FIRST TERM EXAMINATION [FEB. 2017]
EIGHTH SEMESTER [B.TECH.]
ADHOC AND SENSOR NETWORK
(ETEC–406)

Time : 1½ hrs. **M.M. : 30**

Note: *Q.1. is Compulsory. Attempt any two more Questions from the rest.*

Q.1. (a) Why is power management important for AD HOC wireless networks? **(2.5)**

Ans. The power constraints in sensor networks are much more stringent than those in ad hoc wireless networks. This is mainly because the sensor nodes are expected to operate in harsh environmental or geographical conditions, with minimum or no human supervision and maintenance. In certain case, the recharging of the energy source is impossible. Running such a network, with nodes powered by a battery source with limited energy, demands very efficient protocol at network, data link, and physical layer.

Q.1. (b) What are the various issues in designing MAC protocol for AD HOC networks? **(2.5)**

Ans. The main issues in designing MAC protocol for ad hoc wireless network are:

Bandwidth efficiency Bandwidth must be utilized in efficient manner

Minimal Control overhead BW = ratio of BW used for actual data transmission to the total available BW

Quality of service support

Essential for supporting time-critical traffic sessions

They have resource reservation mechanism that takes into considerations the nature of wireless channel and the mobility of nodes.

Synchronization

MAC protocol must consider synchronization between nodes in the network

Synchronization is very important for BW (time slot) reservation by nodes Exchange of control packets may be required for achieving time synchronization among nodes

Hidden and exposed terminal problems

The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender but are within the transmission range of the receiver. Collision occurs when both nodes transmit packets at the same time without knowing about the transmission of each other.

Q.1. (c) List the design issues in ADHOC Network. **(2.5)**

Ans. The major issues that affect the design, deployment, and performance of an ad hoc wireless network system are :

- Medium Access Scheme.
- Transport Layer Protocol.
- Routing.
- Multicasting.
- Energy Management.
- Self-Organization.
- Security.
- Addressing & Service discovery.
- Deployment considerations.

- Scalability.
- Pricing Scheme.
- Quality of Service Provision

Q.1. (d) What do you mean by contention based protocols? **(2.5)**

Ans. These protocols follow a contention-based channel access policy. A node does not make any resource reservation a priori. Whenever it receives a packet to be transmitted, it contends with its neighbour nodes for access to the shared channel. Contention-based protocols cannot provide QoS guarantees to sessions since nodes are not guaranteed regular access to the channel. Random access protocols can be further divided into two types:

- **Sender-initiated protocols:** Packet transmissions are initiated by the sender node.
- **Receiver-initiated protocols:** The receiver node initiates the contention resolution protocol.

Sender-initiated protocols can be further divided into two types:

- **Single-channel sender-initiated protocols**: In these protocols, the total available bandwidth is used as it is, without being divided. A node that wins the contention to the channel can make use of the entire bandwidth.
- **Multichannel sender-initiated protocols:** In multi channel protocols, the available bandwidth is divided into multiple channels. This enables several nodes to simultaneously transmit data, each using a separate channel.

Q.2. (a) Compare MACA with MACAW protocol. **(5**

Ans. MACAW (MACA for Wireless) is a revision of MACA.

- The sender senses the carrier to see and transmits a RTS (Request To Send) fram if no nearby station transmits a RTS.
- The receiver replies with a CTS (Clear To Send) frame.
- The MACAW protocol uses one more control packet called the request-for-reques to-send (RRTS)

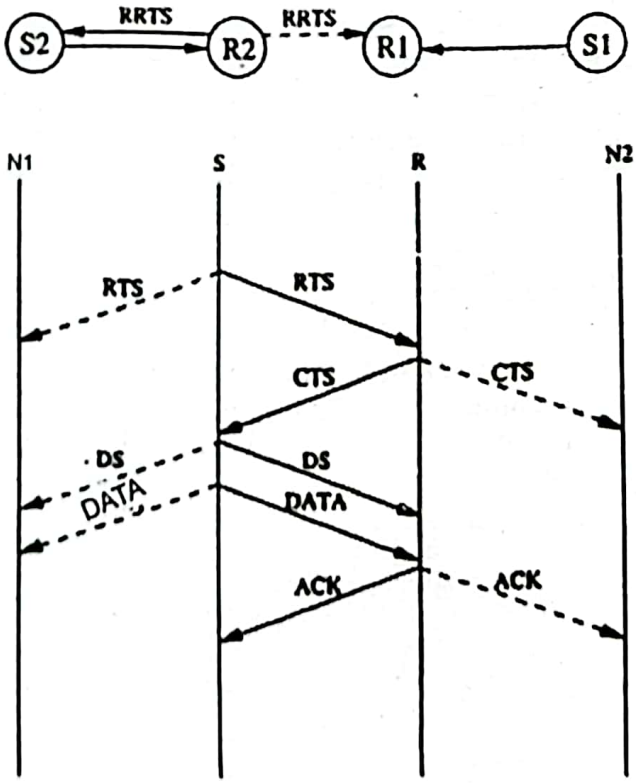


Fig. Packet Exchange in MACAW

Neighbours

- see CTS, then keep quiet.
- see RTS but not CTS, then keep quiet until the CTS is back to the sender.

The receiver sends an ACK when receiving an frame.

- Neighbours keep silent until see ACK.

Collisions

- There is no collision detection

The senders know collision when they don't receive CTS.

- They each wait for the exponential back-off time.

Q.2. (*b*)Compare Ad HOC networks with Cellular network. **[5]**

Ans.

Cellular Netowrks	Ad HOC Wireless Networks
(a) Fixed infrastructure-based	(a) Infrastructure-less
(b) Single-hop wireless links	(b) Multi-hop wireless links
(c) Guaranteed bandwidth (designed for voice traffic)	(c) Shared radio channel (more suitable for best-effort data traffic)
(d) Centralized routing	(d) Distributed routing
(e) Circuit-switched (evolveing toward packet switching)	(e) Packet-switched (evolving toward emulation of circuit switching)
(f) Seamless connectivity (low call drops during handoffs)	(f) Frequent path breaks due to mobility
(g) High cost and time of deployment	(g) Quick and cost-effective deployment
(h) Reuse of frequency spectrum through geographical channel reuse	(h) Dynamic frequency reuse based on carrier sense mechnism
(i) Easier to achieve time synchronization	(i) Time synchronization is difficult and consumes bandwidth
(j) Easier to employ bandwidth reservation	(j) Bandwidth reservation requires complex medium access control protocols
(k) Application domains include mainly civilian and commerical sectors	(k) Application domains include battle-fields, emergency search and resue operations, and collaborative computing.
(l) High cost of network maintenance (backup power source, staffing etc.)	(l) Self-organization and maintenance properties are built into the network
(m) Mobile losts are of relatively low complexity	(m) Mobile hosts require more intelligence (should have a transceiver as well as routing/switching capability)
(n) Major goals of routing and call admission are to maximize the call acceptance ratio and minimize the call drop ratio	(n) Main aim of routing is to find paths with minimum overhead and also quick reconfiguration of broken paths
(o) Widely deployed and currently in the third generation of evolution	(o) Several issues are to be addressed for successful commercial deployment even though widespread use exists in defense

Q.3. Classify and explain in details various types of routing protocol for ADHOC wireless networks. **[10]**

Ans.

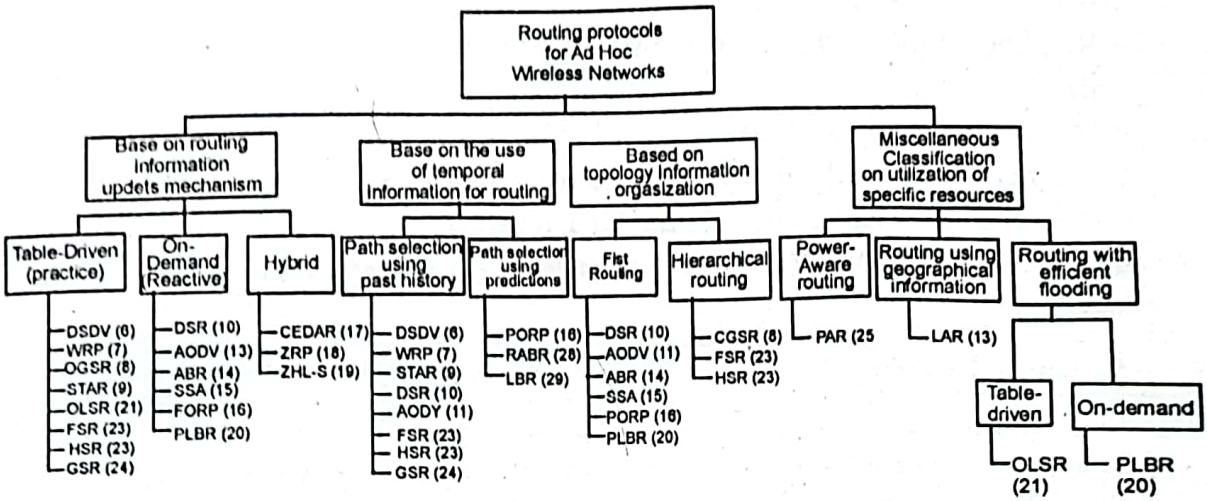


Fig. Classification of routing protocols

The routing protocol for ad hoc wireless networks can be broadly classified into 4 categories based on

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

(a) Based on the routing information update mechanism:

Ad hoc wireless network routing protocols can be classified into 3 major categories based on the routing information update mechanism. They are:

Proactive or table-driven routing protocols :

- Every node maintains the network topology information in the form of routing tables by periodically exchanging routing information.
- Routing information is generally flooded in the whole network.
- Whenever a node requires a path to a destination, it runs an appropriate path-finding algorithm on the topology information it maintains.

Reactive or on-demand routing protocols:

- Do not maintain the network topology information.
- Obtain the necessary path when it is required, by using a connection establishment process.

Hybrid routing protocols:

- Combine the best features of the above two categories.
- Nodes within a certain distance from the node concerned, or within a particular geographical region, are said to be within the routing zone of the given node.
- For routing within this zone, a table-driven approach is used.

• For nodes that are located beyond this zone, an on-demand approach is used.

(b) Based on the use of temporal information for routing

The protocols that fall under this category can be further classified into two types

Routing protocols using past temporal information:

• Use information about the past status of the links or the status of links at the time of routing to make routing decisions.

Routing protocols that use future temporal information:

• Use information about the about the expected future status of the wireless links to make approximate routing decisions.

• Apart from the lifetime of wireless links, the future status information also includes information regarding the lifetime of the node, prediction of location, and prediction of link availability.

(c) Based on the routing topology

Ad hoc wireless networks, due to their relatively smaller number of nodes, can make use of either a flat topology or a hierarchical topology for routing.

Flat topology routing protocols:

• Make use of a flat addressing scheme similar to the one used in IEEE 802.3 LANs.

• It assumes the presence of a globally unique addressing mechanism for nodes in an ad hoc wireless network.

• Hierarchical topology routing protocols:

• Make use of a logical hierarchy in the network and an associated addressing scheme.

• The hierarchy could be based on geographical information or it could be based on hop distance.

• Based on the utilization of specific resources

• Power-aware routing:

• Aims at minimizing the consumption of a very important resource in the ad hoc wireless networks: the battery power.

• The routing decisions are based on minimizing the power consumption either logically or globally in the network.

Q.4. (a) Explain hidden and exposed terminal problem. **[5]**

Ans. The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender but are within the transmission range of the receiver. Collision occurs when both nodes transmit packets at the same time without knowing about the transmission of each other

• S1 and S2 are hidden from each other & they transmit simultaneously to R1 which leads to collision

• The exposed terminal problem refers to the inability of a node, which is blocked due to transmission by a nearby transmitting node, to transmit to another node

• If S1 is already transmitting to R1, then S3 cannot interfere with on-going transmission & it cannot transmit to R2.

• The hidden & exposed terminal problems reduce the throughput of a network when traffic load is high

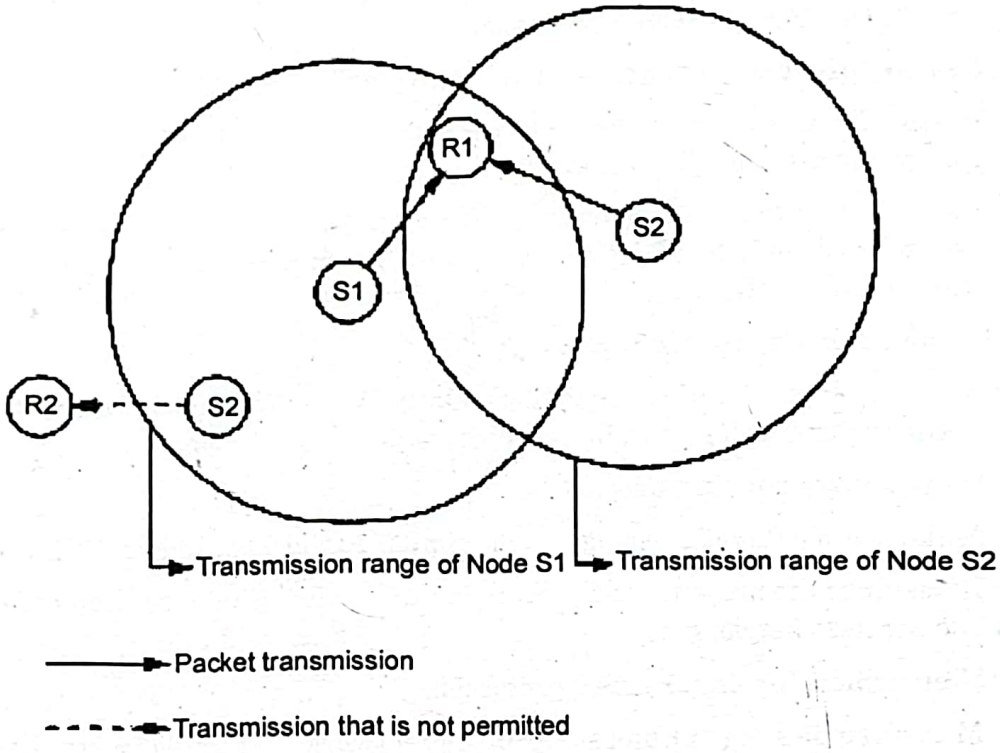


Fig. Hidden and exposed terminal problems.

Q.4. (*b*) Why TCP protocols used in wired network is not suitable for wireless network? [5]

Ans. The major reasons behind throughput degradation that TCP faces when used in ad hoc wireless networks are the following:

• **Misinterpretation of packet loss:** Traditional TCP was designed for wired networks where the packet loss is mainly attributed to network congestion. Network congestion is detected by the sender's packet RTO period. Once a packet loss is detected, the sender node assumes congestion in the network and invokes a congestion control algorithm.

• **Frequent path breaks:** Ad hoc wireless networks experience dynamic changes in network topology because of the unrestricted mobility of the nodes in the network. The topology changes lead to frequent changes in the connectivity of wireless links and hence the route to a particular destination may need to be recomputed very often.

• **Effect of path length:** It is found that the TCP throughput degrades rapidly with an increase in path length in string (linear chain) topology ad hoc wireless networks.

• **Misinterpretation of congestion window:** TCP considers the congestion window as a measure of the rate of transmission that is acceptable to the network and

the receiver. In ad hoc wireless networks, the congestion control mechanism is invoked when the network gets partitioned or when a path break occurs

- **Asymmetric link behavior:** The radio channel used in ad hoc wireless networks has different properties such as location-dependent contention, environmental effects on propagation, and directional properties leading to asymmetric links. The directional links can result in delivery of a packet to a node, but failure in the delivery of the acknowledgment back to the sender.

END TERM EXAMINATION [MAY-JUNE 2017]
EIGHTH SEMESTER [B.TECH.]
ADHOC AND SENSOR NETWORK
(ETEC–406)

Time : 3 hrs. **M.M. : 75**

Note: *Q.1. is Compulsory. Attempt any five more Questions from the rest.*

Q.1. (a)What is an ad-hoc network? Why ad hoc network are needed? Discuss. **(4)**

Ans. Ad hoc wireless networks are defined as the category of wireless networks that utilize multi-hop radio relaying and are capable of operating without the support of any fixed infrastructure (hence they are also called infrastructure less networks). The absence of any central coordinator or base station makes the routing a complex one compared to cellular networks.

Advantages of Ad Hoc Network: The rapid development in ad hoc technology is widely used in portable computing such as laptop, mobile phone used to access the web services, telephone calls when the user are in travelling. Development of self-organizing network decrease the communication cost. The growth of 4G technology enhances anytime, anywhere, anyhow communication in ad hoc network. Ad hoc network is simple to design and install. The advantages of an ad hoc network include: Separation from central network administration.

- Self-configuring nodes are also routers.
- Self-healing through continuous re-configuration.
- Scalability incorporates the addition of more nodes.
- Mobility allows ad hoc networks created on the fly in any situation where there are multiple wireless devices.
- Flexible ad hoc can be temporarily setup at anytime, in any place.
- Lower getting-started costs due to decentralized administration.
- The nodes in ad hoc network need not rely on any hardware and software. So, i can be connected and communicated quickly.

Q.1. (b) List the applications of ad-hoc networks. List the benefits whe deployment of ad-hoc wireless networks compared to wired network. **(4**

Ans. Ad hoc wireless networks, due to their quick and economically less demandin deployment, find applications in several areas. Some of these include: militar applications, collaborative and distributed computing, emergency operations, wireles mesh networks, wireless sensor networks, and hybrid wireless network architectures

Military Applications: Ad hoc wireless networks can be very useful in establishin communication among a group of Soldiers for tactical operations. Setting up a fixe infrastructure for communication among a group of soldiers in enemy territories or i inhospitable terrains may not be possible. In such environments, ad hoc wireles

networks provide the required communication mechanism quickly. Another application in this area can be the coordination of military objects moving at high speeds such as fleets of airplanes or warships.

Collaborative and Distributed Computing; Another domain in which the ad hoc wireless networks find applications is collaborative computing. The requirement of a temporary communication infrastructure for quick communication with minimal configuration among a group of people in a conference or gathering necessitates the formation of an ad hoc wireless network

Emergency Operations: Ad hoc wireless networks are very useful in emergency operations such as search and rescue, crowd control, and commando operations. The major factors that favor ad hoc wireless networks for such tasks is self-configuration of the system with minimal overhead, independent of fixed or centralized infrastructure, the nature of the terrain of such applications, the freedom and flexibility of mobility, and the unavailability of conventional communication infrastructure.

Q.1. (c) What do you mean by contention based protocols? Explain. **(3)**

Ans. These protocols follow a contention-based channel access policy. A node does not make any resource reservation a priori. Whenever it receives a packet to be transmitted, it contends with its neighbor nodes for access to the shared channel. Contention-based protocols cannot provide QoS guarantees to sessions since nodes are not guaranteed regular access to the channel. Random access protocols can be further divided into two types:

- Sender-initiated protocols: Packet transmissions are initiated by the sender node.
- Receiver-initiated protocols: The receiver node initiates the contention resolution protocol.

Sender-initiated protocols can be further divided into two types:

- Single-channel sender-initiated protocols: In these protocols, the total available bandwidth is used as it is, without being divided. A node that wins the contention to the channel can make use of the entire bandwidth.
- Multichannel sender-initiated protocols: In multi channel protocols, the available bandwidth is divided into multiple channels. This enables several nodes to simultaneously transmit data, each using a separate channel. Some protocols dedicate a frequency channel exclusively for transmitting control information.

Q.1. (d) What are the responsibilities of routing protocol? Discuss the major challenges in designing routing protocols. **(5)**

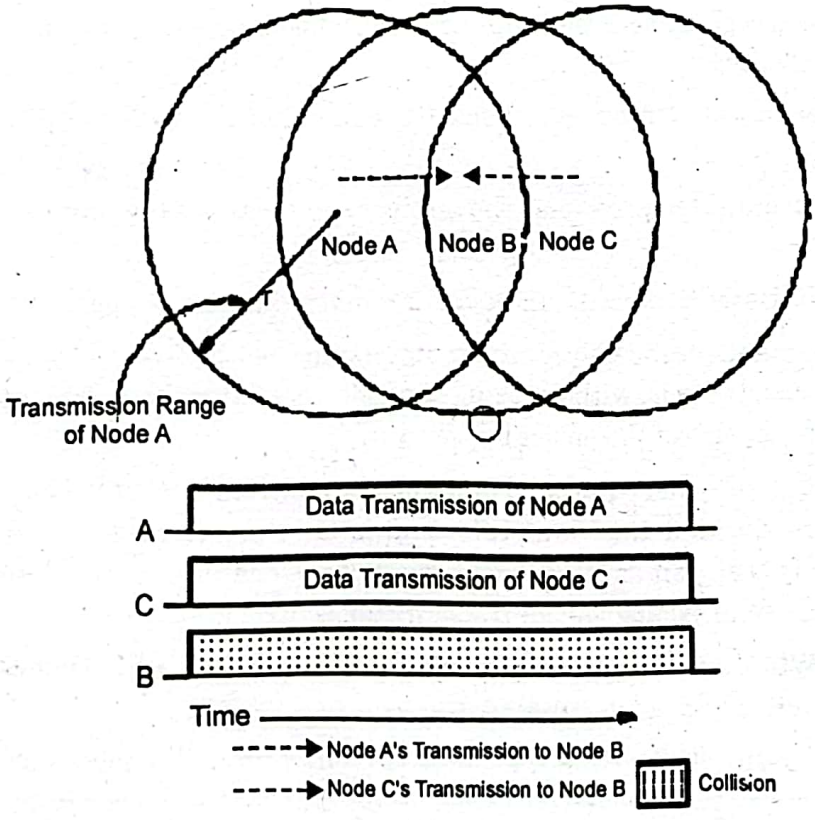
Routing protocols for wireless sensor networks are responsible for maintaining the routes in the network and have to ensure reliable multi-hop communication under these conditions. The major challenges that a routing protocol designed for ad hoc wireless networks faces are:

- **Mobility of nodes:** wired network routing protocols cannot be used in ad hoc wireless networks where the mobility of nodes results in frequently changing network topologies. Routing protocols for ad hoc wireless networks must be able to perform efficient and effective

- **Bandwidth Constrained:** wireless network, the radio band is limited, and hence the data rates it can offer are much less than what a wired network can offer. This requires that the routing protocols use the bandwidth optimally by keeping the overhead as low as possible.

- **Error-Prone Shared Broadcast Radio Channel:** The broadcast nature of the radio channel poses a unique challenge in ad hoc wireless networks. The wireless links have time-varying characteristics in terms of link capacity and link-error probability. This requires that the ad hoc wireless network routing protocol interacts with the MAC layer to find alternate routes through better-quality links

- **Hidden and Exposed Terminal Problems:** The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver. Collision occurs when both nodes transmit packets at the sometime without knowing about the transmission of each other. For example, consider Figure. Here, if both node A and node C transmit to node B at the same time, their packets collide at node B. This is due to the fact that both nodes A and C are hidden from each other, as they are not within the direct transmission range of each other and hence do not know about the presence of each other.



Q.1. (e) What is wireless sensor network? What are the components of WSN? (5)

Ans. Sensor networks are highly distributed networks of small, lightweight wireless nodes, deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or relative

humidity. Building sensors has been made possible by the recent advances in microelectromechanical systems (MEMS) technology. Sensor nodes are used in a variety of applications which require constant monitoring and detection of specific events. The military applications of sensor nodes include battlefield surveillance and monitoring, guidance systems of intelligent missiles, and detection of attack by weapons of mass destruction, such as chemical, biological, or nuclear. Sensors are also used in environmental applications such as forest fire and flood detection, and habitat exploration of animals. Sensors can be extremely useful in patient diagnosis and monitoring. Patients can wear small sensor devices that monitor their physiological data such as heart rate or blood pressure.

Components of WSN: Each node of the sensor network consists of three subsystems: the sensor subsystem which senses the environment, the processing subsystem which performs local computations on the sensed data, and the communication subsystem which is responsible for message exchange with neighboring sensor nodes. While individual sensors have limited sensing region, processing power, and energy, networking a large number of sensors gives rise to a robust, reliable, and accurate sensor network covering a wider region. The network is fault tolerant because many nodes are sensing the same events. Further, the nodes cooperate and collaborate on their data, which leads to accurate sensing of events in the environment. The two most important operations in a sensor network are data dissemination, that is, the propagation of data/ queries throughout the network, and data gathering, that is, the collection of observed data from the individual sensor nodes to a sink.

Q.1. (f) Why TCP protocols used in wired network is not suitable for wireless network? Compare the different TCP protocols over ad hoc networks. (4)

Ans. The major reasons behind throughput degradation that TCP faces when used n ad hoc wireless networks are the following:

- **Misinterpretation of packet loss:** Traditional TCP was designed for wired ietworks where the packet loss is mainly attributed to network congestion. Network ongestion is detected by the sender's packet RTO period. Once a packet loss is detected, he sender node assumes congestion in the network and invokes a congestion control lgorithm

- **Frequent path breaks:** Ad hoc wireless networks experience dynamic changes n network topology because of the unrestricted mobility of the nodes in the network. The topology changes lead to frequent changes in the connectivity of wireless links and ience the route to a particular destination may need to be recomputed very often.

- **Effect of path length:** It is found that the TCP throughput degrades rapidly vith an increase in path length in string (linear chain) topology ad hoc wireless networks

- **Misinterpretation of congestion window:** TCP considers the congestion window is a measure of the rate of transmission that is acceptable to the network and the eceiver. In ad hoc wireless networks, the congestion control mechanism is invoked vhen the network gets partitioned or when a path break occurs

- **Asymmetric link behavior:** The radio channel used in ad hoc wireless networks has different properties such as location-dependent contention, environmental effects

on propagation, and directional properties leading to asymmetric links. The directional links can result in delivery of a packet to a node, but failure in the delivery of the acknowledgment back to the sender.

UNIT–I

Q.2. (a) What are the characteristics and features of ad hoc networks? List the design goal of MAC protocol for ad hoc networks. (6)

Ans. Ad hoc networks are multi-hop network that use wireless communication for transmission without any fixed infrastructure. The networks are form and deform on-the-fly without the need for any system. Ad hoc structure does not require an access point, it is easy to setup, especially in a small or temporary network. Each node in the network forwards the packet without the need of central administration. In ad hoc network, node acts as a router to send and receive the data. An advantage of the system is robustness, flexibility and mobility. Ad hoc network are capable for analyzing radio propagation environment to optimize the performance. This typically requires that the network node have positioning capability as well as memory to recall geographical local condition. An ad hoc network typically refers to any set of network where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE802.11 wireless networks.

The design goal of MAC protocol for ad hoc networks.

The following are the important goals to be met while designing a medium access control (MAC) protocol for ad hoc wireless networks:

- The operation of the protocol should be distributed.
- The protocol should provide QoS support for real-time traffic.
- The access delay, which refers to the average delay experienced by any packet to get transmitted, must be kept low.
- The available bandwidth must be utilized efficiently.
- The protocol should ensure fair allocation (either equal allocation or weighted allocation) of bandwidth to nodes.
- Control overhead must be kept as low as possible.
- The protocol should minimize the effects of hidden and exposed terminal problems
- The protocol must be scalable to large networks.
- It should have power control mechanisms in order to efficiently manage energy consumption of the nodes.
- The protocol should have mechanisms for adaptive data rate control (adaptive rate control refers to the ability to control the rate of outgoing traffic from a node after taking into consideration such factors as load in the network and the status of neighbor nodes).
- It should try to use directional antennas which can provide advantages such as reduced interference, increased spectrum reuse, and reduced power consumption.

• Since synchronization among nodes is very important for bandwidth reservations, the protocol should provide time synchronization among nodes.

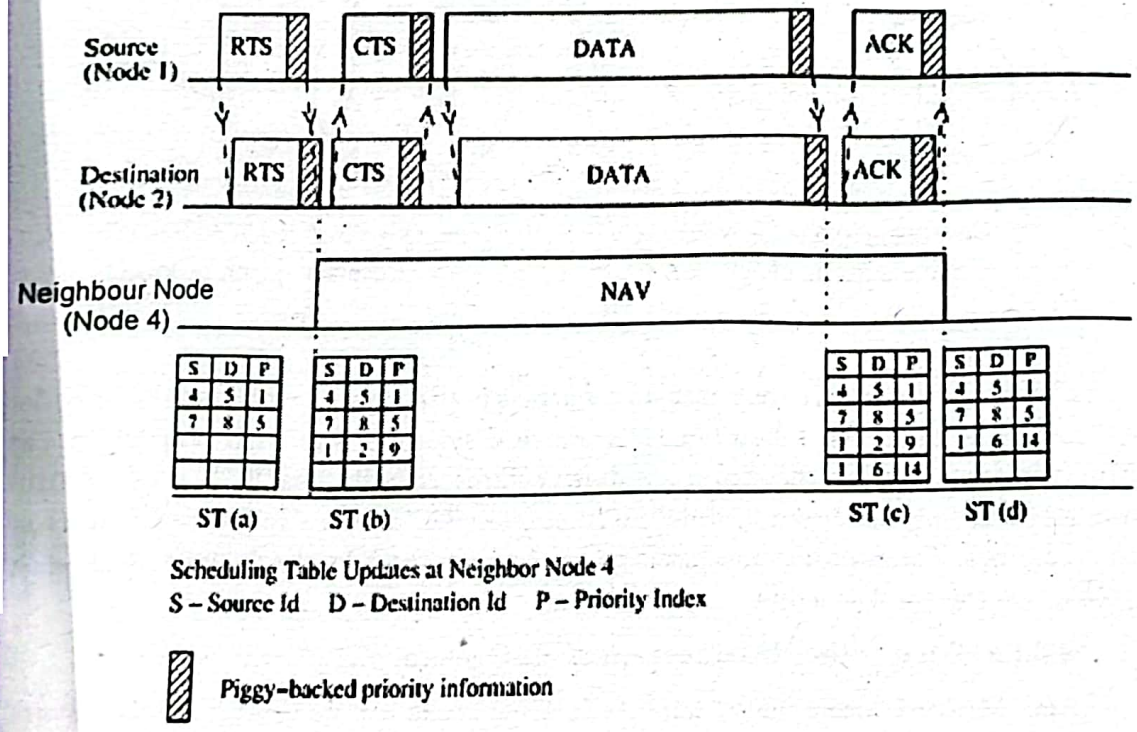
Q.2. (b) What do you mean by contention based protocols with scheduling mechanism? Discuss. **(6.5)**

Ans. Protocols that fall under category of contention based protocols with scheduling mechanism focus on packet scheduling at the nodes and transmission scheduling of the nodes. Scheduling decisions may take into consideration various factors such as delay targets of packets, laxities of packets, traffic load at nodes, and remaining battery power at nodes.

1. Distributed Priority Scheduling and Medium Access in Ad Hoc Networks

The first technique, called distributed priority scheduling (DPS), piggy-backs the priority tag of a node's current and head-of-line packets on the control and data packets. By retrieving information from such packets transmitted in its neighborhood, a node builds a scheduling table from which it determines its rank (information regarding its position as per the priority of the packet to be transmitted next)compared to other nodes in its neighborhood.

This rank is incorporated into the back-off calculation mechanism in order to provide an approximate schedule based on the ranks of the nodes. The second scheme, called multi-hop coordination, extends the DPS scheme to carry out scheduling over multi-hop paths. The downstream nodes in the path to the destination increase the relative priority of a packet in order to compensate for the excessive delays incurred by the packet at the upstream nodes.



Scheduling Table Updates at Neighbor Node 4
S – Source Id D – Destination Id P – Priority Index

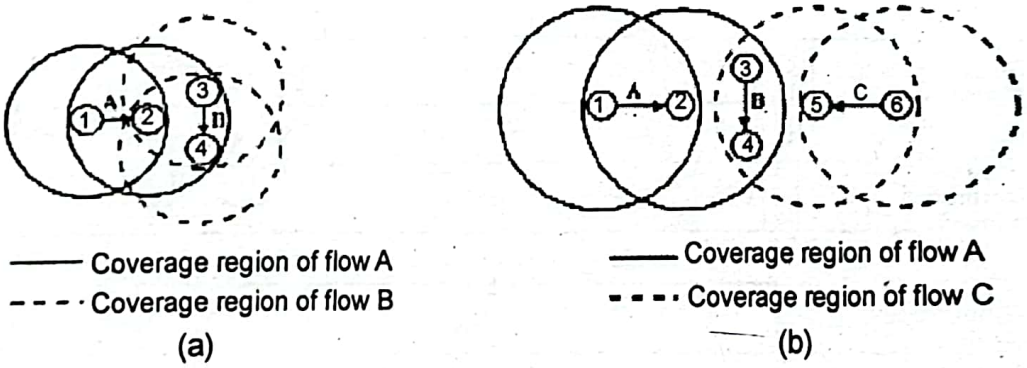
Piggy-backed priority information

Figure illustrates the piggy-backing and table update mechanism. Node 1 needs to transmit a DATA packet (with priority index value 9) to node 2. It first transmits an RTSpacket carrying piggy-backed information about this DATA packet. The initial state

of the STbf node 4 which is a neighbor of nodes 1 and 2 is shown in ST (a). Node 4, on hearing thirsts packet, retrieves the piggybacked priority information and makes a corresponding entry in its ST, as shown in ST (b). The destination node 2 responds by sending a CTS packet. The actual DATA packet is sent by the source node once it receives the CTS packet. This DATA packet carries piggy-backed priority information regarding the head-of-line packet at node 1. On hearing this DATA packet, neighbor node 4 makes a corresponding entry for the head-of-line packet of node 1, in its ST. ST (c) shows the new updated status of the ST at node 4. Finally, the receiver node sends an Backpacked to node 1. When this packet is heard by node 4, it removes the entry made for the corresponding DATA packet from its ST. The state of the scheduling table at the end of this data transfer session is depicted in ST (d).

2. Distributed Wireless Ordering Protocol

The distributed wireless ordering protocol (DWOP) consists of a media access scheme along with a scheduling mechanism. It is based on the distributed priority scheduling scheme. DWOP ensures that packets access the medium according to the order specified by an ideal reference scheduler such as first-in-first-out (FIFO), virtual clock, or earliest deadline first. In this discussion, FIFO is chosen as the reference scheduler. In FIFO, packet priority indices are set to the arrival times of packets. Similar to DPS, control packets are used in DWOP to piggyback priority information regarding head-of-line packets of nodes. As the targeted FIFO schedule would transmit packets in order of the arrival times, each node builds up a scheduling table (ST) ordered according to the overheard arrival times.



DWOP tries to ensure that packets get access to the channel according to the order defined by a reference scheduler. The above discussion was with respect to the FIFOscheduler. Though the actual schedule deviates from the ideal FIFO schedule due to information asymmetry and state information in STs, the receiver participation and the stale entry elimination mechanisms try to keep the actual schedule as close as possible to the ideal schedule.

Q.3.(*a*) What is the classification of MAC protocol? **(6)**

Ans. MAC protocols for ad hoc wireless networks can be classified into several categories based on various criteria such as initiation approach, time synchronization and reservation approaches. Ad hoc network MAC protocols can be classified into three basic types:

- Contention-based protocols

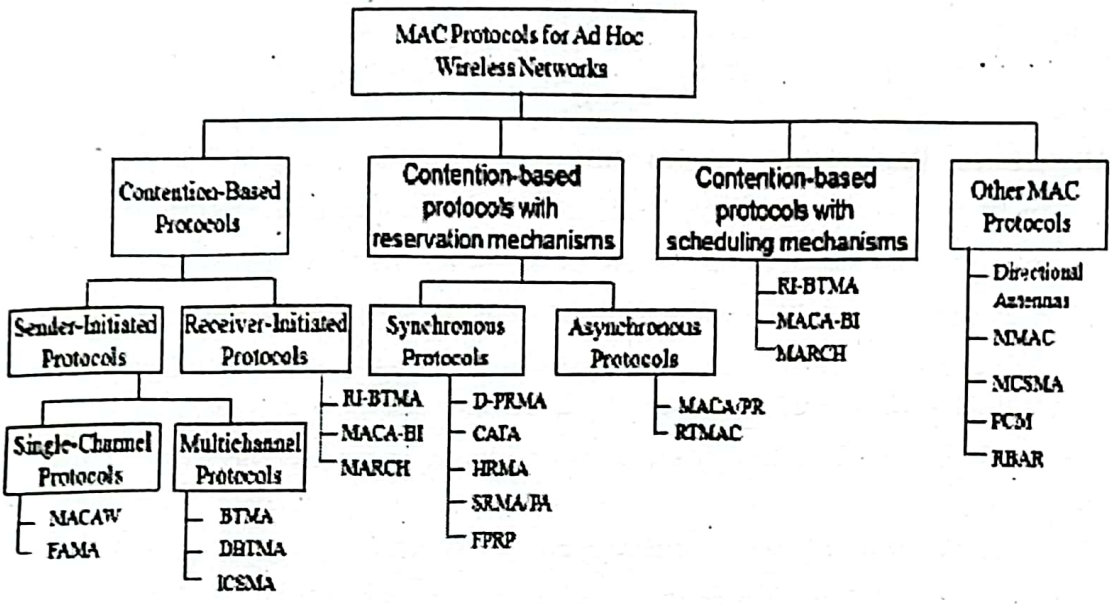


Fig. Classification of MAC

- Contention-based protocols with reservation mechanisms
- Contention-based protocols with scheduling mechanisms

Contention-based protocols

- Sender-initiated protocols: Packet transmissions are initiated by the sender node.
- Single-channel sender-initiated protocols: A node that wins the contention to the channel can make use of the entire bandwidth.
- Multichannel sender-initiated protocols: The available bandwidth is divided into multiple channels.
- Receiver-initiated protocols: The receiver node initiates the contention resolution protocol.

Contention-based protocols with reservation mechanisms

- Synchronous protocols: All nodes need to be synchronized. Global time synchronization is difficult to achieve.
- Asynchronous protocols: These protocols use relative time information for effecting reservations.

Contention-based protocols with scheduling mechanisms

- Node scheduling is done in a manner so that all nodes are treated fairly and no node is starved of bandwidth.
- Scheduling-based schemes are also used for enforcing priorities among flows whose packets are queued at nodes.
- Some scheduling schemes also consider battery characteristics.

Q.3. (*b*) What are the advantages of reservation based mac protocol over contention based mac protocol? Discuss. **(6.5)**

Ans. Ad hoc wireless networks sometimes may need to support real-time traffic, which requires QoS guarantees to be provided. In contention-based protocols, nodes are

not guaranteed periodic access to the channel. Hence they cannot support real-time traffic. In order to support such traffic, certain protocols have mechanisms for reserving bandwidth a priority. Such protocols can provide QoS support to time-sensitive traffic sessions.

Distributed Packet Reservation Multiple Access Protocol

Implicit reservation (PRMA - Packet Reservation Multiple Access):

- A certain number of slots form a frame, frames are repeated
- Stations compete for empty slots according to the slotted aloha principle
- Once a station reserves a slot successfully, this slot is automatically assigned to this station in all following frames as long as the station has data to send
- Competition for this slots starts again as soon as the slot was empty in the last frame

Collision avoidance time allocation protocol (CATA)

- Based on dynamic topology-dependent transmission scheduling
- Nodes contend for and reserve time slots by means of a distributed reservation and handshake mechanism.
- Support broadcast, unicast, and multicast transmissions.
- The operation is based on two basic principles:
- The receiver(s) of a flow must inform the potential source nodes about the reserved slot on which it is currently receiving packets. The source node must inform the potential destination node(s) about interferences in the slot.
- Usage of negative acknowledgements for reservation requests, and control packet transmissions at the beginning of each slot, for distributing slot reservation information to senders of broadcast or multicast sessions.

Hop reservation multiple access protocol (HRMA)

- A multichannel MAC protocol which is based on half-duplex, very slow frequency-hopping spread spectrum (FHSS) radios
- Uses a reservation and handshake mechanism to enable a pair of communicating nodes to reserve a frequency hop, thereby guaranteeing collision-free data transmission.
- Can be viewed as a time slot reservation protocol where each time slot is assigned a separate frequency channel.

Soft reservation multiple access with priority assignment (SRMA/PA)

- Developed with the main objective of supporting integrated services of real-time and non-real-time application in ad hoc networks, at the same time maximizing the statistical multiplexing gain.
- Nodes use a collision-avoidance handshake mechanism and a soft reservation mechanism.

Five-Phase Reservation Protocol (FPRP)

- A single-channel time division multiple access (TDMA)-based broadcast scheduling protocol.

- Nodes use a contention mechanism in order to acquire time slots.
- The protocol assumes the availability of global time at all nodes.
- The reservation takes five phases: reservation, collision report, reservation confirmation, reservation acknowledgement, and packing and elimination phase.

MACA with Piggy-Backed Reservation (MACA/PR)

- Provide real-time traffic support in multi-hop wireless networks
- Based on the MACAW protocol with non-persistent CSMA
- The main components of MACA/PR are:

  A MAC protocol, A reservation protocol, A QoS routing protocol

UNIT–II

Q.4. (a) List the characteristics of ideal routing protocol for ad hoc wireless network. **(6)**

Ans. A routing protocol for ad hoc wireless networks should have the following characteristics:

1. It must be fully distributed, as centralized routing involves high control overhead and hence is not scalable. Distributed routing is more fault tolerant than centralized routing, which involves the risk of single point of failure.

2. It must be adaptive to frequent topology changes caused by the mobility of nodes.

3. Route computation and maintenance must involve a minimum number of nodes. Each node in the network must have quick access to routes, that is, minimum connection setup time is desired.

4. It must be localized, as global state maintenance involves a huge state propagation control overhead.

5. It must be loop-free and free from stale routes.

6. The number of packet collisions must be kept to a minimum by limiting the number of broadcasts made by each node. The transmissions should be reliable to reduce message loss and to prevent the occurrence of stale routes.

7. It must converge to optimal routes once the network topology becomes stable. The convergence must be quick.

8. It must optimally use scarce resources such as bandwidth, computing power, memory, and battery power.

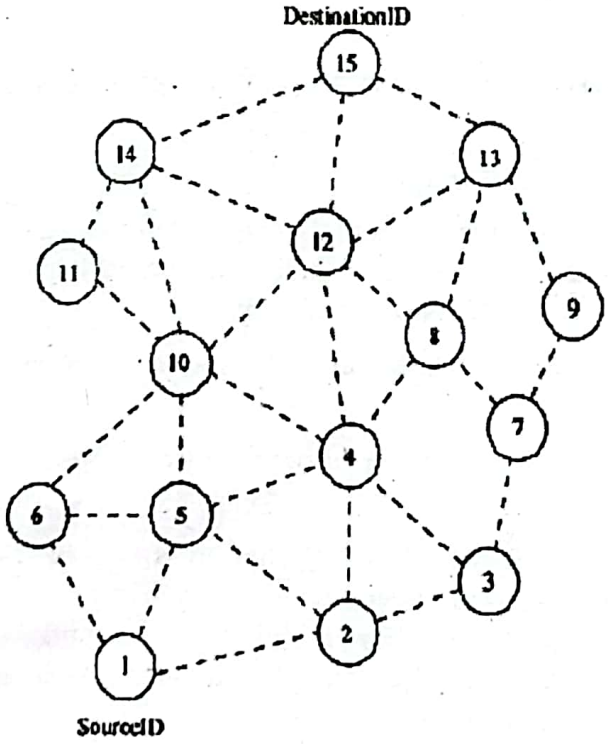
9. Every node in the network should try to store information regarding the stable local topology only. Frequent changes in local topology, and changes in the topology of parts of the network with which the node does not have any traffic correspondence, must not in any way affect the node, that is, changes in remote parts of the network must not cause updates in the topology information maintained by the node.

10. It should be able to provide a certain level of quality of service (QoS) as demanded by the applications, and should also offer support for time-sensitive traffic.

Q.4. (b) Discuss table driven protocol with examples. (6.5)

Ans. In table-driven routing protocols, every node maintains the network topology information in the form of routing tables by periodically exchanging routing information. Routing information is generally flooded in the whole network. Whenever a node requires a path to a destination, it runs an appropriate path-finding algorithm on the topology information it maintains. The destination sequenced distance-vector routing protocol (DSDV), wireless routing protocol (WRP), source-tree adaptive routing protocol (STAR), and cluster-head gateway switch routing protocol (CGSR) are some examples for the protocols that belong to this category.

Destination Sequenced Distance-Vector Routing Protocol: As it is a table-driven routing protocol, routes to all destinations are readily available at every node at all times. The tables are exchanged between neighbors at regular intervals to keep an up-to-date view of the network topology. The tables are also forwarded if a node observes a significant change in local topology. The table updates are of two types: incremental updates and full dumps. An incremental update takes a single network data packet unit (NDPU), while a full dump may take multiple NDPUs. Incremental updates are used when a node does not observe significant changes in the local topology. A full dump is done either when the local topology changes significantly or when an incremental update requires more than a single NDPU. Table updates are initiated by a destination with a new sequence number which is always greater than the previous one. Upon receiving an updated table, a node either updates its tables based on the received information or holds it for some time to select the best metric (which may be the lowest



(a) Topology graph of the network

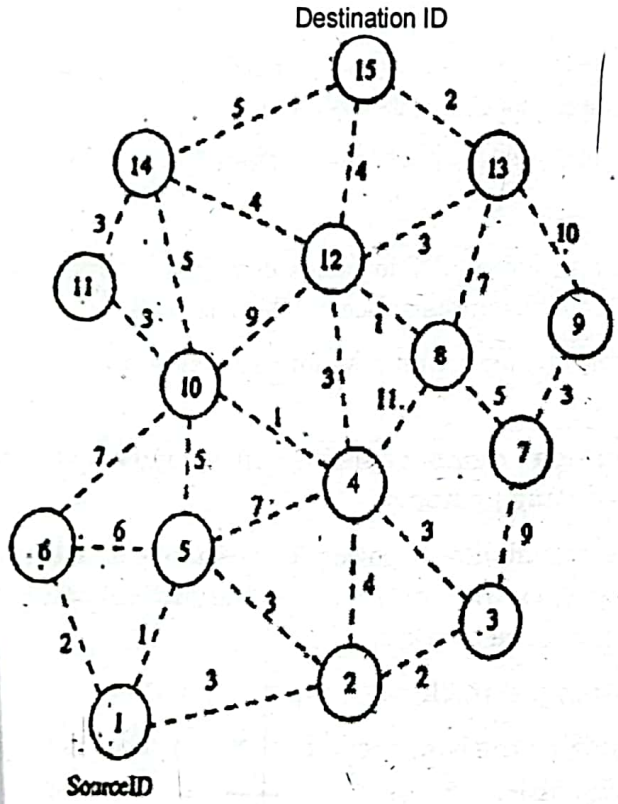
Desi	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	250

(b) Routing table for Node 1

number of hops) received from multiple versions of the same update table from different neighboring nodes. Based on the sequence number of the table update, it may forward or reject the table. Consider the example as shown in Figure. Here node 1 is the source node and node 15 is the destination. As all the nodes maintain global topology information, the route is already available as shown in Figure. Here the routing table of node 1 indicates that the shortest route to the destination node (node 15) is available through node 5 and the distance to it is 4 hops, as depicted in Figure

Wireless Routing Protocol (WRP)

WRP is similar to DSDV; it inherits the properties of the distributed bellman-ford algorithm. To counter the count-to-infinity problem and to enable faster convergence, it employs a unique method of maintaining information regarding the shortest distance to every destination node in the network and penultimate hop node on the path to every destination node. Maintains an up-to-date view of the network, every node has a readily available route to every destination node in the network.



Routing Entry at Each Node for Destination ID is

Node	Next Node	Pred	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	15	12	4
11	14	14	8
10	4	12	8
9	13	13	12
8	12	12	5
7	8	12	10
6	10	12	15
5	10	12	13
4	12	12	10
3	4	12	7
2	4	12	11
1	2	12	14

Fig. Route Establishment in WRP.

It differs from DSDV in table maintenance and in the update procedures. While DSDV maintains only one topology table, WRP uses a set of tables to maintain more accurate information.

The tables that are maintained by a node are :

- Distance table (DT): contains the network view of the neighbors of a node. It contains a matrix where each element contains the distance and the penultimate node reported by the neighbor for a particular destination.
- Routing table (RT): contains the up-to-date view of the network for all known destinations. It keeps the shortest distance, the predecessor/penultimate node, the successor node, and a flag indicating the status of the path. The path status may be a simplest (correct) path or a loop (error), or destination node not marked (null).
- Link cost table (LCT): contains the cost of relaying messages through each link. The cost of broken link is ∞. It also contains the number of update periods passed since the last successful update was received from that link.
- Message retransmission list (MRL): contains an entry for every update message that is to be retransmitted and maintains a counter for each entry.

After receiving the update message, a node not only updates the distance for transmitted neighbors but also checks the other neighbors' distance, hence convergence is much faster than DSDV.

Advantages

- WRP has the same advantages as that of DSDV.
- It has faster convergence and involves fewer table updates.

Disadvantages

- The complexity of maintenance of multiple tables demands a larger memory and greater processing power from nodes in the adhoc wireless network.
- It is not suitable for highly dynamic and also for very large ad hoc wireless networks.

Q.5. (a) What is the need for power management in ad hoc network? Discuss approaches for power aware routing protocol. (6.5)

Ans. The limitation on the availability of power for operation is a significant bottleneck. Hence, the use of routing metrics contributes to the efficient utilization of energy and increases the lifetime of the network.

Minimal energy consumption per packet

- This metric aims at minimizing the power consumed by a packet in traversing from source node to the destination node.
- The energy consumed by a packet when traversing through a path is the sum of the energies required at every intermediate hop in that path.
- This metric doesn't balance the load
- Disadvantages
- Selection of path with large hop length
- Inability to measure the power consumption in advance
- Inability to prevent the fast discharging of batteries at some nodes

Maximize network connectivity

- This metric attempt to balance the routing load among the cut set (the subset of the nodes in the network, the removal of which results in network partitions).
- It is difficult to achieve a uniform battery draining rate for the cut set.

Maximum variance in Node power levels

- This metric proposes to distribute the load among all nodes in the network so that the power consumption pattern remains uniform across them.
- This problem is very complex when the rate and size of the data packets vary

Minimum cost per packet

- In order to maximize the life of every node in the network, this routing metric is made as a function of the state of the node's battery.
- A node's cost decreases with an increase in its battery change and vice versa.
- Cost of node can be easily computed
- Advantage congestion handling & cost calculation

Minimize maximum node cost

- This metric minimizes the maximum cost per node for a packet after routing a number of packets or after a specific period.
- This delays the failure of a node, occurring due to higher discharge because of packet forwarding

Q.5. (*b*) What do you understand by network security requirements? Discuss the issues and challenges in secure routing of ad hoc wireless networks. (6)

Ans. A security protocol for ad hoc wireless networks should satisfy the following requirements.

- **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.

- **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.

- **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.

- **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.

The issues and challenges in secure routing of ad hoc wireless networks are

• **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.

• **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.

• **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.

• **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.

• **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.

• **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.

UNIT-III

Q.6. (a) Explain about the hardware components of sensor nodes. (6)

Ans. The main components of a sensor node are a microcontroller, transceiver, external memory, power source and one or more transducers (sensors).

Controller: The controller performs tasks, processes data and controls the functionality of other components in the sensor node. While the most common controller is a microcontroller, other alternatives that can be used as a controller are: a general purpose desktop microprocessor, digital signal processors, FPGAs and ASICs.

Transceiver: Sensor nodes often make use of ISM band, which gives free radio, spectrum allocation and global availability. The possible choices of wireless transmission media are radio frequency (RF), optical communication (laser) and infrared. Lasers require less energy , but need line-of-sight for communication and are sensitive to atmospheric conditions. Infrared, like lasers, needs no antenna but it is limited in its broadcasting capacity.

External memory: From an energy perspective, the most relevant kinds of memory are the on-chip memory of a microcontroller and Flash memory—off-chip RAM is rarely, if ever, used. Flash memories are used due to their cost and storage capacity. Memory requirements are very much application dependent. Two categories of memory based on the purpose of storage are: user memory used for storing application related or personal data, and program memory used for programming the device. Program memory also contains identification data of the device if present.

Power source: A wireless sensor node is a popular solution when it is difficult or impossible to run a mains supply to the sensor node. However, since the wireless sensor node is often placed in a hard-to-reach location, changing the battery regularly can be costly and inconvenient. An important aspect in the development of a wireless sensor node is ensuring that there is always adequate energy available to power the system. The sensor node consumes power for sensing, communicating and data processing.

Sensors (Transducers): Sensors are used by wireless sensor nodes to capture data from their environment. They are hardware devices that produce a measurable response to a change in a physical condition like temperature or pressure. Sensors measure physical data of the parameter to be monitored and have specific characteristics such as accuracy, sensitivity etc. The continual analog signal produced by the sensors is digitized by an analog-to-digital converter and sent to controllers for further processing. Some sensors contain the necessary electronics to convert the raw signals into readings which can be retrieved via a digital link (e.g. I2C, SPI) and many convert to units such as °C. Most sensor nodes are small in size, consume little energy, operate in high volumetric densities, be autonomous and operate unattended, and be adaptive to the environment. As wireless sensor nodes are typically very small electronic devices, they can only be equipped with a limited power source of less than 0.5-2 ampere-hour and 1.2-3.7 volts.

Q.6. (*b*) Write notes on Dynamic Energy & power management. (6.5)

Ans. Power management is defined as the process of managing the sources & consumers of energy in a node or in the network for enhancing the lifetime of a network.

Features of energy management are :

- Shaping the energy discharge pattern of a node's battery to enhance battery life.
- Finding routes that consumes minimum energy
- Using distributed scheduling schemes to improve battery life.
- Handling the processor & interface devices to minimize power consumption.

Energy management can be classified into the following categories :

a. Transmission power management :

- The power consumed by the Radio Frequency (RF) module of a mobile node is determined by several factors such as the state of operation, transmission power and technology used for the RF circuitry.
- The state of operation refers to transmit, receive, and sleep modes of the operation.

•The transmission power is determined by Reach ability requirement of the network, Routing protocol and MAC protocol employed.

b. Battery energy management :

The battery management is aimed at extending the battery life of a node by taking advantage of its chemical properties, discharge patterns, and by the selection of a battery from a set of batteries that is available for redundancy.

c. Processor power management :

- The clock speed and the number of instructions executed per unit time are some of the processor parameters that affect power consumption.
- The CPU can be put into different power saving modes during low processing load conditions.
- The CPU power can be completely turned off if the machines are idle for a long time. In such a cases, interrupts can be used to turn on the CPU upon detection of user interaction or other events.

d. Devices power management :

Intelligent device management can reduce power consumption of a mobile node significantly. This can be done by the operating system(OS) by selectively powering down interface devices that are not used or by putting devices into different power saving modes, depending on their usage.

Q.7. (a) Discuss and explain about the MAC protocol in WSN. (6)

Ans. Following are the MAC protocol in WSN

• Sensor MAC (S-MAC)

It operates by placing a node in a state that listens to the medium; if a node hears nothing it sends a SYNC packet with a schedule defining listens and sleep periods. All nodes hearing this packet will adopt the schedule. Nodes may adopt two or more schedules (if different neighbors have different schedules). Nodes keep tables with the schedules of their neighbors. During a listen period, a node with a packet to send

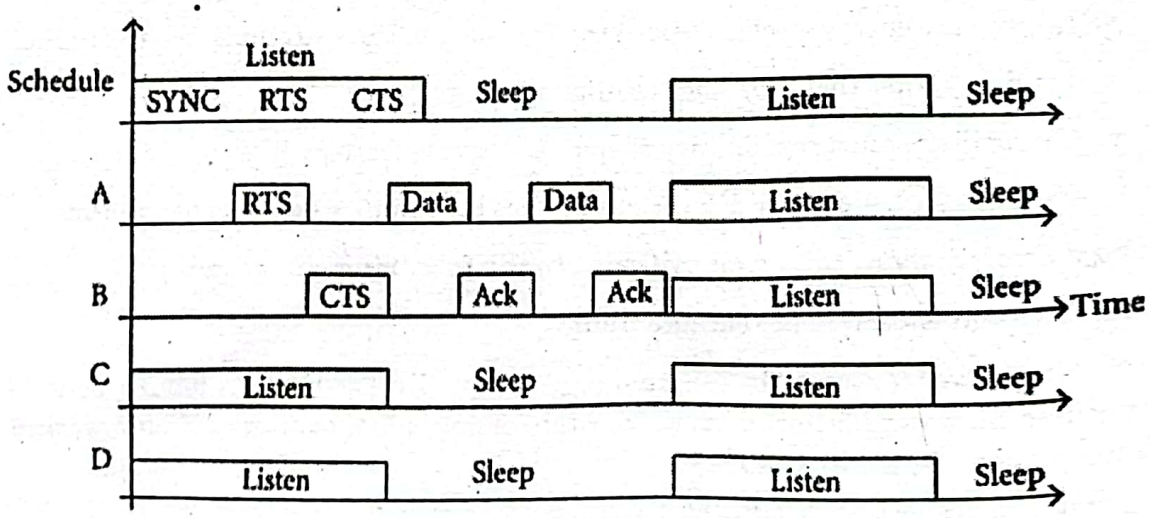


Fig: S-MAC

xecutes a procedure similar to 802.11 virtual channel sensing, it will send a request to end (RTS) frame and the receiver node will answer with a clear to send (CTS) frame. ll nodes not involved in the conversation will enter a sleep state while the mmunicating nodes send data packets and ACKs. Sleeping decreases energy nsumption but introduces latency since communication with a sleeping node must ait until it wakes up . Figure shows an example of the sequence of events occurring in mmunication between four nodes using S-MAC.

- **Berkeley Media Access Control for Low-Power Sensor Networks (B-MAC)**

B-MAC employs an adaptive preamble to reduce idle listening, a major source of ergy usage in many protocols. When a node has a packet to send, it waits during a ck off time before checking the channel. If the channel is clear, the node transmits; herwise it begins a second (congestion) back off. Each node must check the channel riodically using LPL (low-power listening); if the channel is idle and the node has no ta to transmit, the node returns to sleep . The B-MAC preamble sampling scheme justs the interval in which the channel is checked to equal the frame preamble size. an example, if the medium is checked every 100 ms, the preamble of the packet must st 100 ms as a minimum, in order for the receiver to detect the packet. Upper layers ay change the preamble duration, according to the application requirements.

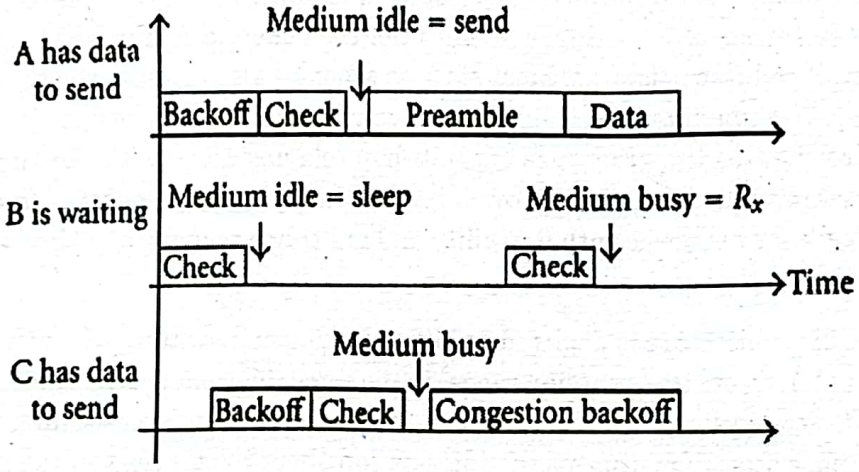


Fig B MAC

- **Predictive Wake-UP MAC (PW-MAC)**

PW-MAC improves on protocols like S-MAC and B-MAC because it uses pseudo ndom schedules, thus not all nodes will wake up and transmit at the same time, oiding collisions. A node that has just woke up sends a short beacon so other nodes ow it is up. A sender can then transmit a data packet and request more information om the receiver, such as current time and current seed for the pseudo random schedule ed by receiver. By using the seed in a linear congruential generator (LCG), sender in W-MAC can predict when a receiver will wake up; hence sender sleeps until a little bit efore the receiver is awake.

However, there are hardware variations that generate errors in the sender prediction. W-MAC uses a "sender wake-up advance time" a compensating value particular to very platform, including clock drift, operating system delay, and hardware latency. The

value helps correcting errors each node can do when predicting a receiver wake-up time.

Low-Energy Adaptive Clustering Hierarchy (LEACH)

LEACH includes application, routing, MAC, and physical characteristics for communication in WSNs. A specific application considered is remote monitoring where data gathered by neighboring nodes may be redundant. LEACH assumes all nodes are synchronized, they can control their transmission power, and they can reach one base station (BS, equivalent to the sink in other protocols) if needed. The nodes also have sufficient processing capabilities to implement different MAC protocols and perform signal processing functions, such that all information can be aggregated in only one message. Nodes organize in clusters, elect a cluster head (CH), and then start sending information. Every cluster uses DSSS with a different code, to minimize interference

Q.7. (b) Write short note on routing in hybrid wireless networks. (6.5)

Ans. One of the major application areas of ad hoc wireless networks is in hybrid wireless architectures such as multi-hop cellular networks (MCNs) and integrated cellular ad hoc relay (iCAR) networks. The tremendous growth in the subscriber base of existing cellular networks has shrunk the cell size up to the pico-cell level. The primary concept behind cellular networks is geographical channel reuse. Several techniques such as cell sectoring, cell resizing, and multi tier cells have been proposed to increase the capacity of cellular networks. Most of these schemes also increase the equipment cost. The capacity (maximum throughput) of a cellular network can be increased if the network incorporates the properties of multi-hop relaying along with the support of existing fixed infrastructure. MCNs combine the reliability and support of fixed base stations of cellular networks with flexibility and multi-hop relaying of ad hoc wireless networks.

The MCN architecture is depicted in Figure In this architecture, when two nodes (which are not in direct transmission range) in the same cell want to communicate with each other, the connection is routed through multiple wireless hops over the intermediate nodes. The base station maintains the information about the topology of the network for efficient routing. The base station may or may not be involved in this multi-hop path. Suppose node A wants to communicate with node B. If all nodes are capable of operating in MCN mode, node A can reach node B directly if the node B is within node A's transmission range. When node C wants to communicate with node E and both are in the same cell, node C can reach node E through node D, which acts as an intermediate relay node. Such hybrid wireless networks can provide high capacity resulting in lowering the cost of communication to less than that in single-hop cellular networks. The major advantages of hybrid wireless networks are as follows:

- Higher capacity than cellular networks obtained due to the better channel reuse provided by reduction of transmission power, as mobile nodes use a power range that is a fraction of the cell radius.

- Increased flexibility and reliability in routing. The flexibility is in terms of selecting the best suitable nodes for routing, which is done through multiple mobile nodes or through base stations, or by a combination of both. The increased reliability is in terms

of resilience to failure of base stations, in which case a node can reach other nearby base stations using multi-hop paths.

• Better coverage and connectivity in holes (areas that are not covered due to transmission difficulties such as antenna coverage or the direction of antenna) of a cell can be provided by means of multiple hops through intermediate nodes in the cell.

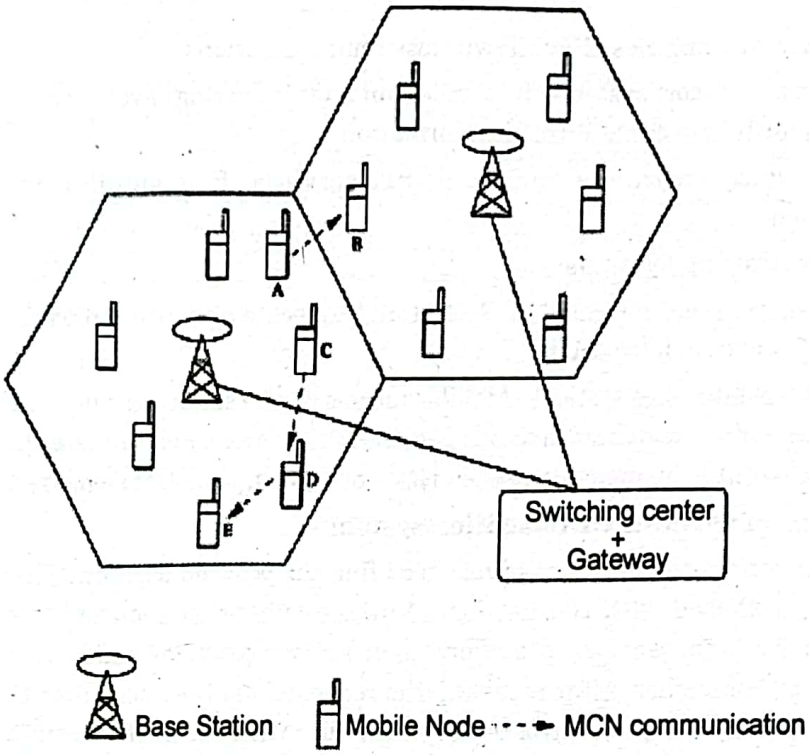


Fig: MCN

UNIT–IV

Q.8. What is Wireless geo location system? Discuss and explain the wireless olocation system architecture. **(12.5)**

Ans. There are many terms used to determine the location of mobile station such position, location, geo location, radio location etc. This includes the information out latitude and longitude. Geo location technology is widely used in military and mmercial applications. Here location based service means providing service to remote bile user based on their geographical position. Positioning systems are used in many plications such as mapping service, information services, reservation, booking service . in such system, accuracy is very important. It is similar to Bit error rate in ecommunication systems. Voice packets tolerate only one percentage of bit error e. Location based system accuracy is defined as the area of uncertainty around the ct location where the % of repeated location measurement are reported. The physical aracteristic such as radio propagation environment, noise and interference aracteristics and receiver design affects the system. The GOS in telecommunication tem is the call blocking rate during the peak hour. In these systems the coverage responds to the availability of measurements to perform a location computation.

Indoor Geo location applications:

Some examples are given below:

Locating person within the building

Finding mentally impaired patients in hospitals

PLS (personal locator service) – It has the locator device which is available with a person.

Telemetric- It combines GP with wireless communications

Intelligent transport systems- It includes automatic steering of vehicles, navigation of vehicles according to current traffic information.

E-911 services- wireless enhanced -911 services. It is suitable to cellular communication.

Types of positioning systems:

1. Self-positioning systems- Mobile station can locate own position by measuring its distance from known locations.

2. Remote positioning systems- Mobile stations can be small size and consume low power. Receiver which is in known location on the network together compute the location of mobile transmitter by measuring the distance of this mobile from each receiver.

Architecture of wireless GEO location system:

Location estimation of the mobile is used find the position location. This location information is shared with the network. Initially subscriber requests the location information from the service provider. Then service provider sends the location information to subscriber. After receiving the request from the subscriber the service provider contact the location control center which can gather the information to calculate the location of the mobile station. With the past information about mobile station location, a set of base is used to page the mobile station. After collecting this information the location control center find out the location of the mobile while can be given to the service provider.

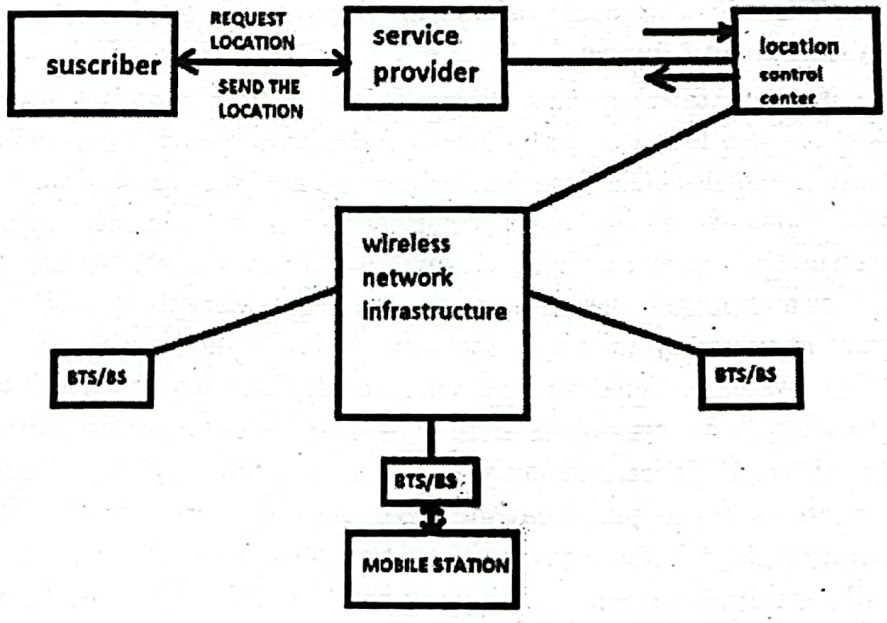
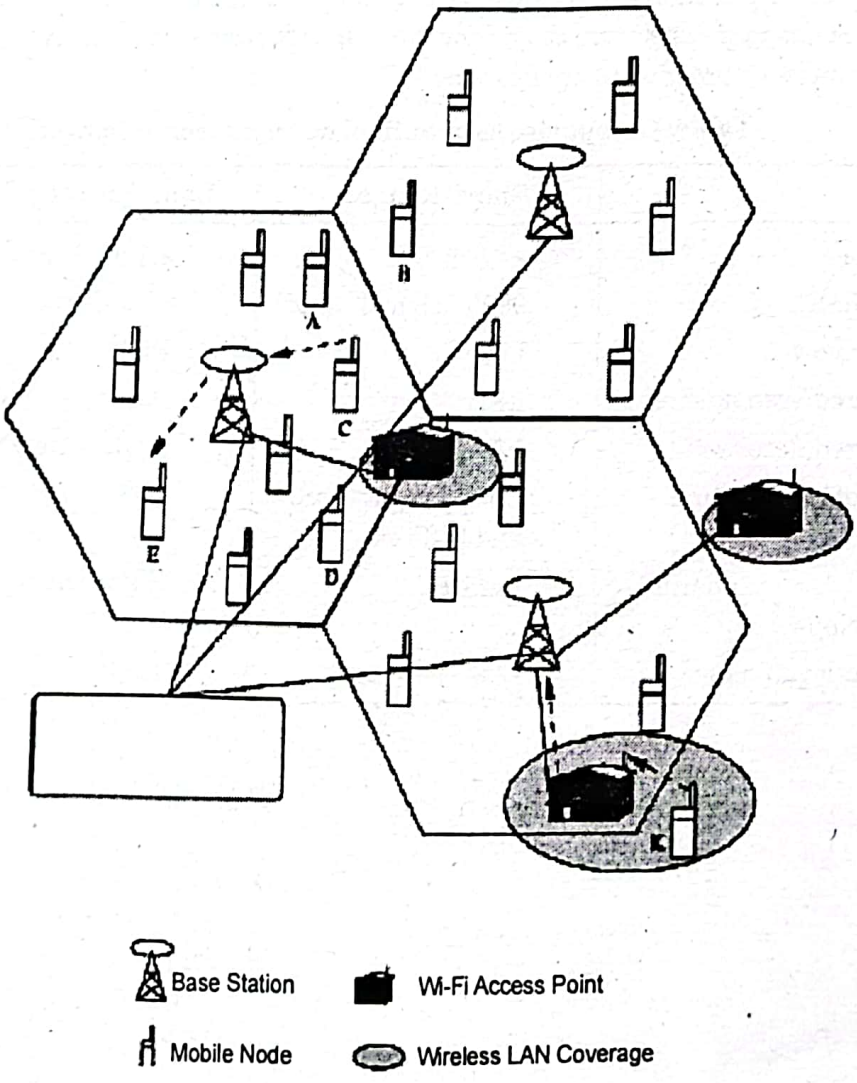


Fig: Architecture of wireless GEO location system

Q.9. Write short note on:

Q.9. (a) Wireless fidelity systems. **(6.5)**

Wireless fidelity (Wi-Fi) system is the high-speed wireless LAN that was originally ıended to extend the wired Ethernet in offices to wireless clients. The coverage area d ability to support high bit rates are the two major reasons behind the name Wi-Fi. ough the popular wireless LAN standards IEEE802.11b and 802.11a are considered the standard Wi-Fi candidates, conceptually any high-speed wireless LAN protocol :h as HiperLAN can be used. The integration of Wi-Fi hotspots (wireless LAN access nts) with wide area wireless networking technologies such as GSM and GPRS provides added advantage for the mobile nodes. Such an integrated system provides secure, able, and high speed wireless connectivity. A Wi-Fi network can be used to connect ıputers to each other, to the Internet, and to wired networks. Wi-Fi networks operate he unlicensed 2.4 GHz and 5GHz radio bands, with an 802.11b or 802.11a, or with ducts that contain both bands (dual band), so that they can provide an enriched work experience. Wi-Fi systems are potential candidates for provisioning high-speed timedia content delivery in areas such as indoor offices, airport lounges, and shopping ls. The Wi-Fi Alliance is a nonprofit international association formed in 1999 to ify interoperability of IEEE 802.11-based products in order to make the objectives



of Wi-Fi a reality. The advantages of Wi-Fi systems are ease-of-use, high-speed Internet access, low cost of operation, and flexibility of reconfiguration.

Q.9. (b) Optical wireless networks (8)

Ans. Optical wireless communication enables communication using infrared rays and light waves operating at frequencies well beyond the visible spectrum for high data rate local communication. Optical wireless communication technology exhibits a number of properties that makes it a suitable alternative to indoor RF communication. The advantages of optical wireless communication include significantly less interference due to its lack of penetration through walls, positioning of spectrum at a completely unregulated and unlicensed band, increased security, and high data rate. Optical wireless technology promises broadband data delivery at short ranges in point-to multipoint LANs and point-to-point medium-distance optical links. Optical wireless transmission can be classified into short-range communication and long-range communication systems. A comparison of these two types of optical wireless transmission schemes is given in Table. Long-range communication systems are mainly used for outdoor point-to-point optical links and short-range systems are used in indoor and outdoor applications. Unlike the long-haul networks in fiber-based optical networks, the long-range optical wireless systems can operate over a distance of hundreds of meters only. The short-range systems operate over a distance of few meters. With the ever growing demand for broadband wireless connectivity, the utilization of RF spectrum is a bottleneck due to the spectrum congestion, licensing requirements, and unsuitability of certain bands for broadband applications.

Table: Comparisons of optical wireless technologies.

Issue	Short-Range	Long-Range
Distance	< 10 m	< 1,000 m
Data Rate	9600 bps to 4 Mbps	< 10 Gbps
Source Power	Low	High
Preferred Transmitter	LED	Laser
Preferred Receiver	PIN Diode	Avalanche Diode
Mode of Propagation	Line of Sight (LoS) and Diffused	LoS
Effect of Atmospheric Conditions	Limited	Significant
Cost of Equipment	Low	High

FIRST TERM EXAMINATION [FEB. 2018]
EIGHTH SEMESTER [B.TECH]
ADHOC AND SENSOR NETWORK [ETEC-406]

ne : 1½ hrs. M.M. : 30

te: *Q. no. 1 is compulsory. Attempt any two more questions from the rest.*

Q.1. (a) What is an ad-hoc network? Why ad hoc network are needed? Discuss. (2.5)

Ans. Ad hoc wireless networks are defined as the category of wireless networks that ize multi-hop radio relaying and are capable of operating without the support of any d infrastructure (hence they are also called infrastructure less networks). The ence of any central coordinator or base station makes the routing a complex one pared to cellular networks.

Advantages of Ad Hoc Network: The rapid development in ad hoc technology is ely used in portable computing such as laptop, mobile phone used to access the web ices, telephone calls when the user are in travelling. Development of self-organizing work decrease the communication cost. The growth of 4G technology enhances anytime, where, anyhow communication in ad hoc network. Ad hoc network is simple to design install. The advantages of an ad hoc network include: Separation from central work administration.

- Self-configuring nodes are also routers.
- Self-healing through continuous re-configuration.
- Scalability incorporates the addition of more nodes.
- Mobility allows ad hoc networks created on the fly in any situation where there multiple wireless devices.
- Flexible ad hoc can be temporarily setup at anytime, in any place.
- Lower getting-started costs due to decentralized administration.
- The nodes in ad hoc network need not rely on any hardware and software. So, it be connected and communicated quickly.

Q.1. (b) What are the various issues in designing MAC protocol for AD HOC works? (2.5)

Ans. The main issues in designing MAC protocol for ad hoc wireless network are:

Bandwidth efficiency: Bandwidth must be utilized in efficient manner Minimal ntrol overhead BW = ratio of BW used for actual data transmission to the total ilable BW

Quality of service support: Essential for supporting time-critical traffic sessions They have resource reservation mechanism that takes into considerations the nature vireless channel and the mobility of nodes.

Synchronization: MAC protocol must consider synchronization between nodes in network

Synchronization is very important for BW (time slot) reservation by nodes Exchange ontrol packets may be required for achieving time synchronization among nodes

Hidden and exposed terminal problems: The hidden terminal problem refers to e collision of packets at a receiving node due to the simultaneous transmission of ose nodes that are not within the direct transmission range of the sender but are within e transmission range of the receiver. Collision occurs when both nodes transmit ckets at the same time without knowing about the transmission of each other.

Q.1. (c)List the characteristics of ideal routing protocol for ad hoc wireless network. **(2.5)**

Ans. A routing protocol for ad hoc wireless networks should have the following characteristics:

1. It must be fully distributed, as centralized routing involves high control overhead and hence is not scalable. Distributed routing is more fault tolerant than centralized routing, which involves the risk of single point of failure.

2. It must be adaptive to frequent topology changes caused by the mobility of nodes.

3. Route computation and maintenance must involve a minimum number of nodes. Each node in the network must have quick access to routes, that is, minimum connection setup time is desired.

4. It must be localized, as global state maintenance involves a huge state propagation control overhead.

5. It must be loop-free and free from state routes.

Q.1. (d)Why is need of power management important in AD HOC network? **(2.5)**

Ans. The power constraints in sensor networks are much more stringent than those in ad hoc wireless networks. This is mainly because the sensor nodes are expected to operate in harsh environmental or geographical conditions, with minimum or no human supervision and maintenance. In certain case, the recharging of the energy source is impossible. Running such a network, with nodes powered by a battery source with limited energy, demands very efficient protocol at network, data link, and physical layer.

Q.2 Compare MACA with MACAW protocol. **(10**

Ans. MACAW (MACA for Wireless) is a revision of MACA.

- The sender senses the carrier to see and transmits a RTS (Request To Send) frame if no nearby station transmits a RTS.
- The receiver replies with a CTS (Clear to Send) frame.
- The MACAW protocol uses one more control packet called the request-for-request-to-send (RRTS)

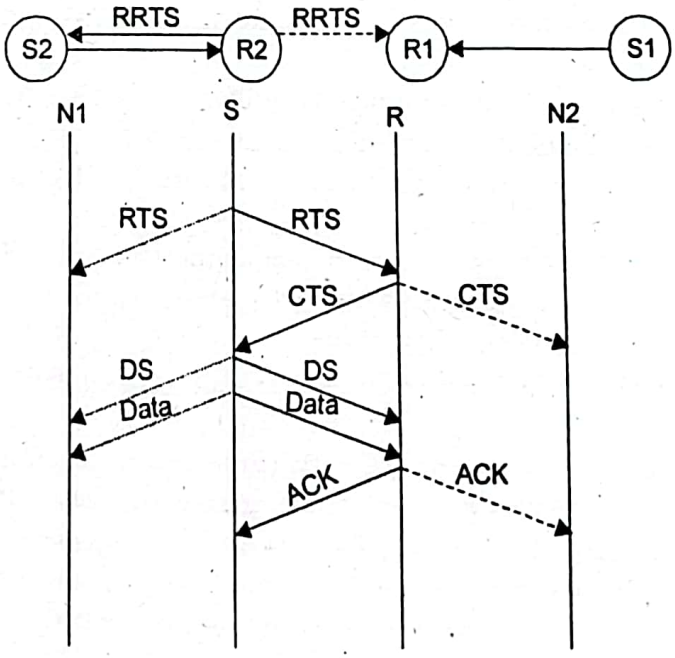


Fig. Packet exchange in MACAW.

Neighbors

- see CTS, then keep quiet.
- see RTS but not CTS, then keep quiet until the CTS is back to the sender.

The receiver sends an ACK when receiving an frame.

- Neighbors keep silent until see ACK.

Collisions

- There is no collision detection

The senders know collision when they don't receive CTS.

- They each wait for the exponential back-off time.

Q.3 (a)What is the classification of MAC protocol? **(5)**

Ans. MAC protocols for ad hoc wireless networks can be classified into several categories based on various criteria such as initiation approach, time synchronization, and reservation approaches. Ad hoc network MAC protocols can be classified into three basic types:

- Contention-based protocols
- Contention-based protocols with reservation mechanisms
- Contention-based protocols with scheduling mechanisms

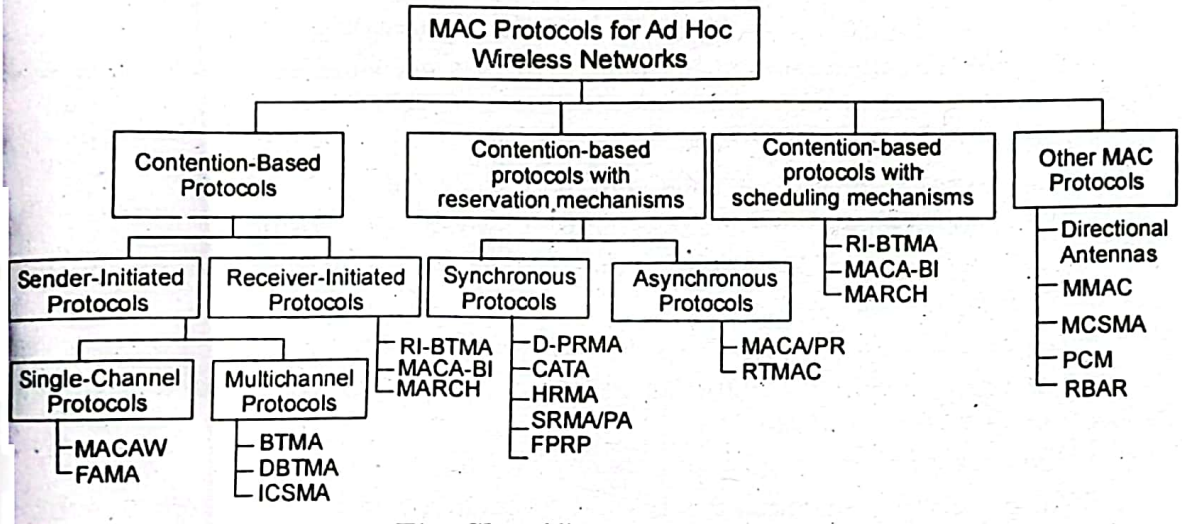


Fig. Classification of MAC

Contention-based protocols

- Sender-initiated protocols: Packet transmissions are initiated by the sender node.
- Single-channel sender-initiated protocols: A node that wins the contention to the channel can make use of the entire bandwidth.
- Multichannel sender-initiated protocols: The available bandwidth is divided into multiple channels.
- Receiver-initiated protocols: The receiver node initiates the contention resolution protocol.

Contention-based protocols with reservation mechanisms

- Synchronous protocols: All nodes need to be synchronized. Global time synchronization is difficult to achieve.
- Asynchronous protocols: These protocols use relative time information for effecting reservations.

Contention-based protocols with scheduling mechanisms

• Node scheduling is done in a manner so that all nodes are treated fairly and no node is starved of bandwidth.

• Scheduling-based schemes are also used for enforcing priorities among flows whose packets are queued at nodes.

• Some scheduling schemes also consider battery characteristics.

Q.3. (b) What are the characteristics and features of ad hoc networks? List the design goal of MAC protocol for ad hoc networks. (5)

Ans. Ad hoc networks are multi-hop network that use wireless communication for transmission without any fixed infrastructure. The networks are form and deform on-the-fly without the need for any system. Ad hoc structure does not require an access point, it is easy to setup, especially in a small or temporary network. Each node in the network forwards the packet without the need of central administration. In ad hoc network, node acts as a router to send and receive the data. An advantage of the system is robustness, flexibility and mobility. Ad hoc network are capable for analyzing radio propagation environment to optimize the performance. This typically requires that the network node have positioning capability as well as memory to recall geographical local condition. An ad hoc network typically refers to any set of network where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE802.11 wireless networks.

The design goal of MAC protocol for ad hoc networks.

The following are the important goals to be met while designing a medium access control

(MAC) protocol for ad hoc wireless networks:

• The operation of the protocol should be distributed.

• The protocol should provide QoS support for real-time traffic.

• The access delay, which refers to the average delay experienced by any packet to get transmitted, must be kept low.

• The available bandwidth must be utilized efficiently.

• The protocol should ensure fair allocation (either equal allocation or weighted allocation) of bandwidth to nodes.

• Control overhead must be kept as low as possible.

• The protocol should minimize the effects of hidden and exposed terminal problems.

• The protocol must be scalable to large networks.

• It should have power control mechanisms in order to efficiently manage energy consumption of the nodes.

Q.4. Classify and explain in details various types of routing protocol ADHOC wireless networks.

Ans. Refer of Q.3. First Term Exam 2017.

END TERM EXAMINATION MAY-JUNE 2018
EIGHTH SEMESTER [B.TECH]
ADHOC AND SENSOR NETWORK [ETEC-406]

Time : 3 hrs. **M.M. : 75**

Note: *Attempt any five questions in all including Q.no. 1. which is compulsory. Select one question from each unit.*

Q.1. (a) What is the difference between cellular and Ad Hoc wireless networks. **(3)**

Ans. Refer Q.2. (b) of First Term Exam Pg.3-2017.

Q.1. (b) What are the application of Ad Hoc wireless network. **(3)**

Ans. Refer Q.1 (b) of End Term Exam Pg. 8-2017.

Q.1. (c) Define Inter symbol Interference and method to avoid it. **(3)**

Ans. Inter symbol interference (ISI) is a form of distortion of a signal in which one ymbol interferes with subsequent symbols. This is an unwanted phenomenon as the revious symbols have similar effect as noise, thus making the communication less eliable. The spreading of the pulse beyond its allotted time interval causes it to interfere ith neighboring pulses. ISI is usually caused by multipath propagation or the inherent near or non-linear frequency response of a communication channel causing successive mbols to "blur" together.

The presence of ISI in the system introduces errors in the decision device at the ceiver output. Therefore, in the design of the transmitting and receiving filters, the jective is to minimize the effects of ISI, and thereby deliver the digital data to its stination with the smallest error rate possible.

In order to have no ISI at the receiver, we must treat this pulse-shaping filter, and y filtering done at the transmitter, the channel and the receiver all together as part of e channel.

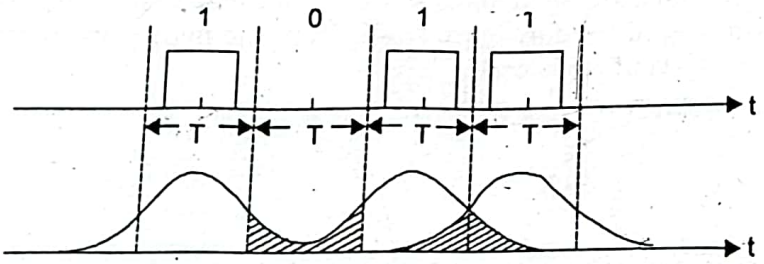


Fig. 1. Inter Symbol Interference.

Q.1. (d) What are the major functions performed by TCP? **(4)**

Ans. The objectives of a transport layer protocol include the setting up of an end-to d connection, end-to-end delivery of data packets, flow control, and congestion control. ere exist simple, unreliable, and connection-less transport layer protocols such as DP, and reliable, byte-stream-based, and connection oriented transport layer protocols ch as TCP for wired networks. These traditional wired transport layer protocols are t suitable for ad hoc wireless networks due to the inherent problems associated with e latter. The transmission control protocol (TCP) is the most predominant transport yer protocol in the Internet today. It transports more than 90% percent of the traffic n the Internet. Its reliability, end-to-end congestion control mechanism, byte stream ransport mechanism, and, above all, its elegant and simple design have not only ntributed to the success of the Internet, but also have made TCP an influencing protocol n the design of many of the other protocols and applications. Its adaptability to the

congestion in the network has been an important feature leading to graceful degradation of the services offered by the network at times of extreme congestion. TCP in its traditional form was designed and optimized only for wired networks.

Q.1. (e) Discuss the issues in designing a Transport Layer Protocol for Ad hoc wireless network. **(4)**

Ans. The various usues in designing transport layer protocol are: Induced traffic: Unlike wired networks, ad hoc wireless networks utilize multi-hop radio relaying. A link-level transmission affects the neighbor nodes of both the sender and receiver of the link. In a path having multiple links, transmission at a particular link affects one upstream link and one downstream link.

Induced throughput unfairness: This refers to the throughput unfairness at the transport layer due to the throughput/delay unfairness existing at the lower layers such as the network and MAClayers

Separation of congestion control, reliability, and flow control: A transport layer protocol can provide better performance if end-to-end reliability, flow control, and congestion control are handled separately. Reliability and flow control are end-to-end activities, whereas congestion can at times be a local activity.

Power and bandwidth constraints

Misinterpretation of congestion: Traditional mechanisms of detecting congestion in networks, such as packet loss and retransmission timeout, are not suitable for detecting the network congestion in ad hoc wireless networks

Dynamic topology: Some of the deployment scenarios of ad hoc wireless networks about experience rapidly changing network topology due to the mobility of nodes

Q.1. (f) Why does TCP not work well in ad hoc network? Explain. **(4)**

Ans. Refer Q.4 (b) of First Term Exam 2017.

Q.1. (g) Discuss the load balancing in hybrid wireless networks. **(4)**

Ans. Load balancing refers to the distribution of relay traffic load uniformly throughout the network so that no region in the network is particularly overloaded. The need for load balancing arises from the fact that the amount of relay traffic (traffic relayed by a node) in a static multi-hop wireless network is dependent on the position of the nodes in the network and the node density in the region. As a result, the nodes close the center of the network need to relay more traffic than the nodes away from the center when the shortest path routing is used.

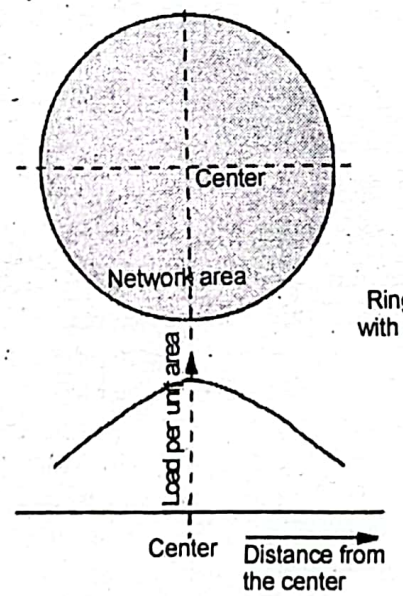
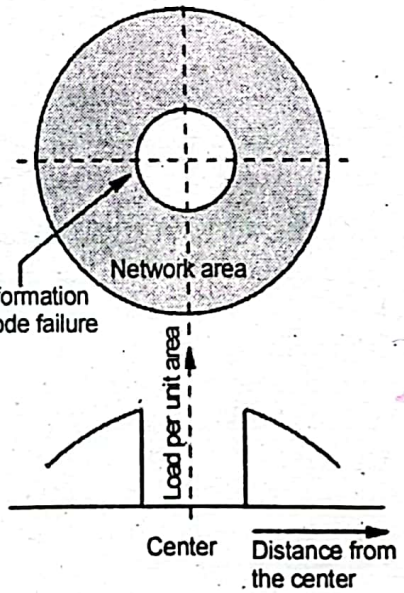


Fig. (a) Load density varies with distance from the center of the network



(b) Formation of ring due to the failure of nodes at the center of the network caused by excessive relay traffic

The load balancing is important in hybrid wireless networks such as MCNs, when the traffic locality is low (traffic locality is defined as the fraction of originated calls that gets terminated in the same cell). Traffic locality varies between 0 and 1, where locality = 0 refers to the case where the source and destination are in different cells and locality = 1 refers to a situation where all the calls get terminated within the cell. With low values of traffic locality, the probability that the BS will become saturated is high. Load balancing can improve performance in such situations.

UNIT-I

Q.2. Define AD HOC network. Explain in detail architecture of ad hoc network with its significant aspects. **(6.5)**

Ans. Ad hoc wireless networks are defined as the category of wireless networks that tilize multi-hop radio relaying and are capable of operating without the support of any xed infrastructure (hence they are also called infrastructure less networks). The bsence of any central coordinator or base station makes the routing a complex one mpared to cellular networks.

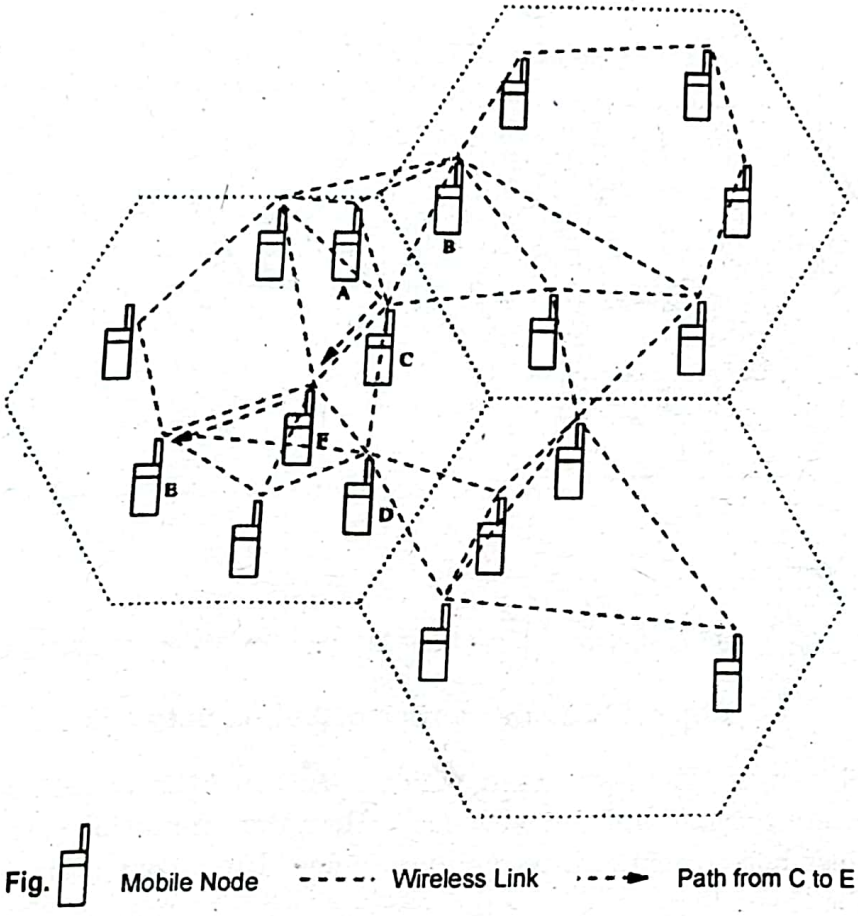


Fig. Mobile Node Wireless Link Path from C to E

d hoc wireless networks are defined as the category of wireless networks that utilize -hop radio relaying and are capable of operating without the support of any fixed tructure (hence they are also called infrastructure less networks). The absence of entral coordinator or base station makes the routing a complex one compared to ar networks. The rapid development in ad hoc technology is widely used in portable uting such as laptop, mobile phone used to access the web services, telephone calls the user are in travelling. Development of self-organizing network decrease the

communication cost. The growth of 4G technology enhances anytime, anywhere, anyhow communication in ad hoc network. Ad hoc network is simple to design and install. The advantages of an ad hoc network include: Separation from central network administration.

- Self-configuring nodes are also routers.
- Self-healing through continuous re-configuration.
- Scalability incorporates the addition of more nodes.
- Mobility allows ad hoc networks created on the fly in any situation where there are multiple wireless devices.
- Flexible ad hoc can be temporarily setup at anytime, in any place.
- Lower getting-started costs due to decentralized administration.
- The nodes in ad hoc network need not rely on any hardware and software. So, it can be connected and communicated quickly.

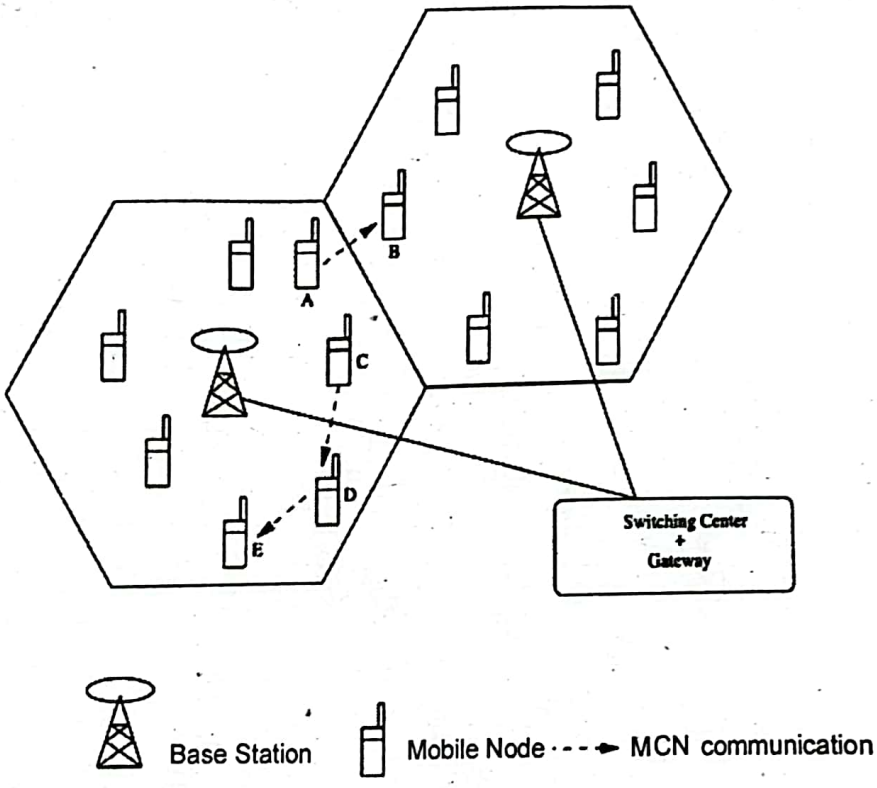


Fig: MCN Architecture of Adhoc network

In this architecture, when two nodes (which are not in direct transmission range) in the same cell want to communicate with each other, the connection is routed through multiple wireless hops over the intermediate nodes. The base station maintains the information about the topology of the network for efficient routing. The base station may or may not be involved in this multi-hop path. Suppose node A wants to communicate with node B. If all nodes are capable of operating in MCN mode, node A can reach node B directly if the node B is within node A's transmission range. When node C wants to communicate with node E and both are in the same cell, node C can reach node E through node D, which acts as an intermediate relay node. Such hybrid wireless networks can provide high capacity resulting in lowering the cost of communication to less than that in single-hop cellular networks.

Q. 2. (b) Explain the contention based protocols with scheduling and ervation in detail. **(6)**

Ans. Refer Q.2 (b) of End Term Exam Pg. 13-2017.

Q.3. (a) Explain the issues in designing a MAC protocol for ad hoc wireless tworks. **(6.5)**

Ans. The main issues in designing MAC protocol for ad hoc wireless network are:

ındwidth efficiency

- Bandwidth must be utilized in efficient manner.
- Minimal Control overhead
- BW = ratio of BW used for actual data transmission to the total available B W.

Quality of service support

- Essential for supporting time-critical traffic sessions.
- They have resource reservation mechanism that takes into considerations the ıre of wireless.
- Channel and the mobility of nodes.

Synchronization

- MAC protocol must consider synchronization between nodes in the network.
- Synchronization is very important for BW (time slot) reservation by nodes.
- Exchanges of control packets may be required for achieving time synchronization ng nodes.

Hidden and exposed terminal problems

- The hidden terminal problem refers to the collision of packets at a receiving node to the simultaneous transmission of those nodes that are not within the direct smission range of the sender but are within the transmission range of the receiver.
- Collision occurs when both nodes transmit packets at the same time without ning about the transmission of each other .

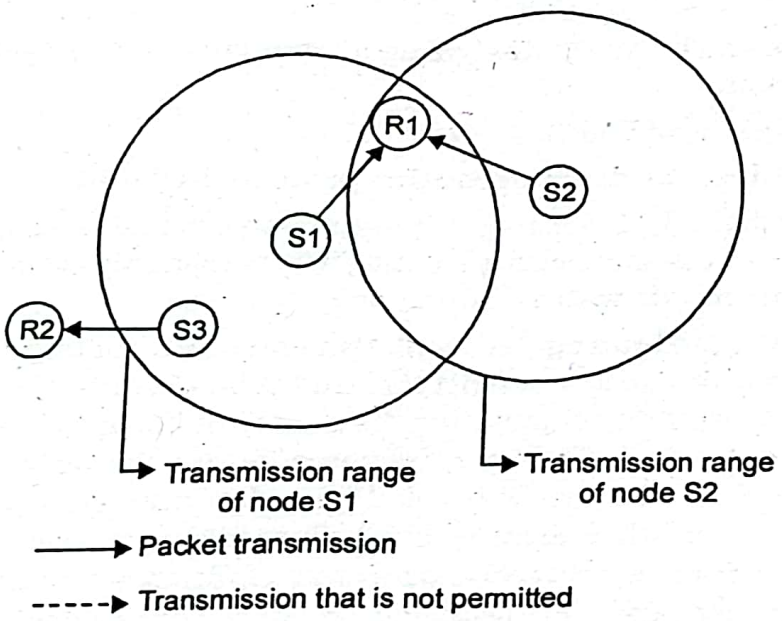


Fig. Hidden and exposed terminal problems

and S2 are hidden from each other & they transmit simultaneously to R1 which collision.

• The exposed terminal problem refers to the inability of a node, which is blocked due to transmission by a nearby transmitting node, to transmit to another node.

• If S1 is already transmitting to R1, then S3 cannot interfere with on-going transmission & it cannot transmit to R2.

• The hidden & exposed terminal problems reduce the throughput of a network when traffic load is high.

Error-prone shared broadcast channel

• When a node is receiving data, no other node in its neighbourhood should transmit a node should get access to the shared medium only when its transmission do not affect any ongoing session.

• MAC protocol should grant channel access to nodes in such a manner that collision are minimized.

• Protocol should ensure fair BW allocation.

• Distributed nature/lack of central coordination.

• Do not have centralized coordinates.

• Nodes must be scheduled in a distributed fashion for gaining access to the channel.

• MAC protocol must make sure that additional overhead, in terms of BW consumption, incurred due to this control information is not very high.

• Mobility of nodes.

• Nodes are mobile most of the time.

• The protocol design must take this mobility factor into consideration so that the performance of the system is not affected due to node mobility.

Q. 3. (b) classify the MAC protocol and what are the advantages of reservation based MAC ptorocol over contention based MAC protocol? (6)

Ans. Refer Q. 3 (a) & (b) of End Term Exam Pg.14-2017.

UNIT-II

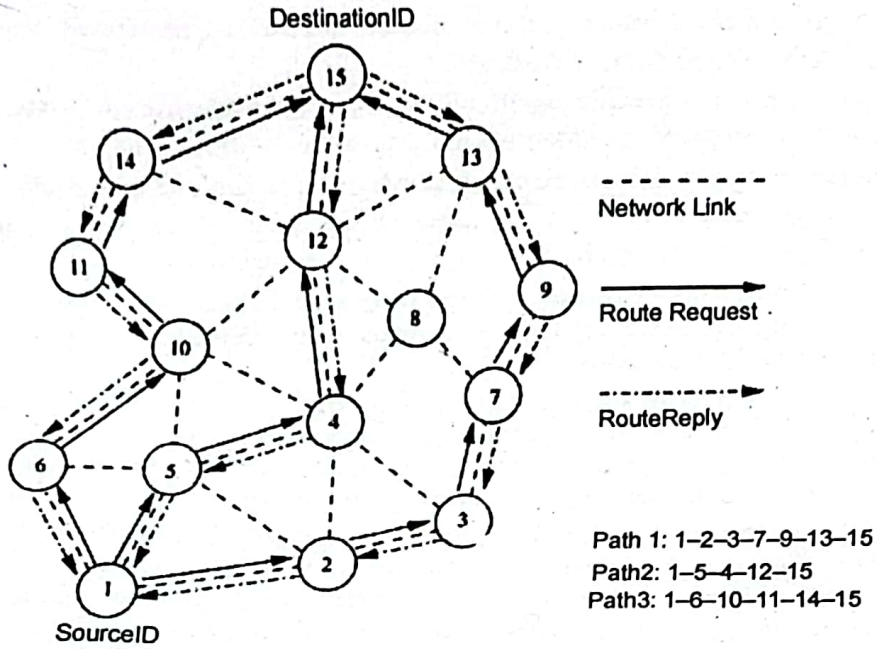
Q. 4. (a) List the issues in designing a transport layer protocol for Ad Hoc wireless networks. (6)

Ans. Refer Q.1. (e) of End Term Exam 2018.

Q. 4. (b) Explain the demand routing protocol in detail. (6.5)

Ans. Unlike the table-driven routing protocols, on-demand routing protocols execute the path-finding process and exchange routing information only when a path is required by a node to communicate with a destination

Dynamic Source Routing Protocol: Dynamic source routing protocol (DSR)is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The major difference between this and the other on demand routing protocols is that it is *beacon-less* and hence does not require periodic *hello*packet (*beacon*) transmissions, which are used by a node to inform its neighbors of its presence. The basic approach of this protocol (and all other on-demand routing protocols) during the route construction phase is to establish a route by flooding *RouteRequest* packets in the network. The destination node, on receiving a *RouteRequest* packet, responds by sending a *RouteReply* packet back to the source, which carries the route traversed by the *RouteRequest* packet received.



Ad Hoc On-Demand Distance-Vector Routing Protocol:

Ad hoc on-demand distance vector (AODV) routing protocol uses an on demand proach for finding routes, that is, a route is established only when it is required by a rce node for transmitting data packets. It employs destination sequence numbers to ntify the most recent path. The major difference between AODV and DSR stems out n the fact that DSR uses source routing in which a data packet carries the complete h to be traversed. However, in AODV, the source node and the intermediate nodes e the next-hop information corresponding to each flow for data packet transmission. n ondemand routing protocol, the source node floods the *RouteRequest* packet in the ork when a route is not available for the desired destination. It may obtain multiple es to different destinations from a single *RouteRequest*. The major difference between V and other on-demand routing protocols is that it uses a destination sequence ber (DestSeqNum) to determine an up-to-date path to the destination. A node es its path information only if the DestSeqNum of the current packet received is r than the last DestSeqNum stored at the node.

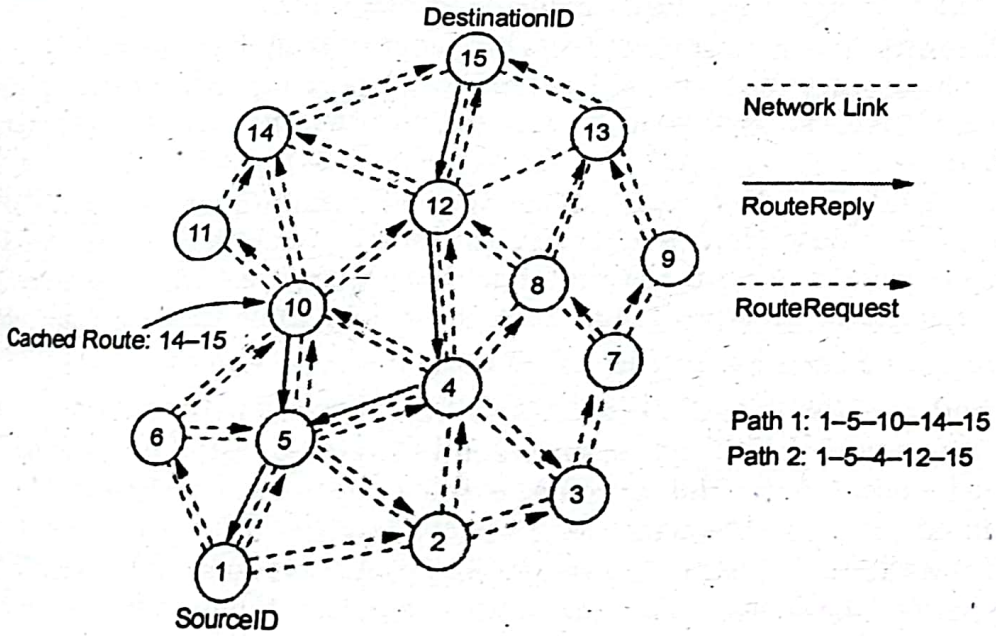


Fig. 2

Q.5 (a) Describe the types of ad hoc network routing protocol based on the routing information update mechanism. **(6)**

Ans. Ad hoc wireless network routing protocols can be classified into three major categories based on the routing information update mechanism. They are:

1. Proactive or table-driven routing protocols: In table-driven routing protocols, every node maintains the network topology information in the form of routing tables by periodically exchanging routing information.

Routing information is generally flooded in the whole network. Whenever a node requires a path to a destination, it runs an appropriate path-finding algorithm on the topology information it maintains.

2. Reactive or on-demand routing protocols: Protocols that fall under this category do not maintain the network topology information. They obtain the necessary path when it is required, by using a connection establishment process. Hence these protocols do not exchange routing information periodically.

3. Hybrid routing protocols: Protocols belonging to this category combine the best features of the above two categories. Nodes within a certain distance from the node concerned, or within a particular geographical region, are said to be within the routing zone of the given node. For routing within this zone, a table-driven approach is used. For nodes that are located beyond this zone, an on-demand approach is used.

Q.5. (b) Why secure routing protocols are needed? List the issues and challenges in security provision of transport layer. **(6.5)**

Ans. Due to the unique characteristics of ad hoc wireless networks, such networks are highly vulnerable to security attacks compared to wired networks or infrastructure-based wireless networks. A security protocol for ad hoc wireless networks should satisfy the following requirements.

- **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.
- **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.
- **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.
- **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.

The issues and challenges in secure routing of ad hoc wireless networks are

- **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.

• **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.

• **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.

• **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.

• **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.

• **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.

UNIT-III

Q. 6 (a) Discuss the mechanism for location discovery. **(6)**

Ans. The location information of sensors has to be considered during aggregation of sensed data. This implies each node should know its location and couple its location information with the data in the messages it sends. A low-power, inexpensive, and reasonably accurate mechanism is needed for location discovery. A global positioning system (GPS) is not always feasible because it cannot reach nodes in dense foliage or indoors. It also consumes high power and makes sensor nodes bulkier. Two basic mechanisms of location discovery are

Indoor Localization: Indoor localization techniques use a fixed infrastructure to estimate the location of sensor nodes. Fixed beacon nodes are strategically placed in the field of observation, typically indoors, such as within a building. The randomly distributed sensors receive beacon signals from the beacon nodes and measure the signal strength, angle of arrival, and time difference between the arrival of different beacon signals. Using the measurements from multiple beacons, the nodes estimate their location. Some approaches use simple triangulation methods, while others require a preliminary database creation of signal measurements. The nodes estimate distances by looking up the database instead of performing computations. However, storage of the database may not be possible in each node, so only the BS may carry the database.

Sensor Network Localization: In situations where there is no fixed infrastructure available and prior measurements are not possible, some of the sensor nodes themselves become beacons. They have their location information, using GPS, and these send periodic beacons to other nodes. In the case of communication using RF signals, the received signal strength indicator (RSSI) can be used to estimate the distance, but this is very sensitive to obstacles and environmental conditions. Alternatively, the time difference between beacon arrivals from different nodes can be used to estimate location, if RF or ultrasound signals are used for communication. This offers a lower range of estimation than RSSI, but is of greater accuracy.

Q.6. (b) What are various design challenges in mobile Ad Hoc network and wireless sensor networks. **(6.5)**

Ans. Wireless Sensor Networks

• Sensor networks are special category of Adhoc wireless network that are used to provide a wireless communication infrastructure among the sensors deployed in a specific application domain.

• Sensor nodes are tiny devices that have capability of sensing physical parameters processing the data gathered, & communication to the monitoring system.

The issue that make sensor network a distinct category of adhoc wireless network are the following:

1. Mobility of nodes

• Mobility of nodes is not a mandatory requirement in sensor networks.

• For example, the nodes used for periodic monitoring of soil properties are not required to be mobile & the nodes that are fitted on the bodies of patients in a post-surgery ward of a hospital are designed to support limited or partial mobility.

• In general, sensor networks need not in all cases be designed to support mobility of sensor nodes.

2. Size of the network

The number of nodes in sensor network can be much larger than that in a typical ad hoc wireless network.

3. Density of deployment

The density of nodes in a sensor network varies with the domain of application. For example, Military applications require high availability of the network, making redundancy a high priority.

4. Power constraints

The power constraints in sensor networks are much more stringent than those in ad hoc wireless networks. This is mainly because the sensor nodes are expected to operate in harsh environmental or geographical conditions, with minimum or no human supervision and maintenance.

In certain case, the recharging of the energy source is impossible:

• Running such a network, with nodes powered by a battery source with limited energy, demands very efficient protocol at network, data link, and physical layer.

The power sources used in sensor networks can be classified into the following three categories:

1. Replenishable Power source: The power source can be replaced when the existing source is fully drained.

2. Non-replenishable Power source: The power source cannot be replenished once the network has been deployed. The replacement of sensor node is the only solution.

3. Regenerative Power source: Here, power source employed in sensor network have the capability of regenerating power from the physical parameter under measurement.

5. Data/Information fusion

• Data fusion refers to the aggregation of multiple packets into one before relaying it.

• Data fusion mainly aims at reducing the bandwidth consumed by redundant headers of the packets and reducing the media access delay involved in transmitting multiple packets.

• Information fusion aims at processing the sensed data at the intermediate nodes nd relaying the outcome to the monitor node.

6. Traffic Distribution

• The communication traffic pattern varies with the domain of application in sensor etworks.

• For example, the environmental sensing application generates short periodic ackets indicating the status of the environmental parameter under observation to a ntral monitoring station.

• This kind of traffic requires low bandwith.

• Ad hoc wireless networks generally carry user traffic such as digitized & packetized oice stream or data traffic, which demands higher bandwidth.

Issues in ADHOC Wireless Netoworks

The major issues that affect the design, deployment, & performance of an ad hoc ireless network system are:

1. Medium Access Scheme.
2. Transport Layer Protocol.
3. Routing.
4. Multicasting.
5. Energy Management.
6. Self-Organisation.
7. Security.
8. Addressing & Service discovery.
9. Deployment considerations.
10. Scalability.
11. Pricing Scheme.
12. Quality of Service Provisioning.

Q.7. (a) What is hybrid rouling protocol? Describe hybrid routing protocol. **(6)**

Ans. Refer Q.7. (b) of End Term Exam Pg. 26-2017.

Q.7. (b) Explain the security issues in ad hoc wireless network. **(6.5)**

Ans. The issues and challenges in security of ad hoc wireless networks are.

• **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.

• **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.

• **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.

• **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.

• **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.

• **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.

UNIT-IV

Q.8. What is wireless geolocation? Discuss the technologies and standards for wirelesss gelocation. **(6.5)**

Ans. Refer Q.8 of End Term Exam Pg. 27-2017.

Q.9. Explain the following.

Q.9. (a) Wireless fidelity systems **(6)**

Ans. Refer Q.9 (a) of End Term Exam Pg. 29-2017.

Q.9. (b) Vehicular Sensor Networks:

Ans. Vehicular Sensor Networks (VASNET) inherits its characteristics from both Wireless Sensor Networks (WSN) and Vehicular Ad Hoc Networks (VANET). There is no infrastructure for VANET, therefore the vehicular nodes do perform data collection as well as data routing. Therefore, the necessity of designing a new architecture to overcome the mentioned challenges is transpicuous. VASNET is a fusion of WSNs and MANET, which can be divided in to three layers. The upper layer consisting of traffic monitor stations, e.g. traffic police located at the cities. These are connected by either fiber optic cables to form the backbone of traffic information network. The middle layer is region layer, consisting of traffic check post located through highways. These stations can be connected via the Internet or local networks, and finally the lower layer is the field layer, consisting of WSN nodes deployed on beside the highway and onboard sensors which are carried by the vehicles. These nodes are connected by short-range or medium-range wireless communication. The components are as follows:

(1) Vehicular Sensor Nodes; which are carried by the vehicles. These nodes are supposed to sense the real phenomena e.g. the velocity of the vehicle. The sensor readings are to be sent to the base stations via RSS nodes. These nodes can communicate with each other or the roadside sensor via short-range communication.

(2) Road Side Sensors (RSS); are deployed in a fixed distance beside the road. RSSs act as cluster heads for vehicular nodes. RSS nodes receive the data from mobile nodes and retransmit towards the BSs. These nodes are equipped with two kinds of antenna, unidirectional and bidirectional. Unidirectional antenna is for broadcasting and directional antenna are intended for geo-casting. We need to satisfy the following requirements for deploying the sensor nodes on a road side, such as; (a) high reliability, (b) long time service and (c) high real time.

(3) Base Station (BS); are Police Traffic Control Check-Post, Rescue Team Buildings or Fire Fighting Stations in some fixed point trough the roads. We can have mobile BS like, Traffic Police patrolling team, Firefighting Truck, or ambulance.

FIRST TERM EXAMINATION [FEB. 2019]
EIGHTH SEMESTER [B.TECH]
AD HOC AND SENSOR NETWORK [ETEC–406]

me : 1.5 hrs. M.M. : 30

te: *Attempt Q. 1. is compulsory and any two more questions.*

Q.1. (a) Explain different characteristics of adhoc networks. (2.5)

Ans. Features of ad hoc networks are listed below

Autonomous behaviour: In ad hoc networks, each node acts as both host and router. ach node has autonomy to be

Multi-hop radio relaying: Ad hoc networks are capable of multi-hop routing when source node and a destination node for a data transmission are out of the radio range.

Decentralized control: In ad hoc networks there is distributed nature of operation r security, routing and host configuration. A centralized control is missing.

Dynamic topology: The nodes can join or leave the network anytime, making the twork topology dynamic in nature.

Limited bandwidth: The reliability, efficiency, stability, and capacity of wireless nks are often inferior when compared with wired links. This shows the fluctuating link ndwidth of wireless links.

Mobility: In ad hoc networks nodes are highly mobile.

Collaborative computing: There are intermediate nodes which will act as relays or the data that is sent by the source node to be delivered to the intended destination

Q.1. (b) Differentiate cellular and Ad hoc wireless networks. (2.5)

Ans.

Cellular Netowrks	Ad HOC Wireless Networks
(a) Fixed infrastructure-based	(a) Infrastructure-less
(b) Single-hop wireless links	(b) Multi-hop wireless links
(c) Guaranteed bandwidth (designed for voice traffic)	(c) Shared radio channel (more suitable for best-effort data traffic)
(d) Centralized routing	(d) Distributed routing
(e) Circuit-switched (evolveing toward packet switching)	(e) Packet-switched (evolving toward emulation of circuit switching)
(f) Seamless connectivity (low call drops during handoffs)	(f) Frequent path breaks due to mobility
(g) High cost and time of deployment	(g) Quick and cost-effective deployment
(h) Reuse of frequency spectrum through geographical channel reuse	(h) Dynamic frequency reuse based on carrier sense mechnism
(i) Easier to achieve time synchronization	(i) Time synchronization is difficult and consumes bandwidth
(j) Easier to employ bandwidth reservation	(j) Bandwidth reservation requires complex medium access control protocols
(k) Application domains include mainly civilian and commerical sectors	(k) Application domains include battle-fields, emergency search and resue operations, and collaborative computing.

(l) High cost of network maintenance (backup power source, staffing etc.)	(l) Self-organization and maintenance properties are built into the network
(m) Mobile losts are of relatively low complexity	(m) Mobile hosts require more intelligence (should have a transceiver as well as routing/switching capability)
(n) Major goals of routing and call admission are to maximize the call acceptance ratio and minimize the call drop ratio	(n) Main aim of routing is to find paths with minimum overhead and also quick reconfiguration of broken paths
(o) Widely deployed and currently in the third generation of evolution	(o) Several issues are to be addressed for successful commercial deployment even though widespread use exists in defense

Q.1. (c) What are the issues in adhoc and sensor networks? **(2.5)**

Ans. The major issues that affect the design, deployment, and performance of an ad hoc wireless network system are :

- Medium Access Scheme.
- Transport Layer Protocol.
- Routing.
- Multicasting.
- Energy Management.
- Self-Organization.
- Security.
- Addressing & Service discovery.
- Deployment considerations.
- Scalability.
- Pricing Scheme.
- Quality of Service Provision

Q.1. (d) Explain the different application areas of adhoc wireless network. **(2.5)**

Ans. Refer to Q.1. of End Term Examination 2017.

Q.2. What are the different issues in the designing of MAC protocol for Adhoc wireless network ? **(10)**

Ans. The main issues in designing MAC protocol for ad hoc wireless network are:

Bandwidth efficiency

- Bandwidth must be utilized in efficient manner.
- Minimal Control overhead
- BW = ratio of BW used for actual data transmission to the total available BW.

Quality of service support

- Essential for supporting time-critical traffic sessions.
- They have resource reservation mechanism that takes into considerations the nature of wireless.
- Channel and the mobility of nodes.

Synchronization

- MAC protocol must consider synchronization between nodes in the network.
- Synchronization is very important for BW (time slot) reservation by nodes.
- Exchanges of control packets may be requried for achieving time synchronization among nodes.

ıidden and exposed terminal problems

• The hidden terminal problem refers to the collision of packets at a receiving node ıue to the simultaneous transmission of those nodes that are not within the direct ransmission range of the sender but are within the transmission range of the receiver.

• Collision occurs when both nodes transmit packets at the same time without nowing about the transmission of each other

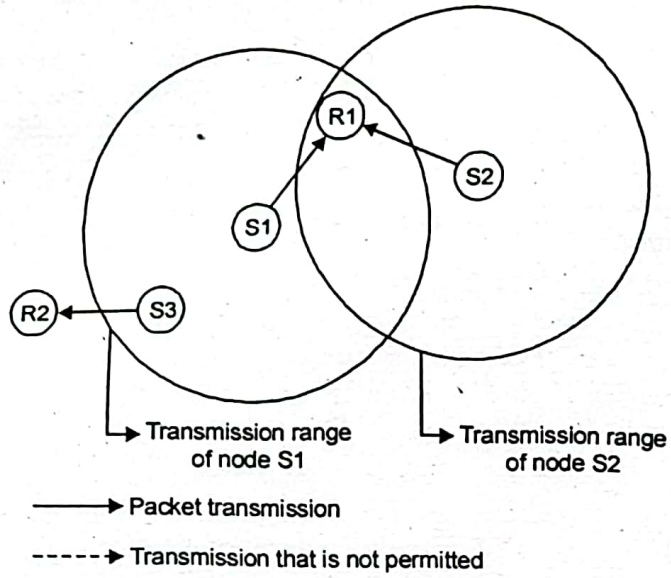


Fig.1. Hidden and exposed terminal problems

• S1 and S2 are hidden from each other & they transmit simultaneously to R1 ich leads to collision.

• The exposed terminal problem refers to the inability of a node, which is blocked ; to transmission by a nearby transmitting node, to transmit to another node.

• If S1 is already transmitting to R1, then S3 cannot interfere with on-going nsmission & it cannot transmit to R2.

• The hidden & exposed terminal problems reduce the throughput of a network en traffic load is high.

:or-prone shared broadcast channel

• When a node is receiving data, no other node in its neighbourhood should transmit ɔde should get access to the shared medium only when its transmission do not affect ' ongoing session.

• MAC protocol should grant channel access to nodes in such a manner that collision minimized.

• Protocol should ensure fair BW allocation.

• Distributed nature/lack of central coordination.

• Do not have centralized coordinates.

• Nodes must be scheduled in a distributed fashion for gaining access to the channel.

• MAC protocol must make sure that additional overhead, in terms of BW sumption, incurred due to this control information is not very high.

• Mobility of nodes.

• Nodes are mobile most of the time.

• The protocol design must take this mobility factor into consideration so that the ormance of the system is not affected due to node mobility.

Q.3. Give a detail classification of MAC protocol for adhoc wireless network l explain any two protocols in details. **(10)**

Ans. MAC protocols for ad hoc wireless networks can be classified into several categories based on various criteria such as initiation approach, time synchronization, and reservation approaches. Ad hoc network MAC protocols can be classified into three basic types:

- Contention-based protocols
- Contention-based protocols with reservation mechanisms
- Contention-based protocols with scheduling mechanisms

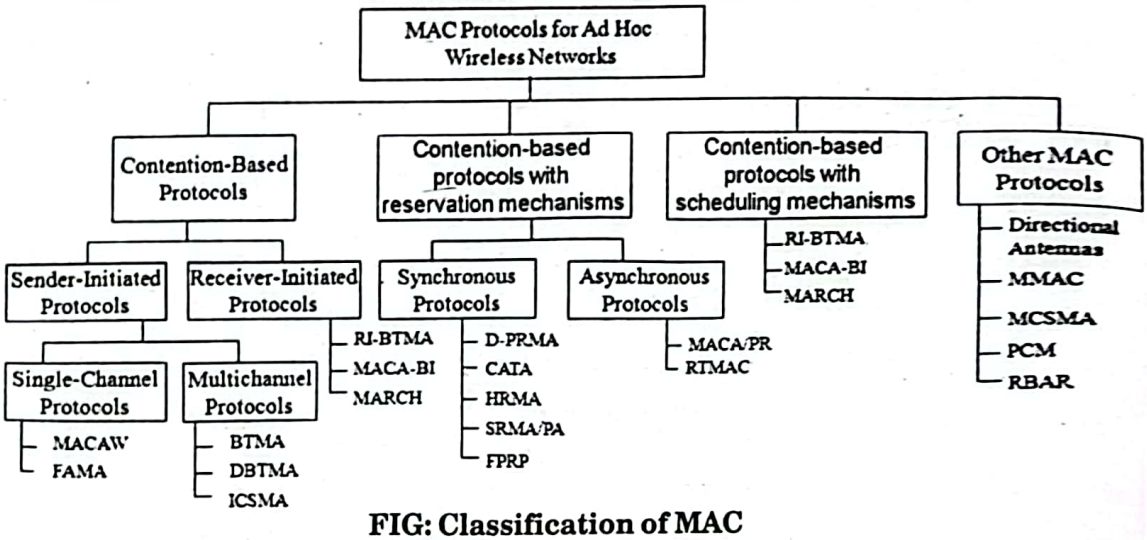


FIG: Classification of MAC

Contention-based protocols

- Sender-initiated protocols: Packet transmissions are initiated by the sender node.
- Single-channel sender-initiated protocols: A node that wins the contention to the channel can make use of the entire bandwidth.
- Multichannel sender-initiated protocols: The available bandwidth is divided into multiple channels.
- Receiver-initiated protocols: The receiver node initiates the contention resolution protocol.

Contention-based protocols with reservation mechanisms

- Synchronous protocols: All nodes need to be synchronized. Global time synchronization is difficult to achieve.
- Asynchronous protocols: These protocols use relative time information for effecting reservations.

Contention-based protocols with scheduling mechanisms

- Node scheduling is done in a manner so that all nodes are treated fairly and no node is starved of bandwidth.
- Scheduling-based schemes are also used for enforcing priorities among flows whose packets are queued at nodes.
- Some scheduling schemes also consider battery characteristics.

Q.4. What are designing issues in routing protocol for ad hoc wireless network? Explain any one table driven routing protocol. (10)

Ans. The major challenges that a routing protocol designed for ad hoc wireless networks faces are mobility of nodes, resource constraints, error-prone channel state, and hidden and exposed terminal problems.

- **Mobility:** The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes, hence an on-going session suffers frequent path breaks. Disruption occurs either due to the movement of the intermediate nodes in the path or due to the movement of end nodes.

• **Bandwidth Constraint:** Limited bandwidth

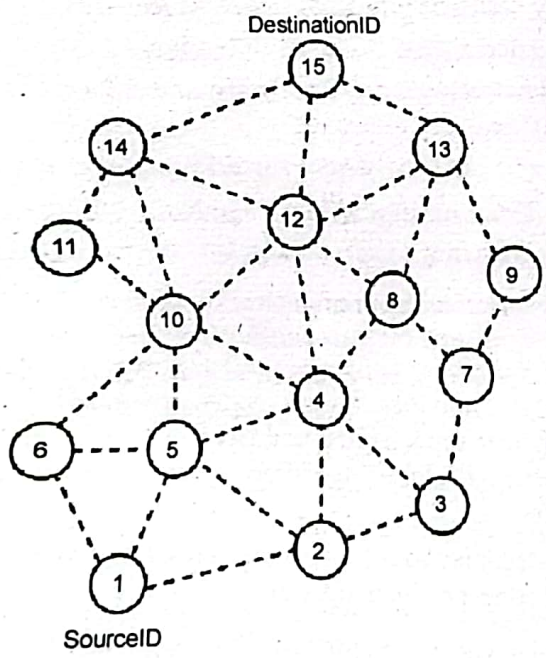
• Error-Prone Shared Broadcast Radio Channel

The broadcast nature of the radio channel poses a unique challenge in ad hoc less networks. The wireless links have time-varying characteristics in terms of link city and link-error probability.

• Hidden and Exposed Terminal Problems

The hidden terminal problem refers to the collision of packets at a receiving node to the simultaneous transmission of those nodes that are not within the direct smission range of the sender, but are within the transmission range of the receiver.

Destination Sequenced Distance-Vector Routing Protocol: As it is a table-driven ing protocol, routes to all destinations are readily available at every node at all times. tables are exchanged between neighbors at regular intervals to keep an up-to-date of the network topology. The tables are also forwarded if a node observes a significant ge in local topology. The table updates are of two types: incremental updates and full ps. An incremental update takes a single network data packet unit (NDPU), while a lump may take multiple NDPUs. Incremental updates are used when a node does bserve significant changes in the local topology. A full dump is done either when the topology changes significantly or when an incremental update requires more than a e NDPU. Table updates are initiated by a destination with a new sequence number h is always greater than the previous one. Upon receiving an updated table, a node r updates its tables based on the received information or holds it for some time to t the best metric (which may be the lowest number of hops) received from multiple ons of the same update table from different neighboring nodes. Based on the sequence ber of the table update, it may forward or reject the table. Consider the example as n in Figure Here node 1 is the source node and node 15 is the destination. As all the s maintain global topology information, the route is already available as shown in Figure. the routing table of node 1 indicates that the shortest route to the destination node



(a) Topology graph of the network

Dest	NextNode	Dist	Seq.No.
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

(b) Routing table for Node 1

END TERM EXAMINATION [MAY. 2019]
EIGHTH SEMESTER [B.TECH]
AD HOC AND SENSOR NETWORK [ETEC–06]

Time : 3 hrs. **M.M. : 75**

Note: *Attempt five questions in all including Q. 1. which is compulsory. Select one question from each unit.*

Q.1. (a) Define and explain the ad hoc network. Why ad hoc networks are needed? **(4)**

Ans. Ad hoc wireless networks are defined as the category of wireless networks that utilize multi-hop radio relaying and are capable of operating without the support of any fixed infrastructure (hence they are also called infrastructure less networks). The absence of any central coordinator or base station makes the routing a complex one compared to cellular networks.

Advantages of Ad Hoc Network: The rapid development in ad hoc technology is widely used in portable computing such as laptop, mobile phone used to access the web services, telephone calls when the user are in travelling. Development of self-organizing network decrease the communication cost. The growth of 4G technology enhances anytime, anywhere, anyhow communication in ad hoc network. Ad hoc network is simple to design and install. The advantages of an ad hoc network include: Separation from central network administration.

- Self-configuring nodes are also routers.
- Self-healing through continuous re-configuration.
- Scalability incorporates the addition of more nodes.
- Mobility allows ad hoc networks created on the fly in any situation where there are multiple wireless devices.
- Flexible ad hoc can be temporarily setup at anytime, in any place.
- Lower getting-started costs due to decentralized administration.
- The nodes in ad hoc network need not rely on any hardware and software. So, it can be connected and communicated quickly.

Q.1. (b) List the issues of designing a MAC protocol for ad hoc networks. **(4)**

Ans. Refer to Q.1. (b) of First Term Examination 2018. (Page No. 1-2018)

Q.1. (c) Relate the Sensor network with ad hoc network. **(4)**

Ans. While both ad hoc wireless networks and sensor networks consist of wireless nodes communicating with each other, there are certain challenges posed by sensor networks. The number of nodes in a sensor network can be several orders of magnitude larger than the number of nodes in an ad hoc network. Sensor nodes are more prone to failure and energy drain, and their battery sources are usually not replaceable or rechargeable. Sensor nodes may not have unique global identifiers, so unique addressing is not always feasible in sensor networks.

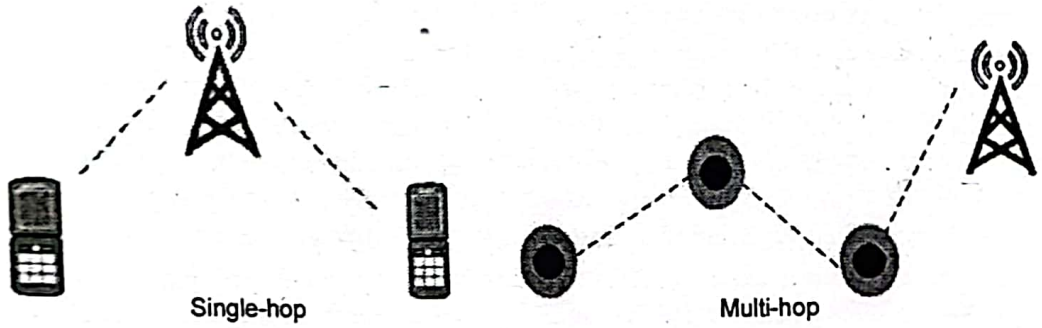
Sensor networks are data-centric, that is, the queries in sensor networks are addressed to nodes which have data satisfying some conditions.

On the other hand, ad hoc networks are address-centric, with queries addressed to particular nodes specified by their unique address. Hence, sensor networks require a different mechanism for routing and answering queries. Most routing protocols used in

ad hoc networks cannot be directly ported to sensor networks because of limitations in memory, power, and processing capabilities in the sensor nodes and the non-scalable nature of the protocols. An important feature of sensor networks is data fusion/ aggregation, whereby the sensor nodes aggregate the local information before relaying. The main goals of data fusion are to reduce bandwidth consumption, media access delay, and power consumption for communication.

Q.1. (d) What multihop wireless communication is required for WSN? Explain. **(4)**

Ans. Ad hoc networks are mainly based upon principle of 'multi-hop relaying'. In a multi-hop network, a data packet has to go through many nodes in order to reach its destination address. Basically the intermediate nodes can act as the peer nodes and these peer nodes can take part in transmitting the information from the source node to the destination node. These networks are self-organizing and self-configuring. If the destination node is not within the direct transmission range of the source node, then the source node will have to take help of some of the intermediate nodes in order to be able to send the data from it to the destination node. This is called multi-hoping relaying.



Q.1. (e) Why does TCP not work well in ad hoc network? Discuss. **(4)**

Ans. The major reasons behind throughput degradation that TCP faces when used in ad hoc wireless networks are the following:

- **Misinterpretation of packet loss:** Traditional TCP was designed for wired networks where the packet loss is mainly attributed to network congestion. Network congestion is detected by the sender's packet RTO period. Once a packet loss is detected, the sender node assumes congestion in the network and invokes a congestion control algorithm.

- **Frequent path breaks:** Ad hoc wireless networks experience dynamic changes in network topology because of the unrestricted mobility of the nodes in the network. The topology changes lead to frequent changes in the connectivity of wireless links and hence the route to a particular destination may need to be recomputed very often.

- **Effect of path length:** It is found that the TCP throughput degrades rapidly with an increase in path length in string (linear chain) topology ad hoc wireless networks.

- **Misinterpretation of congestion window:** TCP considers the congestion window as a measure of the rate of transmission that is acceptable to the network and the receiver. In ad hoc wireless networks, the congestion control mechanism is invoked when the network gets partitioned or when a path break occurs

• **Asymmetric link behavior:** The radio channel used in ad hoc wireless networks has different properties such as location-dependent contention, environmental effects on propagation, and directional properties leading to asymmetric links. The directional links can result in delivery of a packet to a node, but failure in the delivery of the acknowledgment back to the sender.

Q.1. (f) Explain 802.11g IEEE standard. (5)

Ans. IEEE 802.11g was one of the main Wi-Fi standards to follow on from 802.11a and 802.11b. It built on the performance and played a pivotal role in further establishing Wi-Fi as a major wireless standard.

IEEE 802.11g had the advantage that it could support the high data speeds using 2.4 GHz which had previously only attainable using 802.11a within the 5GHz ISM band.

The lower cost of chips using 2.4GHz combined with the higher speed meant that for many years it became the dominant Wi-Fi technology.

It is an amendment to the IEEE 802.11 specification that operates in the 2.4 GHz microwave band. The standard has extended throughput to up to 54 Mbit/s using the same 20MHz bandwidth as 802.11b uses to achieve 11 Mbit/s. This specification under the marketing name of Wi-Fi has been implemented all over the world

UNIT-I

Q.2. (a) Summarize about the schedule based MAC protocols in WSN. (6)

Ans. These protocols focus on packet scheduling at nodes, and also scheduling nodes for access to the channel. Node scheduling is done in a manner so that all nodes are treated fairly and no node is starved of bandwidth. Scheduling-based schemes are also used for enforcing priorities among flows whose packets are queued at nodes. Some scheduling schemes also take into consideration battery characteristics, such as remaining battery power, while scheduling nodes for access to the channel.

Distributed Priority Scheduling and Medium Access in Ad Hoc Networks

The first technique, called distributed priority scheduling (DPS), piggy-backs the priority tag of a node's current and head-of-line packets on the control and data packets. By retrieving information from such packets transmitted in its neighborhood, a node builds a scheduling table from which it determines its rank (information regarding its position as per the priority of the packet to be transmitted next) compared to other nodes in its neighborhood. This rank is incorporated into the back-off calculation mechanism in order to provide an approximate schedule based on the ranks of the nodes. The seccnd scheme, called multi-hop coordination, extends the DPS scheme to carry out scheduling over multi-hop paths. The downstream nodes in the path to the destination increase the relative priority of a packet in order to compensate for the excessive delays incurred by the packet at the upstream nodes.

Distributed Priority Scheduling: The distributed priority scheduling scheme (DPS) is based on the IEEE 802.11 distributed coordination function. DPS uses the same basic RTS-CTS-DATA-ACK packet exchange mechanism. The RTS packet transmitted by a ready node carries the priority tag/priority index for the current DATA packet to be transmitted. The priority tag can be the delay target for the DATA packet. On receiving the RTS packet, the intended receiver node responds with a CTS packet. The receiver node copies the priority tag from the received RTS packet and piggybacks it along with the source node id, on the CTS packet. Neighbor nodes receiving theRTS or CTS packets (including the hidden nodes) retrieve the piggy-backed priority tag information and make a corresponding entry for the packet to be transmitted, in their scheduling tables (STs). Each node maintains an ST holding information about packets, which were originally piggy-backed on control and data packets. The entries in the ST

e ordered according to their priority tag values. When the source node transmits a ATA packet, its head-of-line packet information (consisting of the destination and urce ids along with the priority tag) is piggy-backed on the DATA packet (head-of-ne packet of a node refers to the packet to be transmitted next by the node).

Q.2. (b) List and explain the approaches for power aware routing protocol. **(6.5)**

Ans. The limitation on the availability of power for operation is a significant ttleneck. Hence, the use of routing metrics contributes to the efficient utilization of ergy and increases the lifetime of the network.

Minimal energy consumption per packet

- This metric aims at minimizing the power consumed by a packet in traversing om source node to the destination node.
- The energy consumed by a packet when traversing through a path is the sum of e energies required at every intermediate hop in that path.
- This metric doesn't balance the load
- Disadvantages
- Selection of path with large hop length
- Inability to measure the power consumption in advance
- Inability to prevent the fast discharging of batteries at some nodes

Maximize network connectivity

- This metric attempt to balance the routing load among the cut set (the subset of e nodes in the network, the removal of which results in network partitions).
- It is difficult to achieve a uniform battery draining rate for the cut set.

Maximum variance in Node power levels

- This metric proposes to distribute the load among all nodes in the network so at the power consumption pattern remains uniform across them.
- This problem is very complex when the rate and size of the data packets vary

Minimum cost per packet

- In order to maximize the life of every node in the network, this routing metric is ade as a function of the state of the node's battery.
- A node's cost decreases with an increase in its battery change and vice versa.
- Cost of node can be easily computed
- Advantage congestion handling & cost calculation

Minimize maximum node cost

- This metric minimizes the maximum cost per node for a packet after routing a umber of packets or after a specific period.
- This delays the failure of a node, occurring due to higher discharge because of acket forwarding

Q.3. (a) Explain design challenge in Ad hoc and Sensor Networks. **(6)**

Ans. Refer Q.6 (b) of End Term Examination 2018. (Page No. 14-2018)

Q.3. (b) Explain the contention based protocols with scheduling and eservation in detail. **(6.5)**

Ans. Refer Q.2 (b) of End Term Examination 2017. (Page No. 13-2017)

UNIT-II

Q.4. (a) Define wireless sensor networks. Discuss the components present in sensor Networks. **(4)**

Ans. The main components of a sensor node are a microcontroller, transceiver, external memory, power source and one or more transducers (sensors).

Controller: The controller performs tasks, processes data and controls the functionality of other components in the sensor node. While the most common controller is a microcontroller, other alternatives that can be used as a controller are: a general purpose desktop microprocessor, digital signal processors, FPGAs and ASICs.

Transceiver: Sensor nodes often make use of ISM band, which gives free radio, spectrum allocation and global availability. The possible choices of wireless transmission media are radio frequency (RF), optical communication (laser) and infrared. Lasers require less energy , but need line-of-sight for communication and are sensitive to atmospheric conditions. Infrared, like lasers, needs no antenna but it is limited in its broadcasting capacity.

External memory: From an energy perspective, the most relevant kinds of memory are the on-chip memory of a microcontroller and Flash memory—off-chip RAM is rarely, if ever, used. Flash memories are used due to their cost and storage capacity. Memory requirements are very much application dependent. Two categories of memory based on the purpose of storage are: user memory used for storing application related or personal data, and program memory used for programming the device. Program memory also contains identification data of the device if present.

Power source: A wireless sensor node is a popular solution when it is difficult or impossible to run a mains supply to the sensor node. However, since the wireless sensor node is often placed in a hard-to-reach location, changing the battery regularly can be costly and inconvenient. An important aspect in the development of a wireless sensor node is ensuring that there is always adequate energy available to power the system. The sensor node consumes power for sensing, communicating and data processing.

Sensors (Transducers): Sensors are used by wireless sensor nodes to capture data from their environment. They are hardware devices that produce a measurable response to a change in a physical condition like temperature or pressure. Sensors measure physical data of the parameter to be monitored and have specific characteristics such as accuracy, sensitivity etc. The continual analog signal produced by the sensors is digitized by an analog-to-digital converter and sent to controllers for further processing. Some sensors contain the necessary electronics to convert the raw signals into readings which can be retrieved via a digital link (e.g. I2C, SPI) and many convert to units such as °C. Most sensor nodes are small in size, consume little energy, operate in high volumetric densities, be autonomous and operate unattended, and be adaptive to the environment. As wireless sensor nodes are typically very small electronic devices, they can only be equipped with a limited power source of less than 0.5-2 ampere-hour and 1.2-3.7 volts.

Q.4. (b) List the advantages and disadvantages of DSDV routing protocols. **(4)**

Ans. Advantages and Disadvantages of DSDV routing protocol

The availability of routes to all destinations at all times implies that much less delay is involved in the route setup process. The mechanism of incremental updates with sequence number tags makes the existing wired network protocols adaptable to

ad hoc wireless networks. Hence, an existing wired network protocol can be applied to ad hoc wireless networks with many fewer modifications. The updates are propagated throughout the network in order to maintain an up-to-date view of the network topology at all the nodes. The updates due to broken links lead to a heavy control overhead during high mobility. Even a small network with high mobility or a large network with low mobility can completely choke the available bandwidth. Hence, this protocol suffers from excessive control overhead that is proportional to the number of nodes in the network and therefore is not scalable in ad hoc wireless networks, which have limited bandwidth and whose topologies are highly dynamic.

Another disadvantage of DSDV is that in order to obtain information about a particular destination node, a node has to wait for a table update message initiated by the same destination node. This delay could result in stale routing information at nodes.

Q.4. (c) Discuss issues and challenges in security provisioning of transport layer. (4.5)

Ans. Designing a foolproof security protocol for ad hoc wireless is a very challenging task.

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.

Insecure operational environment: The operating environments where ad hoc wireless networks are used may not always be secure.

Lack of central authority: In wired networks and infrastructure-based wireless networks, it would be possible to monitor the traffic on then network through certain important central points (such as routers, base stations, and access points) and implement security mechanisms at such points.

Lack of association: Since these networks are dynamic in nature, a node can join or leave the network at any point of the time Limited resource availability: Resources such as bandwidth, battery power, and computational power (to a certain extent) are scarce in ad hoc wireless networks.

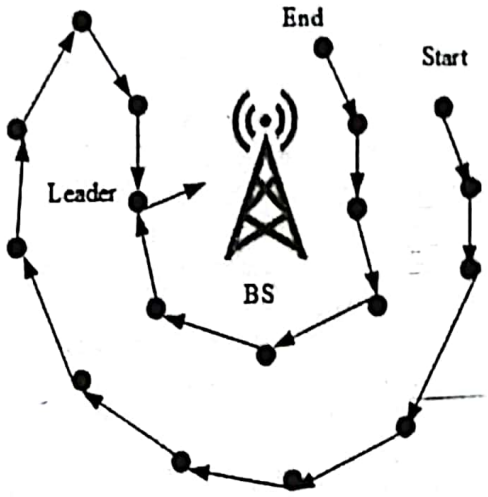
Physical vulnerability: Nodes in these networks are usually compact and hand-held in nature

Q.5. (a) Summarize the power management techniques in WSN. List the approaches for power aware routing protocol. (6)

Ans. Power-Efficient Gathering for Sensor Information Systems

It is data-gathering protocol based on the assumption that all sensor nodes know the location of every other node, that is, the topology information is available to all nodes. Also, any node has the required transmission range to reach the BS in one hop, when it is selected as a leader.

A greedy algorithm is used to construct a chain of sensor nodes, starting from the node farthest from the BS. At each step, the nearest neighbor which has not been visited is added to the chain. The chain is constructed a priori, before data transmission begins, and is reconstructed when nodes die out. At every node, data fusion or aggregation is carried out, so that only one message is passed on from one node to the next. A node which is designated as the leader finally transmits one message to the BS. Leadership is transferred in sequential order, and a token is passed so that the nodes know in which direction to pass messages in order to reach the leader.



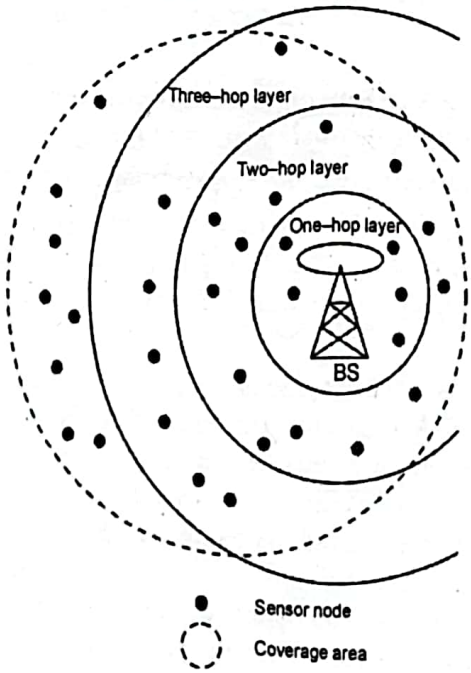
Q.5. (b) Discuss the classification of routing protocols based on the routing information update mechanism. **(6.5)**

Ans. Refer Q.5 (a) of End Term Examination 2018. (Page No. 12-2018)

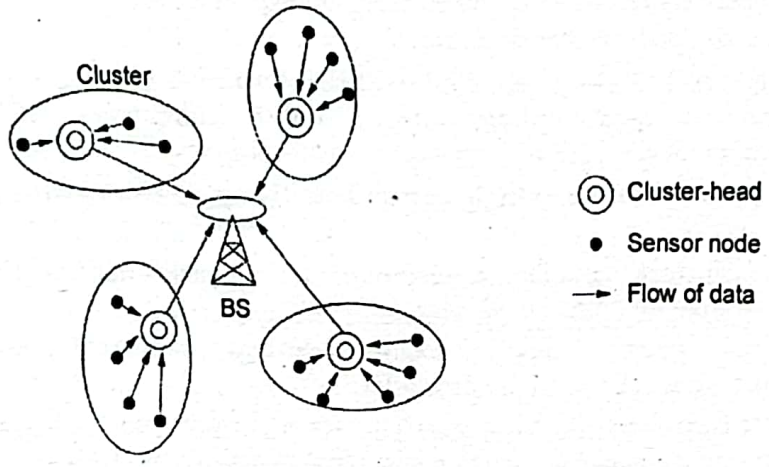
UNIT-III

Q.6. (a) Explain WSN Network architecture with sensor operations. **(6.5)**

Ans. The two basic kinds of sensor network architecture are layered and clustered. A layered architecture has a single powerful base station (BS), and the layers of sensor nodes around it correspond to the nodes that have the same hop-count to the BS. Layered architectures have been used with in-building wireless backbones, and in military sensor-based infrastructure, such as the multi-hop infrastructure network architecture (MINA). The users of the network have hand-held devices such as PDAs which communicate via the small nodes to the BS. Similarly, in a military operation, the BS is a data-gathering and processing entity with communication link to a larger network. A set of wireless sensor nodes is accessed by the hand-held devices of the soldiers. The advantage of a layered architecture is that each node is involved only in short-distance, low-power transmissions to nodes of the neighboring layers.



A clustered architecture organizes the sensor nodes into clusters, each governed by a cluster-head. The nodes in each cluster are involved in message exchanges with their respective cluster-heads, and these heads send messages to a BS, which is usually an access point connected to a wired network. Clustered architecture is especially useful for sensor networks because of its inherent suitability for data fusion. The data gathered by all members of the cluster can be fused at the cluster-head, and only the resulting information needs to be communicated to the BS. Sensor networks should be self-organizing, hence the cluster formation and election of cluster-heads must be an autonomous, distributed process. This is achieved through network layer protocols such as the low-energy adaptive clustering hierarchy (LEACH)



Q.6. (b) Highlight the salient feature in location based routing. **(6)**

Ans. Location based routing protocols are used in Wireless Sensor Network (WSN) in which the information about the location of nodes is used for communication. It is also known as geographic routing protocol or position based routing protocols. These protocols reduce the energy consumption and increase the lifetime of the network. As these are based on location information, it saves a lot of energy and also increase the lifetime of network. Location information can be obtained through various methods like GPS, GIS etc. Location based protocols can be used with flat as well as hierarchical topologies. Although there are many locations based routing protocols exist with a different working but the main aim of these protocols is to save energy.

Salient features

- It reduces control overhead as this scheme does not require flooding.
- It saves the energy consumption through various techniques.
- The cost of route setup is reduced as it is based on the location of destination.
- It requires less memory as there is no need to store the entire network information.
- It is scalable i.e. any number of nodes can join the network.
- It also needs less maintenance.

Q.7. (a) Discuss qualities of service metrics that are used to evaluate the performance of the network. **(6)**

Ans. There are many different ways to measure the performance of a network, as each network is different in nature and design.

The following measures are often considered important

Bandwidth commonly measured in bits/second is the maximum rate that information can be transferred.

Throughput is the number of messages successfully delivered per unit time. Throughput is controlled by available bandwidth, as well as the available signal-to-noise ratio and hardware limitations. Throughput for the purpose of this article will be understood to be measured from the arrival of the first bit of data at the receiver, to decouple the concept of throughput from the concept of latency. For discussions of this type the terms 'throughput' and 'bandwidth' are often used interchangeably.

Latency the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter is the undesired deviation from true periodicity of an assumed periodic signal in electronics and telecommunications, often in relation to a reference clock source. Jitter may be observed in characteristics such as the frequency of successive pulses, the signal amplitude, or phase of periodic signals.

The bit error rate or bit error ratio (BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. BER is a unit less performance measure, often expressed as a percentage.

Q.7. (b) Differentiate single hop and multi hop networks with neat diagram. (6.5)

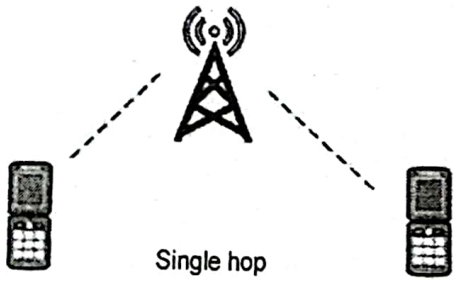
Ans. A hop means number of different networks a packet has to go through in order to reach its final destination address.

The main difference between single & multi-hop network is the number of hops a packet takes to reach the final destination.

Single hop network: In a single hop network , when a packet leaves the source it just takes a single hop (goes through another network or you can say it passes through another router from a different network) before reaching its destination address.

Multi-hop network: In a multi-hop network a packet has to go through 2 or more networks in order to reach its destination address.

While taking a hop through a different network a packet may go through various devices like Routers, network bridges, switches, etc...



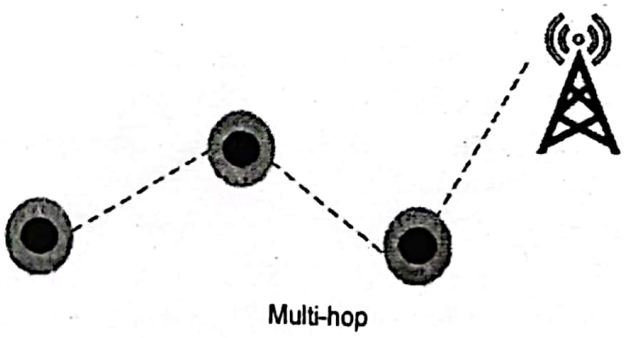


Fig. Single hop and multi hop relaying.

UNIT-IV

Q.8. (a) What is Geolocation? Give the architecture of geolocation. List various services offered by localization. **(6)**

Ans. Refer Q.8 of End Term Examination 2017. (Page. No. 27-2017).

Q.8. (b) Discuss the design issues on higher layer in WSN. **(6.5)**

Ans. Sensor networks pose certain design challenges due to the following reasons:

• Sensor nodes are randomly deployed and hence do not fit into any regular topology. Once deployed, they usually do not require any human intervention.

Hence, the setup and maintenance of the network should be entirely autonomous.

• Sensor networks are infrastructure-less. Therefore, all routing and maintenance algorithms need to be distributed.

• An important bottleneck in the operation of sensor nodes is the available energy. Sensors usually rely only on their battery for power, which in many cases cannot be recharged or replaced. Hence, the available energy at the nodes should be considered as a major constraint while designing protocols. For instance, it is desirable to give the user an option to trade off network lifetime

for fault tolerance or accuracy of results.

• Hardware design for sensor nodes should also consider energy efficiency as a primary requirement. The micro-controller, operating system, and application software should be designed to conserve power.

• Sensor nodes should be able to synchronize with each other in a completely distributed manner, so that TDMA schedules can be imposed and temporal ordering of detected events can be performed without ambiguity.

• A sensor network should also be capable of adapting to changing connectivity due to the failure of nodes, or new nodes powering up. The routing protocols should be able to dynamically include or avoid sensor nodes in their paths.

• Real-time communication over sensor networks must be supported through provision of guarantees on maximum delay, minimum bandwidth, or other QoS parameters.

Q.9. Write short note on:-

Q.9. (a) Optical wireless network. **(6)**

Ans. Optical wireless communication enables communication using infrared rays and light waves operating at frequencies well beyond the visible spectrum for high data rate local communication. Optical wireless communication technology exhibits a number of properties that makes it a suitable alternative to indoor RF communication. The advantages of optical wireless communication include significantly less interference due to its lack of penetration through walls, positioning of spectrum at a completely unregulated and unlicensed band, increased security, and high data rate. Optical wireless technology promises broadband data delivery at short ranges in point-to multipoint LANs and point-to-point medium-distance optical links. Optical wireless transmission can be classified into short-range communication and long-range communication systems. A comparison of these two types of optical wireless transmission schemes is given in Table. Long-range communication systems are mainly used for outdoor point-to-point optical links and short-range systems are used in indoor and outdoor applications. Unlike the long-haul networks in fiber-based optical networks, the long-range optical wireless systems can operate over a distance of hundreds of meters only. The short-range systems operate over a distance of few meters. With the ever growing

demand for broadband wireless connectivity, the utilization of RF spectrum is a bottleneck due to the spectrum congestion, licensing requirements, and unsuitability of certain bands for broadband applications.

Table: Comparisons of optical wireless technologies.

Issue	Short-Range	Long-Range
Distance	< 10 m	< 1,000 m
Data Rate	9600 bps to 4 Mbps	< 10 Gbps
Source Power	Low	High
Preferred Transmitter	LED	Laser
Preferred Receiver	PIN Diode	Avalanche Diode
Mode of Propagation	Line of Sight (LoS) and Diffused	LoS
Effect of Atmospheric Conditions	Limited	Significant
Cost of Equipment	Low	High

Q.9. (b) Ultra wide band radio communication. **(6.5)**

Ans. Ultra-Wide Band (UWB) is a communication method used in wireless networking that uses very low power consumption to attain high bandwidth connections or we can say, it's meant to transmit a lot of data over a short distance without using too much power. Originally UWB was designed for commercial radar systems. UWB wireless radios send short signal pulses over an extensive spectrum. This means the data is transmitted over a number of frequency channels at once, anything over 500 MHz. it is also called digital pulse wireless.

For example, a UWB signal centred at 5 GHz typically extends across 4 GHz and 6 GHz. The wide signal allows UWB to commonly support high wireless data rates of 480 Mbps up to 1.6 Gbps, at distances up to a few meters.

When compared to the spread spectrum, UWB uses broad spectrum use means that it doesn't interfere with other transmissions in the same frequency band, like narrowband and carrier wave transmissions. After some initial successes in the mid-2000s, interest in UWB declined considerably in favor of Wi-Fi and 60 GHz wireless network protocols.The major differences between the ultra-wide band (UWB) technology and the existing narrow-band and wide-band technologies are the following:

(i) The bandwidth of UWB systems, as defined by the Federal Communications Commission (FCC), is more than 25% of the center frequency or a bandwidth greater than 500 MHz.

(ii) The narrow-band and wide-band technologies make use of a radio frequency (RF) carrier to shift the base band signal to the center of the carrier frequency, whereas theUWB systems are implemented in a carrier- less fashion in which the modulation scheme can directly modulate base band signals into an impulse with very sharp rise and fall time, thus resulting in a waveform ranging several GHz of bandwidth.

MID TERM EXAMINATION [MAY-2023]
EIGHT SEMESTER [B.TECH]
AD HOC AND SENSOR NETWORKS [ETEC-406]

ime: 1.5 Hrs. Max. Marks: 30

ote: Attempt Q. No. 1 which is compulsory and any two questions from the emaining.

Q.1. (a) What is the difference between cellular and ad-hoc wireless etworks? (2.5)

Ans. Refer to Q.1 (b) First Term Examination 2019 (Pg. No. 1-2019).

Q.1. (b) What are the major functions performed by the TCP? (2.5)

Ans. Refer to Q.1 (d) End Term Examination 2018 (Pg. No. 5-2018).

Q.1. (c) What are the applications of Wireless Ad-Hoc networks? (2.5)

Ans. Refer to Q.3 Model Test Paper III (Pg. No. M.P. III-3).

Q.1. (d) What are the major Network Security Attacks? (2.5)

Q.2. (a) Classify the MAC protocols. What are the advantages of reservation-ased MAC protocols over contention-based MAC protocols? (7)

Ans. Refer to Q.3 (a), (b) End Term Examination 2017 (Pg. No. 14,15-2017.

Q.2. (b) Compare the pros and cons of using scheduling based MAC rotocols over reservation-based MAC protocols? (3)

Q.3. (a) Describe the major challenges faces during a routing protocol lesigned for ad hoc wireless networks? (5)

Ans. Refer to Q.1 (d) End Term Examination 2017 (Pg. No. 9-2017).

Q.3. (b) Why secure routing protocols are needed? Describe issues and hallenges in securing provisioning of transport layer. (5)

Ans. Refer to Q.5 (b) End Term Examination 2018 (Pg. No. 12-2018).

Q.4. (a) Describe a common method used in alleviating the hidden terminal roblem at the MAC layer. (5)

Q.4. (b) Why does TCP not perform well in Ad Hoc Wireless Networks? Explain. (5)

Ans. Refer to Q.1 (e) End Term Examination 2019 (Pg. No. 7-2019).

END TERM EXAMINATION [JULY-2023]
EIGHT SEMESTER [B.TECH]
AD HOC AND SENSOR NETWORKS [ETEC-406]

Time: 3 Hrs. **Max. Marks: 75**

Note: Attempt five questions in all including Q. No. 1 which is compulsory. Select one question from each unit.

Q.1. Attempt All:

Q.1. (a) What is an ad-hoc network? Why ad hoc networks are needed? Discuss. (4)

Ans. Refer to Q.1 (a) End Term Examination 2019 (Pg. No. 6-2019).

Q.1. (b) What is Sensor Network Localization. (4)

Q.1. (c) Explain goals to be achieved in transport layer protocol for ad hoc wireless networks. (4)

Q.1. (d) List the characteristics of ideal routing protocol for ad hoc wireless network.

Ans. Refer to Q.1 (c) First Term Examination 2018 (Pg. No. 2-2018).

Q.1. (e) Define data relaying in a WSN. (4)

Q.1. (f) What is data dissemination in a wireless sensor network? (4)

UNIT - I

Q.2. (a) Explain about the Contention-based MAC protocols with scheduling mechanism. (6.5)

Ans. Refer to Q.2 (b) End Term Examination 2017 (Pg. No. 13-2017).

Q.2. (b) Outline the design challenges in mobile adhoc networks and wireless sensor network. (6)

Q.3. (a) What are the advantages of reservation based MAC protocols over contention based MAC protocols? (6.5)

Ans. Refer to Q.3 (b) End Term Examination 2017 (Pg. No. 15-2017).

Q.3. (b) Explain the issues in designing the MAC protocols in ad hoc networks and give the classification of MAC protocols. (6)

Ans. Refer to Q.3 (a) End Term Examination 2018 (Pg. No. 9-2018) & Refer to Q.3 (a) End Term Examination 2017 (Pg. No. 14-2017).

UNIT - II

Q.4. (a) What is the need for power management in ad hoc network? Discuss the approaches for power aware routing protocol. (6)

Ans. Refer to Q.5 (a) End Term Examination 2017 (Pg. No. 20-2017).

Q.4. (b) Give classification of routing protocols in ad hoc networks. Explain any two. (6.5)

Ans. Refer to Q.5 (a) End Term Examination 2018 (Pg. No. 12-2018).

Q.5. (a) Why TCP protocols used in wired network is not suitable for wireless networks? (6.5)

Ans. Refer to Q.4 (b) First Term Examination 2017 (Pg. No. 6-2017).

Q.5. (b) What do you understand by network security requirements? Discuss the issues and challenges in secure routing of ad hoc wireless networks. (6)

Ans. Refer to Q.5 (b) End Term Examination 2017 (Pg. No. 21-2017).

Q.6. (a) What is a wireless sensor network? Explain with diagrammatic illustration of wireless sensor network architecture. (6.5)

Ans. Refer to Q.4 (a) End Term Examination 2019 (Pg. No. 10-2019).

Q.6. (b) Why is routing in multi-hop ad-hoc networks complicated, what are the special challenges? (6)

Q.7. (a) Explain about UWB radio communication systems. (6)

Ans. Refer to Q.9 (b) End Term Examination 2019 (Pg. No. 16-2019).

Q.7. (b) What is wireless geolocation? Discuss the geolocation system architecture. (6.5)

Ans. Refer to Q.8 End Term Examination 2017 (Pg. No. 27-2017).

Q.8. Write short note on:

Q.8. (a) Geolocation standards for E-911 Services. (6)

Ans. Refer to Q.8 Model Test Paper III (Pg. No. 10-MP-III).

Q.8. (b) Vehicular sensor networks. (6.5)

Ans. Refer to Q.9 (b) End Term Examination 2018 (Pg. No. 16-2018).