EC 8702-AD HOC AND WIRELESS SENSOR NETWORKS

TWO MARKS QUESTIONS WITH ANSWERS & QUESTION BANK

UNIT-1 Ad-Hoc Networks- Introductions and Routing Protocol

Elements of Ad hoc Wireless Networks, Issues in Ad hoc wireless networks, Example commercial applications of Ad hoc networking, Ad hoc wireless Internet, Issues in Designing a Routing Protocol for Ad Hoc Wireless Networks, Classifications of Routing Protocols, Table Driven Routing Protocols - Destination Sequenced Distance Vector (DSDV), On–Demand Routing protocols –Ad hoc On–Demand Distance Vector Routing (AODV).

PART-A

1. What is an Ad-Hoc Network?

- The term 'ad hoc' implies spontaneous construction of temporary wireless network that composed of individual devices communicating with one another directly with no centralized administration.
- Due to above ad hoc is an infrastructure less network otherwise Multi-hop wireless network (MHWN) in that computers or other devices are enabled to send data packets on to each other instead of browsing a centralized access point
- In other words Ad hoc networks are temporary network composed of mobile nodes without pre-existing communication infrastructure such as AP (Access Point) and BSS (Basic service set). Each node plays the role of router for multi-hop routing.

2. Define MHWN?

Multi-hop wireless network (MHWN) is defined as a set of nodes that communicate with one another wirelessly by using radio signals with a shared common channel. There are several names for MHWN; it might be called packet radio network, Ad-Hoc network or temporary mobile network.

3. List Characteristics/Features of Ad-Hoc network?

- Dynamic topology
- Bandwidth constraints and variable links
- Energy controlled nodes
- Multi-hop communications
- Limited security
- Determining/detecting the sudden changes in network topology
- Maintaining network topology/connectivity
- Scheduling of packet transmission
- Finding the shortest path to reach required destination by proper routing protocols

- Maintaining network connectivity even under changing radio conditions and mobility
- Proper transmission scheduling and channel assignment.

4. List the advantages of Ad-Hoc networks over existing traditional networks?

- Ad-hoc network is more flexible than traditional networks.
- It supports even the nodes under the mobility
- It's having special capability like self-organization and self-reconfiguration.
- It can be "Turn Up" and "Turn Down" in a very short time.
- It can be more economical.
- No need of router and switches during construction of network.
- It supports a robust network because of its non-hierarchical distributed control and management mechanisms.

5. Difference between traditional (cellular) network and ad-hoc network?

Sno.	Cellular Network	Ad-Hoc Network
1.	Based on fixed infrastructure	Based on independent infrastructure or infrastructureless network
2.	It is a single hop wireless links	It is multi hop wireless links
3.	Guaranteed Bandwidth	Not Guaranteed Bandwidth
4.	It is circuit switched	Packet switched
5.	More time deployment required	Less time deployment
6.	Maintenance cost is high	Maintenance cost is low
7.	It belongs seamless connectivity	Frequent Path breaks take places
8.	Static frequency reuse spectrum	Dynamic frequency reuse spectrum
9.	Centralized routing based network	Distributed routing based networks
10.	Easier to achieve time synchronization	Time synchronization is difficult and consumes bandwidth
11.	Easier to employ bandwidth reservation	Bandwidth reservations requires complex medium access control protocols
12.	Application domains includes mainly civilian and commercial sectors	Application domains includes battlefields, emergency search and rescue operations and collaborative computing
13.	There is no self-organizing property	Self-organization, Self reconfiguration and maintenance properties are built into the network

14.	Mobile hosts are relatively less complexity	Mobile host requires more intelligence
15.	Major goals of routing and call admissions are to maximize the call acceptance ratio and minimize the call drop	Goal of routing is to find paths with minimum overheads and also quick reconfiguration of broken paths.
16.	Widely deployed and currently in the third generation of evolution.	Several issues are to be addresses for successful commercial deployment even though widespread use exists in defense.

6. Why Ad-Hoc network is needed?

Ad-hoc networking is often justified by scenario where you cannot deploy and manage an infrastructure based network; on that area we can construct a temporary wireless network without presence of any access point or base station for exchanging the required information in form of data packets between clients (nodes).

7. What are all the challenging issues that affect the performance of Ad-hoc wireless network maintenance?

The major issues that affect the design, deployment and performance of an ad-hoc wireless network system during

- Medium access scheme
- Routing
- Multicasting
- Transport layer protocol
- Pricing scheme
- Quality of service provisioning
- Self-Organization
- Security
- Energy management
- Addressing and Service discovery
- Scalability and deployment considerations

8. List out the various applications of ad-hoc network?

Due to their quick and economically less demanding deployment it finds applications in several areas like

- Military applications like remote sensing area(battle fields)
- Collaborative and distributed computing
- Environmental applications (during different weather conditions, forest fire detection and etc.,)

- Medical applications (monitoring medical diagnosing equipment and patients)
- Educational applications (video conferencing, virtual class rooms)
- During crisis conditions (Flood, earthquake, Tsunami locations)

9. What is Ad-Hoc Wireless Internet?

It is extend the service to end user in ad-hoc network, for provisioning the temporary internet service to

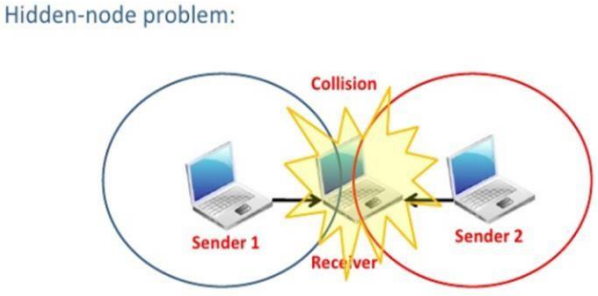
- Major conference venues
- Sports venues
- Temporary military settlements
- Battlefields
- Broadband internet service in rural regions

10. What is Gateway node? What are all the roles of Gateway node in ad-hoc wireless internet?

Gateway is one among the node in ad-hoc network which act as entry point to wired internet, and major part of internet service provisioning lies through this gateway node, generally this node is owned and operated by service provider, and its majors roles are

- Keep tracking the end user
- Bandwidth management
- Load balancing
- Traffic shaping
- Packet filtering
- Bandwidth fairness
- Address service and location discovery.

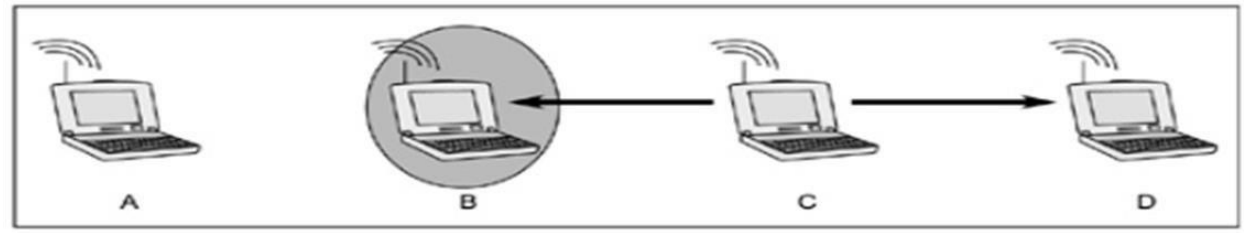
11. What is Hidden terminal problem?



- It refers to collision of packets at a receiving node due to simultaneous transmission of data packets by both senders (1 &2), because both senders are not in the radio range of each other.

- In other words hidden terminal problem is data packet transmission problem that arises when two sender nodes are out of range to each other, they transmits data packets simultaneously to a common receiver node, in that situation there is a chance for collision at receiver.

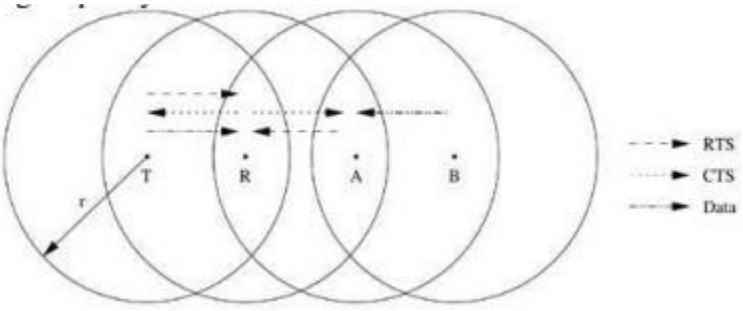
12. What is Exposed terminal Problem?



- C is transmitting to D.
- B overhears this, and is blocked.
- B wants to transmit to A, but is being blocked by C.
- Wasted bandwidth!

- It refers to inability of node for packet data transmission to its required destination node because the corresponding node is blocked by nearby transmitting node, such problems is called a exposed terminal problem.
- In other words exposed terminal problem is a transmission problem that arises when transmitting node is prevented from sending data packets due to interference with another transmitting node.

13. Give the solution for hidden terminal and exposed terminal problem?



- The solution of both problems is the transmitting node first explicitly notifies all potential hidden nodes about the forthcoming transmission by means of “two-way handshake control” called RTS (Request to send) and CTS (Clear to send). This may not solve the problem completely, but it reduces the probability of collisions.

- For reducing the probability of collisions an improved version of protocol has been proposed named as MACAW (Medium Access Collision Avoidance for Wireless).
- This MACAW protocol requires that the receiver acknowledges each successful reception of data packet. Hence successful avoidance of prevented transmissions and collisions to certain level by RTS, CTS, Data transmission and Data Acknowledgement.

14. List the four categories based that the routing protocols are classified in Ad-hoc Networks?

The routing protocols for ad hoc wireless networks can be broadly classified into four categories such as

- Routing information update mechanism
- Use of temporal information for routing
- Routing topology
- Utilization of specific resources.

15. What is proactive routing protocol or Table-driven routing protocol?

- In this protocol every node maintains the network global topology information in form of routing tables.
- Each routing tables consist information like destination node, next node (or) next hop, distance to reach destination, time-in, time-out along with sequence number.
- Routing information's is generally flooded in whole network by periodical exchanging.
- Whenever a node requires a path to destination, it runs an appropriate path-finding algorithm.
- Example-DSDV protocol.

16. What is Reactive (or) On-Demand Routing protocol?

- Protocols that fall under this category do not maintain the network topology information, also not maintaining any table information like proactive.
- They obtain the necessary path when it is required, by using a connection establishment process; hence these protocols do not exchange routing information periodically.
- Example- AODV protocol.

17. What are Hybrid Routing protocols?

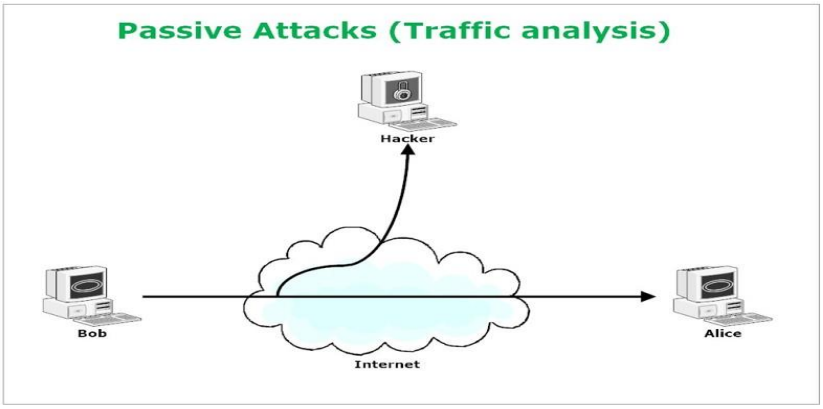
- It combines the best features of both proactive and reactive protocol, Nodes(TX/RX) with in reachable distance, or within a particular geographical

region, or within in same routing zone, a table-drive approach is used for data packet transmission.

- Nodes are in beyond the routing zone means on-demand approach is used for packet transmission

18. What are active and passive attacks during security issues in Ad-hoc wireless network?

Passive Attacks:

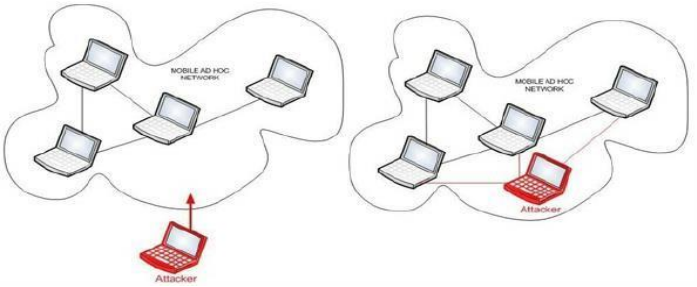


An interruption made by malicious node during data packet transmission between nodes and tries to observe or copy the message without disturbing the network operations called passive attacks

Active Attacks:

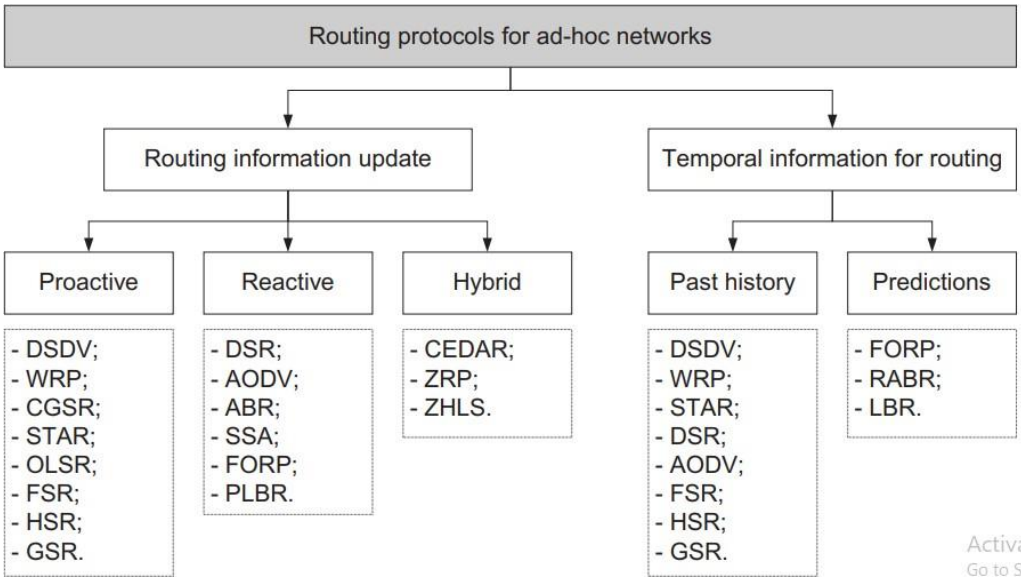
An attempt made by a node from outside the network, and tries to copy and modify the message in all disturbing the network operations is called active attacks.

19. What are internal and external attacks in ad-hoc wireless network?

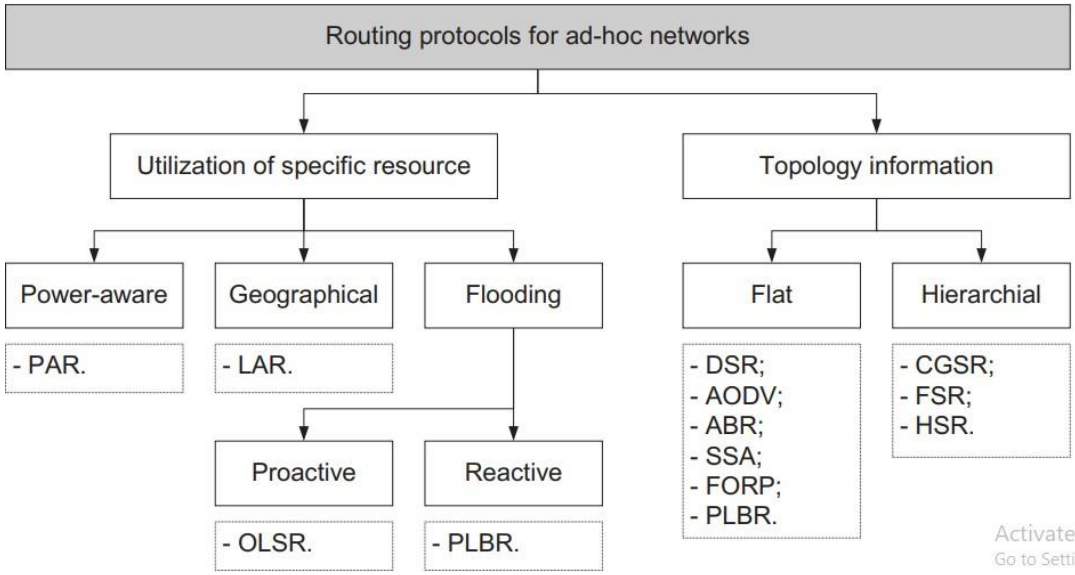


Copying or observing the data packets, modifying the users data packets during TX/RX by node with in network called *Internal Attacks*, if suppose by a node from outside the network belongs *External Attacks*

20. Write down the classification of routing protocol based on routing information update and temporal information in Ad-hoc network?



21. Write down the classification of routing protocol based on utilization of specific resource and topology information in ad-hoc network?



22. What are major activities in self-organization system in Ad-hoc wireless network?

The major activities of self-organization in ad hoc wireless network is following performances

a. Neighbor discovery
b. Topology organizations and
c. Topology reorganization.

During neighbor discovery phase every node in the network gathers information about its neighbor and maintain that information in appropriate data structures.

During topology organization phase, every node in network gathers information about the entire network or part of network in order to maintain topological information's

During topology reorganization phase, updating the topology information by incorporating the topology changes due to the following reasons

- Due to mobility of nodes
- Due to failure of nodes
- By complete depletion of power sources of the nodes.

23. What is meant self-configuring mechanism in ad-hoc network?

- This types mechanism based on typical approaches known as *route discovery approach* and *route update approach*
- In route discovery which can be "*done proactively* or *On-Demand basis*"
- In route update, single or multiple routes are maintained between a pair of nodes which helps a lot during unexpected path breaks takes place during packet transmission or reception duration.

24. What is meant by self-optimizing?

Self-Optimizing which helps to improve the routes with respect to route length (Path aware) or energy consumption (Energy aware) in ad-hoc network.

25. List the advantages of DSDV protocol?

- Less delay involved in the route setup process.
- Mechanism of incremental update with sequence number tags makes the existing wired network protocols adaptable to ad hoc wireless networks.
- The updates are propagated throughout the network in order to maintain an up-to-date view of the network topology at all nodes.

26. List the advantages of AODV protocol?

- Routes are established on demand
- Destination sequence numbers are used to find the latest route to the destination.
- The connection setup delay is less.

27. What is replay attack? How can it be prevented?

- A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it, possibly as part of a masquerade attack by IP packet substitution.
- Prevention Methods:
- Passwords:
  By implementing one-time passwords for sensitive communications, we can prevent the Reply attack. One-time passwords expire either after they've been used or after a short period of time. Either way they are useful for ensuring that important transactions or communications are only taking place between the intended parties.

Digital Signatures:

- Next, you could use digital signatures. A digital signature isn't your name, but rather a complex process that involves algorithms and "keys." Each computer has its own private key, one that only those machines know, to encrypt information on one end and decrypt it on the other. Think of it like sending a coded message to a friend - the only person who knows how to break the code.

28. Is a table-driven routing protocol suitable for high-mobility environments?

No. Table driven routing protocols are not suitable for high mobility environment.

UNIT-1 -PART-B & PART-C -IMPORTANT QUESTIONS

1. Explain the important issues in Adhoc wireless networks. [13 Marks]

2. Explain the commercial applications of Adhoc wireless networks. [13 Marks]

3. Write short notes on Adhoc-wireless internet. [8 Marks]

4. Explain the issues in designing a Routing Protocol for Adhoc wireless networks. [13 Marks]

5. Explain the classifications of Routing Protocols. [8 Marks]

6. Explain Table Driven Destination Sequence Distance Vector Routing Protocols [DSDV] with necessary diagrams. [15 Marks]

7. Explain Adhoc on Demand Distance Vector [AODV] Routing Protocol with necessary Diagrams. [15 Marks]

8. List the major advantages and disadvantages of the ad hoc wireless Internet. [6 Marks]

UNIT II: SENSOR NETWORKS – INTRODUCTION & ARCHITECTURES

Challenges for Wireless Sensor Networks, Enabling Technologies for Wireless Sensor Networks, WSN application examples, Single-Node Architecture - Hardware Components, Energy Consumption of Sensor Nodes, Network Architecture - Sensor Network Scenarios, Transceiver Design Considerations, Optimization Goals and Figures of Merit.

PART A

1. What are the types of node architecture?

(i) Single node architecture means only one sensor will placed on the system architecture.

(ii) Multiple node architecture means more than one sensor will be placed on the system architecture.

2. Mention the components used in the wireless sensor nodes.

1. Controller
2. Sensor/actuators
3. Memory
4. Communication devices
5. Power supply

3. What is meant by controller?

A controller is a processor that process all the relevant data to the task and capable of executing arbitrary code.

4. What is meant by flash memory?

Flash memory is a fastest memory it is used as immediate storage of data in case RAM is insufficient or when power supply of RAM should be shut down.

5. Give the application states of transceivers

1. Transmit state
2. Receive state
3. Idle state
4. Sleep state

6. What are the types of sensors?

1. Passive, Omni directional sensors
2. Passive, narrow beam sensors
3. Active sensors

7. Give the operational states of controller.

1. Active
2. Idle
3. Sleep

8. What is dynamic voltage scaling?

Dynamic voltage scaling is a technique used to reduce the energy consumption by applying such a technique the special care has to be taken to operate the controller within its specification.

9. What are the memories used to reduce energy consumption?

1. On- chip
2. Flash memory

10. What are the advantages of event base programming over process based programming?

1. Event based programming model on the same hardware and the performance is improved by a factor of 8.
2. In event based the instruction/data memory requirements were reduced by a factor of 2 to 30
3. Power consumption was reduced by a factor of 12.

11. What are types of mobility?

1. Node mobility
2. Sink mobility
3. Event mobility

12. What is need for gateway concepts?

The sensor network has a capability to interact with itself only, so the gateway is needed to enable the sensor network over the interact and other information.

13. What is robustness?

Robustness means network should fail when limited number of nodes runs out of energy in the network. Failure of nodes will be compensated using other router.

14. Give some examples of sensor nodes.

1. The mica mote nodes
2. EYES nodes
3. BT nodes
4. Scatter web

15. What is source and types of sources?

A source is an entity in the network that can provide information, i.e., typically a sensor node.

16. Give some examples of radio transceivers?

1. RFM TR100 family
2. Mica motes
3. Chipcon.CC100 and CC2420
4. IEEE 802.15.4/ Ember EM2420 RF transceiver.

17. What is the need of gateway concepts in WSN?

- Gateway is an entry and exit point for wireless data sensing and processing networks.
- It is considered to be a static node with no energy issues, with high calculation capability.
- Provides various connectivity options between sensor nodes (wireless sensing field devices) and task manager (central monitoring station).
- Aggregates sensed data.
  Ex: 9791_WSN Ethernet gateway, 9792 gateway.
- The gateway devices are used as protocol converters, command data forwarders and it can be used as security manager and synchronizer in network

18. Why microcontroller is prepared than other controllers like microprocessor, DSP, FPGA and ASIC in WSN sensor nodes?

- Microcontroller is Suitable for all commercial and specific applications
- Low power consumption (i.e., Reduce the power consumption by going sleep states)
- Instructions sets are amenable to time critical signal processing

- Flexible to connect other devices
- It offers sufficient inbuilt memory's hence no need of external memory unit
- Easy of programming
- Economically Low cost

19. Explain the term 'Auto configuration' in WSN.

- WSN should configure most of its operation parameters automatically without any interruption of external configuration tools
- Nodes should be able to identify their own geographical location
- Nodes should be able to tolerate failure nodes
- Nodes should be able to integrate with new nodes in the network

20. Write down the categories of sensors.

Ability of the sensor device which receives and to measure the natural emission like vibrations, heat, light or other phenomena from its environment, is referred as **Passive sensors.**

A device which provides their own source of energy and observing information about targeted objects in their environment referred as ***Active Sensors*** (or) A sensor which emits its own radiations towards the directions of targeted objects to be investigated.

Sensors are roughly categorized into three categories

- **Passive Omnidirectional**
  Ex: light, thermometer, microphones, hygrometer
- **Passive Narrow Beam**
  Ex: Camera
- **Active Sensor**
  Ex: Radar, Sonar

21. Differentiate Single Hop and Multi Hop networks.

SINGLE HOP	MULTI HOP
Packet transmission - direct path to reach destination	Packet transmission - Multipath to reach destination
There is no intermediate nodes between source to destination	One or more than one nodes act as intermediate nodes
Transmission get failure if any one of node gets shutdown	Transmission may occurs even in any one of intermediate node get failure by finding alternate path
Radio coverage area is less	Radio coverage area is large
High power consumption	Low power consumption

Channel should be Line of sight for event execution	Event execution takes place even in poor channel quality

22. State the differences between ad-hoc and sensor network.

Adhoc networks	Wireless Sensor networks
The medium used in wireless adhoc network is radio waves	The medium used in wireless sensor network are radio waves, infrared, optical media.
Application independent based network	Application dependent based network
Point to point traffic pattern	Traffic pattern is any to any, one to many, many to few.
Wireless router is used as inter connecting device	Application level gateway is used as an inter-connecting devices
Have Global id	Does not have global id
Address centric	Data centric
Topology based	Not topology based
Supports common services	Supports specific applications.

23. Define figure of merit in WSN transmission control.

- Figure of merit or Noise figure of an element is defined as the ratio of the signal to noise ratio at the input of the element to the signal to noise ratio at the output of element.

$$NF = SNR_I \ / \ SNR_O$$
$$NF\ dB = SNR_I\ dB - SNR_O\ dB$$

24. List two even driven application of sensor network.

- Forest fire detection
- Precession agriculture farming applications

25. Write the goal of sensor networks.

- Reliable event detection
- Finding accurate geographic location where event is detected
- Performing specific task without delay
- Distributive and collaborative organizations
- Auto configurations during different environment conditions.

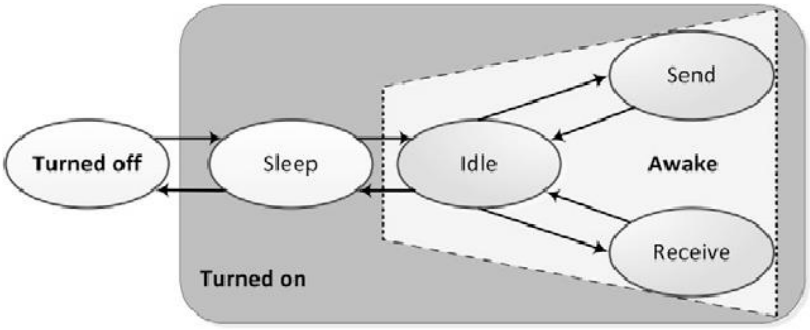
26. List out the various modes of a sensor node.

- ***Transmit mode***: Transmitting data
- ***Receive mode***: Receiving data
- ***Idle mode***: - Ready to receive, but not doing so

  - Some functions in hardware can be switched off

  - Reducing energy consumption a little

- ***Sleep mode***: -Significant parts of the transceiver nodes in network are switched off for reducing energy consumption much more



UNIT-2 -PART-B AND PART-C QUESTIONS

1. Summarize the challenges and the required mechanisms of a wireless sensor network.
2. What are the applications of wireless sensor networks and explain any two with an example each.
3. Explain how the sensor networks are deployed for Military and SAR application.
4. Sketch the RF front end of a transceiver and outline the behavior of operational states.
5. Discuss about the transceiver tasks and characteristics in a sensor node in a wireless sensor network.
6. Describe the enabling technologies and characteristic requirements of the wireless sensor networks.
7. Explain the transceiver characteristics and structure used in the sensor node.
8. Analyze how energy scavenging is realized in wireless sensor network.
9. Distinguish sensor networks from the mobile ad hoc network.
10. Write the detailed notes on energy consumption during the transmission and reception of a signal in WSN with the supporting equations.

11. Derive the expression for energy consumption in a sensor node with an appropriate diagram.
12. Draw the sensor network architecture and describe the components in detail.
13. Categorize the sensor network scenario with diagrams and also explain how mobility can appear in WSN?
14. Explain how optimization goals and figure of merits achieved in WSN with list of factors used to optimize the wireless sensor network.
15. Explain Single node architecture and Hardware components of WSN in detail.

UNIT III

WSN NETWORKING CONCEPTS AND PROTOCOLS

MAC Protocols for Wireless Sensor Networks, Low Duty Cycle Protocols and Wakeup Concepts - S-MAC, The Mediation Device Protocol, Contention based protocols - PAMAS, Schedule based protocols – LEACH, IEEE 802.15.4 MAC protocol, Routing Protocols Energy Efficient Routing, Challenges and Issues in Transport layer protocol.

PART A

1. What is MAC protocol for WSN?

The MAC layer is responsible for the establishment of a reliable and efficient communication link between WSN nodes and is responsible for energy waste. This technique enables dividing collisions from weak signals and takes appropriate decisions to reduce energy consumption.

2. What is meant by path loss and attenuation?

Wireless waveforms are propagating through free space and it is subjected to a distance dependent loss of power called path loss and different kinds of path loss called attenuation

3. Define interference.

Interference refers to the presence of any unwanted signals from external resources which mask a signal. Interference has three types

1. Multiple access interference
2. Co-channel interference
3. Adjacent channel interference

4. Write down the types of synchronization in WSN.

1. Carrier synchronization
2. Bits/Symbol synchronization
3. Frame Synchronization

5. Write the importance responsibilities of data link layer.

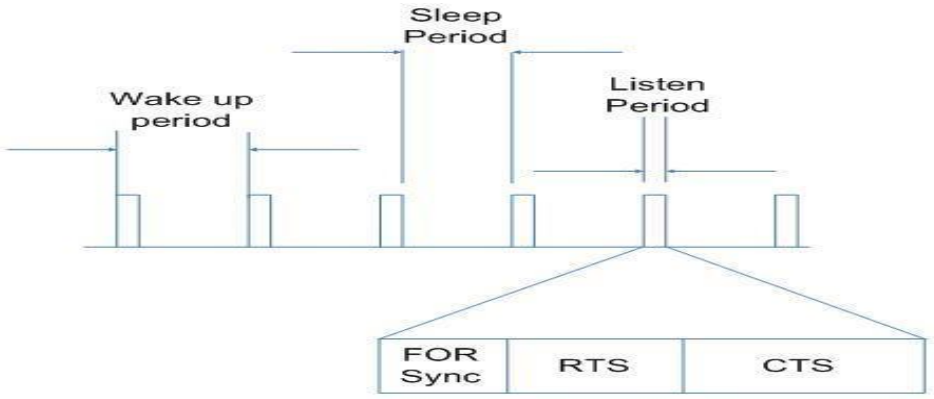
1. Error control
2. Flow control

Error control is used to ensure correctness of transmission and to take appropriate actions in case of transmission errors.

Flow control regulates the rate of transmission to protect a slow receiver from being overwhelmed with data.

6. What is S-MAC?

This protocol tries to reduce energy consumption due to overhearing, idle listening and collision. In this protocol also every node has two states, sleep state and active state. SMAC adopts a periodic wake up scheme. SMAC tries to synchronize the listen periods of neighboring nodes. The listen period of a node is divided into three phases as shown below. The listen period is the time, during which a node is awake rest of the time node is sleeping. The listen and sleep periods in the S-MAC are fixed intervals.



7. Define routing protocol

The transmission of packets from source to destination will be taken by router. Then the protocols used in the routing mechanisms are known as routing.

Types

1. Energy efficient routing
2. Geographic routing

8. Write down the names of address types used in the sensor networks

1. Unique node identifier
2. MAC address
3. Network address
4. Network identifiers
5. Resource identifiers
6. Address management tasks
7. Address allocation
8. Address representation

9. Write the usage of wakeup radio concepts

Wakeup radio concept used to avoid idle state by a simple and powerful receiver that can trigger a main receiver if necessary. Proposed wake up MAC protocol assumes the presence of several parallel data channels separated using FDMA or CDMA schemes.

10. Define frequency band

The frequency allocation is based on frequency band, for communication purposes always a finite portion of electromagnetic spectrum provide a single frequency capacity called frequency band.

11. Define antenna efficiency

An important parameter in a transmission system is the antenna efficiency which is defined as the ratio of the radiated power to the total input power to the antenna and remaining power to the antenna and remaining power is dissipated as heat.

12. Define symbol rate.

The symbol rate is the inverse of the symbol duration for binary modulation. It is also called bit rate.

13. Define demodulation

Modulation is carried out at the transmitter side. The receiver waves to recover the transmitted symbols from a received waveform. The mapping from a received waveform the symbols are called demodulation.

14. How many classes are there in the MAC protocols?

MAC protocols are having three kinds of classes

1. Fixed assignment protocols-TDMA, FDMA, CDMA and SDMA
2. Demands assignment protocols-HIPERLAN12
3. Random access protocol-ALOHA protocol

15. Define low duty cycle

Low duty cycle protocols try to avoid spending much time in the idle state to reduce the communication activities of a sensor node is a minimum level.

16. How many states in nodes?

Each node having four states

1. Transmitting state
2. Receiving state
3. Idling state
4. Sleeping state

17. What are the major problems in wireless transmission?

1. Bit error rate
2. Frequencies
3. Depending on the modulation schemes
4. Thermal noise
5. Time variable
6. Path loss

UNIT-3 -PART-B AND PART-C QUESTIONS

1. Explain MAC protocol for Wireless sensor network with neat diagrams.
2. Explain S-MAC protocol for Wireless sensor network with neat diagrams.
3. Explain Mediation Device protocol for Wireless sensor network with neat diagrams.
4. Explain Contention Based protocol for Wireless sensor network with neat diagrams.
5. Explain Schedule Based protocols for WSN.

6. Explain IEEE 802.14 MAC protocol with neat diagram.
7. Explain Energy Efficient Routing Protocols for wireless sensor networks.
8. Explain the Challenges and Issues in Transport layer protocol.

UNIT IV

SENSOR NETWORK SECURITY

Network Security Requirements, Issues and Challenges in Security Provisioning, Network Security Attacks, Layer wise attacks in wireless sensor networks, possible solutions for jamming, tampering, black hole attack, flooding attack. Key Distribution and Management, Secure Routing – SPINS, reliability requirements in sensor networks

PART-A

1. **Define Confidentiality?**

   The data sent by the sender (source node) must be comprehensible only to the intended receiver (destination node). Though an intruder might get hold of the data being sent, he/she must not be able to derive any useful information out of the data. One of the popular techniques used for ensuring confidentiality is data encryption.

2. **Define Integrity ?**

   The data sent by the source node should reach the destination node as it was sent: unaltered. In other words, it should not be possible for any malicious node in the network to tamper with the data during transmission.

3. **Define Availability?**

   The network should remain operational all the time. It must be robust enough to tolerate link failures and also be capable of surviving various attacks mounted on it. It should be able to provide the guaranteed services whenever an authorized user requires them.

4. **Define Non-repudiation?**

   Non-repudiation is a mechanism to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Digital signatures, which function as unique identifiers for each user, much like a written signature, are used commonly for this purpose.

5. **Define Shared broadcast radio channel?**

Unlike in wired networks where a separate dedicated transmission line can be provided between a pair of end users, the radio channel used for communication in ad hoc wireless networks is broadcast in nature and is shared by all nodes in the network. Data transmitted by a node is received by all nodes within its direct transmission range. So a malicious node could easily obtain data being transmitted in the network. This problem can be minimized to a certain extent by using directional antennas.

6. **Define Insecure operational environment?**

The operating environments where ad hoc wireless networks are used may not always be secure. One important application of such networks is in battlefields. In such applications, nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.

7. **Define Lack of central authority?**

In wired networks and infrastructure-based wireless networks, it would be possible to monitor the traffic on the network through certain important central points (such as routers, base stations, and access points) and implement security mechanisms at such points. Since ad hoc wireless networks do not have any such central points, these mechanisms cannot be applied in ad hoc wireless networks.

8. **Define Lack of association ?**

Since these networks are dynamic in nature, a node can join or leave the network at any point of the time. If no proper authentication mechanism is used for associating nodes with a network, an intruder would be able to join into the network quite easily and carry out his/her attacks.

9. **Define Limited resource availability ?**

Resources such as bandwidth, battery power, and computational power (to a certain extent) are scarce in ad hoc wireless networks. Hence, it is difficult to implement complex cryptography-based security mechanisms in such networks.

10. **Define Physical vulnerability ?**

Nodes in these networks are usually compact and hand-held in nature. They could get damaged easily and are also vulnerable to theft.

11. What are the types of Network Security Attacks?

Attacks on ad hoc wireless networks can be classified into two broad categories, namely, passive and active attacks.

12. Define Passive attack?

A passive attack does not disrupt the operation of the network; the adversary snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an adversary is also able to interpret the data gathered through snooping.

13. Define active attack?

An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network.

14. What are the types of active attack?

Active attacks can be classified further into two categories, namely,

External attack and internal attacks.

15. Define External attacks ?

External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls.

16. Define Internal attacks ?

Internal attacks are from compromised nodes that are actually part of the network. Since the adversaries are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks.

17. Define firewall ?

A firewall is used to separate a local network from the outside world. It is software which works closely with a router program and filters all packets entering the network to determine whether or not to forward those packets toward their intended destinations.

18. Define Wormhole attack?

In this attack, an attacker receives packets at one location in the network and tunnels them (possibly selectively) to another location in the network, where the packets are resent into the network.

19. Define Black hole attack?

In this attack, a malicious node falsely advertises good paths (e.g., shortest path or most stable path) to the destination node during the path-finding process (in on-demand routing protocols) or in the route update messages.

20. Define Byzantine attack ?

Here, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, routing packets on non-optimal paths, and selectively dropping packets.

21. Define Information disclosure?

A compromised node may leak confidential or important information to unauthorized nodes in the network. Such information may include information regarding the network topology, geographic location of nodes, or optimal routes to authorized nodes in the network.

22. Define Routing attacks?

There are several types attacks mounted on the routing protocol which are aimed at disrupting the operation of the network.

23. Define Routing table overflow?

In this type of attack, an adversary node advertises routes to non-existent nodes, to the authorized nodes present in the network.

24. Define Routing table poisoning?

Here, the compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes.

25. Define Packet replication?

In this attack, an adversary node replicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes and also causes unnecessary confusion in the routing process.

26. Define Session hijacking?

Here, an adversary takes control over a session between two nodes. Since most authentication processes are carried out only at the start of a session, once the session between two nodes gets established, the adversary node masquerades as one of the end nodes of the session and hijacks the session.

27. Define Repudiation?

In simple terms, repudiation refers to the denial or attempted denial by a node involved in a communication of having participated in all or part of the communication.

UNIT-4 -PART-B AND PART-C QUESTIONS

1. Write short notes on Network Security Requirements, Issues and Challenges in Security Provisioning.

2. Explain Network Security Attacks, Layer wise attacks in wireless sensor networks.

3. What are the possible solutions for jamming, tampering, black hole attack, flooding attack?

4. Explain Key Distribution and Management in sensor network security.

5. Explain Secure Routing in SPINS and Reliability requirements in sensor networks.

UNIT V

SENSOR NETWORK PLATFORMS AND TOOLS

Sensor Node Hardware – Berkeley Motes, Programming Challenges, Node-level software platforms – TinyOS, nesC, CONTIKIOS, Node-level Simulators – NS2 and its extension to sensor networks, COOJA, TOSSIM, Programming beyond individual nodes – State centric programming.

PART A

1. **Write sensor nodes Hardware**
   - (i) Augmented general purpose computers-Embedded PC's
   - (ii) Dedicated embedded sensor nodes-Berkley mote
   - (iii) System-on-chip nodes –PASTA
2. **Write down the types of programming for sensor networks?**

   Two types of programming method is available for sensor networks

   (i) These which carried out by end users
   (ii) Those which performed by application developers
3. **What is meant by Moto?**

   A Sensor node on a network is called as mote. This node capable of performing some processing, gathering information and communicate with other is connected nodes in network.

4. **Write the types of hardware in sensor node.**

   There are two types of hardware granted for sensor nodes

   - (i) Augmented general purpose computers
   - (ii) Dedicated embedded sensor nodes
   - (iii) System-on-chip
5. **Give some examples for augmented general purpose computers.**
   - (i) Personal digital assistants
   - (ii) Embedded PC's
   - (iii) Linux
   - (iv) Real time operating system
   - (v) Win CE

6. **Define Berkeley Motes?**

A Berkeley mote is a wireless sensor module manufactured by Berkeley. The Berkeley motes are a family of embedded sensor nodes. This node composed of sensing capabilities communication radio, computation unit and power source.

7. **What are the things to be followed in traditional programming in sensor network?**

To apply the traditional programming in sensor networks the following things to be followed

(i) Message passing
(ii) Event synchronization
(iii) Interrupt handling
(iv) Sensor reading

8. **What are the services provided by operating system?**
    1. File management
    2. Memory location
    3. Task scheduling
    4. Peripheral device drivers
    5. Networking
9. **Say some example programming for node level.**

There are two examples available for node level programming such as

1. Tiny OS

2. Tiny GALS

10. **Define tasks in TinyOS.**

Task are providing source for concurrency. Tasks are created by components to a task scheduler. The default implementation of the tinyOS scheduler maintains a task queue and task queue maintain information according the task order posted.

11. **Define nesC.**

The nesC is an imperative language it an extension of C to support and reflect the design of TinyOS V1.0 and above version. It provides a set of language constructs and restrictions to implement Tiny OS components and application.

12. Write the types of interface in nesC components interface.

There are two types of component interface in nesC

1. Provide interface
2. Uses interface

13. Write the types of component in nesC component implementation.

There are two types of component in nesC component implementation

1. Modules
2. Configurations

Modules are implemented by application code and configurations are implemented by connecting interfaces existing components.

14. How many codes in nesC?

The nesC code can be classified into two types.

1. Asynchronous code(AC)
2. Synchronous Code(SC)

15. Define dataflow style language.

Dataflow style languages are more reliable for expressing computation on interrelated data units by specifying data dependencies among those data. Tiny GALS is the example for this language.

16. What is meant by actor?

In a dataflow style language processing units called actors. Actors have ports to receive and produce data.

17. How applications built in Tiny GALS.

An application in Tiny GALS is built in two steps

Step 1: Constructing asynchronous actors from synchronous components

Step2: Constructing an application by connecting the asynchronous components through FIFO queues.

18. State advantages of Tiny GALS applications

1. It has highly structured architecture
2. Efficient scheduling
3. It has event handling code

19. Write the types of node level simulator components.

1. Sensor node model
2. Communication model
3. Physical environmental model
4. Statistics and visualization

20. Write the types of execution model in simulation.

Depending on how the time is advanced in the simulation, there are two types of execution models.

1. Cycle driven simulation
2. Discrete event simulation

21. What is meant by causal component?

Causal component means the output event is computed from an input event. The time stamps of the output event always the reference of input event at present only.

22. What is meant by non-causal component?

Non-causal component means the output event is computed from an input event. The time stamp of the output event contains past and present value of input event.

23. State some functions of processing algorithm.

1. Kalman filtering
2. Bayesian estimation
3. System identification
4. Feedback control laws
5. Finite state automate

24. How many groups available in state centric programming?

1. Collaboration groups
2. Geographically constrained group
3. N-hop neighborhood group
4. Publish/Subscribe
5. Acquaintance group

UNIT-5 -PART-B AND PART-C QUESTIONS

1. Write detailed notes on any one node-level software platform.
2. Discuss on the sensor network programming challenges.
3. Explain the system architecture of Berkeley motes with neat diagram
4. Write short notes on TinyOS and contikios?compare both.
5. Explain the concept of state centric programming in target tracking application carried out using WSN?
6. Discuss about nesC programming and write program for field monitor application?
7. Discuss about NS2 simulator for WSN.
8. Write short note on the following:
   a) TOSSIM
   b) COOJA