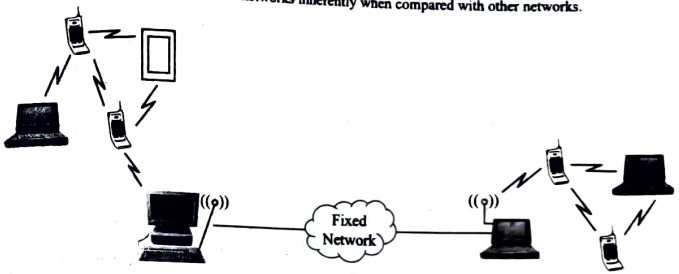

Figure (1): Fixed Network Multihop WANET

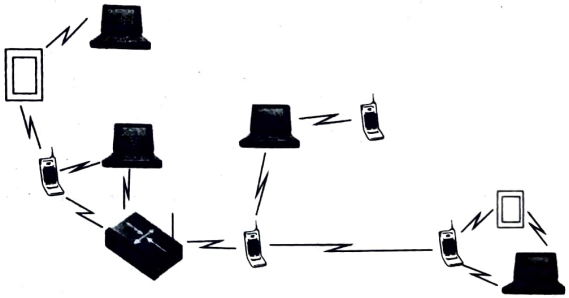

Figure (2): Self Organized Multihop WANET

2.2 ENABLING TECHNOLOGIES FOR WIRELESS SENSOR NETWORKS

Q18. Define wireless sensor networks. Explain in brief about the enabling technologies for wireless sensor networks.

Answer : **Model Paper-I, Q5(a)**

Wireless Sensor Networks

For answer refer Unit-I, Q9, Topic: Wireless Sensor Network (WSN).

Enabling Technologies for Wireless Sensor Networks

Development of wireless sensor networks is possible only with the advancement in enabling the technologies as given below,

1. The first technology adopted to propose the construction of wireless sensor network is to minimize the size of the hardware such as memory chips and microcontroller, which reduces the power consumption of all the components present in the sensor node.
2. The second technology adopted is the use of radio modems for wireless communications which utilizes the energy in an efficient manner. Thus reduced size of the hardware and enhanced energy efficiency also reduces the cost of the construction.
3. The third technology adopted is actual sensing equipment.

The above mentioned technologies have to be accomplished with the power supply. This needs batteries of very high capacity with an avoidable self discharge rate and which can provide the power in smaller units. However, this will be dependent on the type of application being developed.

In addition to the above hardware technologies, there is one more technology to be mentioned is the software. It involves providing the solutions for the below problems.

- How the functionality and tasks are divided in a single node architecture.
- How the operating system and run-time environment works in its architecture. Apart from this, the environment should support modularity, which enables the maintenance of data in a simpler way. It should also support cross layer information exchanged simple retasking.

1. An enhanced version of software architecture should be evolved called network architecture. In this, the problem of dividing the tasks between the multiple nodes exist.
2. The second problem of arranging the interfaces for the application programmers exist.
3. The third problem is adopting the appropriate design methodologies for communication protocols.

2.3 ISSUES AND CHALLENGES IN WIRELESS SENSOR NETWORKS

Q19. Explain design issues of wireless sensor networks. Model Paper-I, Q19)

Answer :

Some of design issues of WSN are as follows,

1. **Adhoc Deployment**

   The sensor nodes must be randomly distributed such that it must be acceptable by the system and provides the connection between the nodes. It must also tolerate with the failures occurring in the network.

2. **Computatioaal Capabilities**

   Sensor networks can perform only limited computations. They cannot handle complex protocols, hence the protocols design for them must be simple and of lighter version.

3. **Energy Consumption without Loosing Accuracy**

   Sensor nodes consume the energy by performing the computation and transmission of information. Even the nodes in a multi hoc network plays dual role by sending and routing the data. All these effect the nodes and their batteries life time. And also the power failure is a major issue which perform changes in the topology. These can be overcome by designing the protocol such that it can support packet rerouting and network reorganization.

4. **Scalability**

   The sensing region consists of many number of sensor nodes. Hence the routing protocol must be design such that it can cope up with the scalability.

5. **Communication Range**

   As the communication range increases the bandwidth of the supply of energy decreases. Hence to provide the effective inter sensor communication various wireless hops are deployed along the path from source to destination.

6. **Control Overhead**

   In wireless environment, on increase in the number of retransmission caused by collisions, the consumption of energy and latency also gets increased. This lead to linear rise in the control packet overhead along with the density of node. Thus, resulting in the existence of trade offs among the latency, conservation of energy and self-configuration.

7. **Fault Tolerance**

   The sensor nodes may get failed due to the reason such as interference caused by environment, physical disasters or low power supply. The routing and *MAC* protocols are designed such that they must tolerate with these failures by reestablishing the links and routes. They must also reduce the usage of energy by regulating signalling rates and transmission power.

8. **Connectivity**

   In WSN, nodes are highly connected to each other as it contains high density of nodes. And therefore, it is highly difficult for complete separation of nodes. However, the size and topology of the network cannot be precluded from shrinking (due to nodes damage) and varying, respectively. The connection of nodes in sensor network is based on its random distribution.

9. **Medium of Transmission**

   A multi-hop sensor network provide link to its nodes (to establish communication) through wireless media. Due to this, the complication of wireless channel such as high error rate, fading etc., have an impact on the functioning of sensor network. Normally, some application scenario of sensor network requires low bandwidth ranging 1-100 Kb/s. But it is difficult to design a *MAC* protocol of *WSNs* that can conserve energy.

10. **Quality of Service (QoS)**

    There are some time constrained applications that operate based on certain conditions like bounded latency or data delivery. This means, as soon as the sensor sense, the data it should deliver it with in a specified time period. If data delivery is late i.e., out of time period, then it will be considered as useless data.

11. **Security**

    In *WSNs* achieving of security is important. Here, security refers to authentication and encryption *WSN* with limited resources might not allow to implement complex algorithm to employ security. This will lead to the existence of trade off between the security level and energy consumption.

Q20. Discuss the security issues in MANETs.

Answer :

The following are the security issues that exist in MANET,

1. **Availability**

   The service attacks may be denied by some security system. Due to this, the available data present at the end user can be blocked by a source. Here, consider an example, where some intermediate router gives a wrong direction (because of the attack) for the packets to be passed from source to destination. Hence, due to this the packets or data are not allowed to reach destination.

2. **Confidentiality**

   The data can be read only by the authorized users. Confidentiality is a method in which the data is encrypted before transmission and it is decrypted after the data has been reached at the destination.

3. **Integrity**

   If data integrity is not maintained then a manipulated message is received by the user. And, if the system integrity is not maintained then a wrong node receives the message.

4. **Pre-keying**

   The encrypted messages are deciphered by exchanging a private key between the sender and receiver. Hence, this key may be trapped since it is exchanged over wireless systems.

5. **Non-repudiation**

If a sender transmits a message or information then he/she does not have the capability of denying that the message has been sent. Suppose, if a user buys a product through credit card then he does not have the capability of denying this.

6. **Resource Constraints**

The following are the mobile resource constraints,

(i) The speed of CPU is slow when compared to a conventional PC.

(ii) Limited memory is available.

(iii) Limited battery life.

A form of attack may be any one of the following,

(i) When data is transmitted or received repeatedly, the device-power gets exhausted.

(ii) When some irrelevant data is received then this may exhausts the device memory.

If these attacks occur in between the route then the entire network gets affected.

7. **Power of Detection**

Due to the attack, the mobile device (that doesn't have the capability to detect signals) receives the data or message through the jammed signals.

8. **Interception Replay**

There exists an interception of signals. The solution to the problem is CDMA and FHSS. If authentication requests and client responses are known, then they can be replayed continuously in the same sequence.

9. **Stealing of the Subscribed Service**

If an attacker seizes the user name and password then a service is received which is subscribed by another client.

10. **Mobility RisksQ**

If the locations of network have been changed then the signals are routed through the paths which may be incorrect.

11. **Spoofing (Impersonating Address)**

A node in a mobile ad hoc network can be treated as an address. Hence, all the routes may be blocked when a comma mode is used for various paths.

12. **Reconfiguration**

The manipulation of routing table leads to an attack which can be prevented by reconfiguring the network periodically.

13. **Eavesdropping**

When two sources are being communicated and some unwanted messages are passed from the another sources then th mechanism is referred to as eavesdropping.

14. **Traffic Analysis**

A security attack exists when the information is extracted from the network traffic analysis.

Some additional security issues in MANET include the following,

1. **Increased Threat of Eavesdropping**

The unwanted messages are transmitted in the wireless region. The probability of this transmission is increased in ad h networks. Each node must be able to identify itself before any other moving node within its vicinity. During this proces eavesdropping occur.

2. **Unknown Node Caching the Information**

To accept an unknown node in the network, rigorous authentication is required. Hence, this node becomes a part of the MANET.

3. **Denial of Service Attacks**

With the help of the attacking nodes, various transmission requests can be flooded into the system. Every request has an authentication process that requires the exchange of messages. Due to this, both MANET and services are blocked and denied respectively.

4. **Authenticated Node becoming Hostile**

For security attacks, the devices that are authenticated previously can be utilized.

Q21. Write short notes on Programming challenges in sensor network.

Answer :

Traditional programming techniques that are provided with processing abstraction, I/O, networking and user interaction hardware, through operating systems. Sensor network programming techniques (that are specify for programming networked embedded system) do not get ripe and such facilities and thereby have to explicitly manage all the task such as,

1. Message passing
2. Event synchronization
3. Interrupt handling and
4. Sensor reading.

This causes an application to exhibit Finite State Machine (FSM) properties, resulting in the following unwanted issues.

(i) Unreliable communication channels

(ii) Long delays

(iii) Irregular message arrival

(iv) Replicated events, etc.

For instance, 40 percent of the code in target tracking application of Linux can implement FSM.

Furthermore, though embedded operating systems employ may different mechanisms such as, 'Microkernel' for modularization of operating system, 'Real time scheduling' for allocating resources to high priority tasks, and 'event driven execution' for conservation of processing power. They are not suitable for programming of sensor networks, because of the following reasons,

1. Sensor networks are large-scale distributed system that derive properties from a large number of its distributed nodes. This complicates the implementation of distributed algorithms which is further influenced by the limited and to formation and limited resources such as power, memory and bandwidth.
2. Sensor networks has to manage simultaneous invocations at the speed of manipulation of physical needs, as they are effectively incorporated in physical world.

IMPORTANT QUESTIONS

SHORT QUESTIONS

Q1. What is Personal Area Network?

Ans: For answer refer Unit-II, Q1.

Q2. What is exposed node problems and hidden node problems?

Ans: For answer refer Unit-II, Q2.

Q3. Write about the military applications of MANETs.

Ans: For answer refer Unit-II, Q5.

Q4. Discuss any four security issues in MANET.

Ans: For answer refer Unit-II, Q7.

Q5. Discuss the few programming challenges in sensor networks.

Ans: For answer refer Unit-II, Q8.

ESSAY QUESTIONS

Q6. Explain in detail about Personal Area Network (PAN) and MANETs.

Ans: For answer refer Unit-II, Q9.

Q7. What are different networking topologies for wireless sensors? Explain.

Ans: For answer refer Unit-II, Q11.

Q8. Discuss about the topology of MANET.

Ans: For answer refer Unit-II, Q13.

Q9. What is mobile-adhoc networks and list its applications?

Ans: For answer refer Unit-II, Q15.

Q10. Compare MANET and WSN.

Ans: For answer refer Unit-II, Q16.

Q11. Define wireless sensor networks. Explain in brief about the enabling technologies for wireless sensor networks.

Ans: For answer refer Unit-II, Q18.

Q12. Explain design issues of wireless sensor networks.

Ans: For answer refer Unit-II, Q19.

Q13. Write short notes on Programming challenges in sensor network.

Ans: For answer refer Unit-II, Q21.