# 3.1 Infrastructure - Less Wireless Networks

## 3.1.1 Adhoc Network

- A Mobile Ad-hoc Network (MANET) is an autonomous system of nodes connected by wireless links. A MANET does not necessarily need support from any existing network infrastructure like an Internet gateway or other fixed stations. The network's wireless topology may dynamically change in an unpredictable manner since nodes are free to move.
- Information is transmitted in a store-and forward manner using multi hop routing. Each node is equipped with a wireless transmitter and a receiver with an appropriate antenna.
- An ad-hoc network consists of a set of nodes that communicate using a wireless medium over single or multiple hops and do not need any preexisting infrastructure such as access points or base stations.
- Ad-hoc networks can comprise of mobile, static or both types of nodes. Ad-hoc networks containing mobile nodes are known as mobile ad-hoc networks.
- In ad-hoc networks all nodes of mobile and can be connected dynamically in an arbitrary manner. All nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network.
- Ad-hoc networks are very useful in emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information and data acquisition operations in inhospitable terrain.
- Ad-hoc networks are wireless, self organizing, systems formed by co-operating nodes within communication range of each other that form temporary networks. Their topology is dynamic, decentralized ever changing and the nodes may move around arbitrarily.
- An ad-hoc network is a multi-hop wireless network where all nodes co-operatively maintain network connectivity without a centralized infrastructure. If these nodes change their positions dynamically, it is called a Mobile Ad-hoc Network (MANET).

**Characteristics**

1. Dynamic topologies : Nodes are free to move arbitrarily.
2. Bandwidth constrained, variable capacity link.
3. Power constrained operations : All the nodes in a MANET rely on batteries for their energy.
4. Limited physical security : Mobile wireless networks are generally more prone to physical security threats than fixed, hard-wired networks.

## 3.2 Design Issues in Adhoc Wireless Network

- Following are the main issues which affect design, implementation and performance of Ad hoc networks.

1. Medium access scheme
2. Routing
3. Multicasting
4. Transport layer protocol
5. Pricing scheme
6. Security
7. Scalability
8. Quality of service provisioning
9. Address and service discovery
10. Energy management
11. Self organization
12. Deployment

### 3.2.1 Medium Access Scheme

- Design goals of a MAC protocol for ad hoc wireless networks are : Synchronization, distributed operation, throughput, hidden and exposed terminals, access delay, fairness, real time traffic support, resource reservation, adaptive rate control, use of directional antenna etc.

1. The operation of the protocol should be distributed.
2. The protocol should provide QoS support for real-time traffic.
3. The access delay, which refers to the average delay experienced by any packet to get transmitted, must be kept low.
4. The available bandwidth must be utilized efficiently.
5. The protocol should ensure fair allocation of bandwidth to nodes.
6. Control overhead must be kept as low as possible.
7. The protocol should minimize the effects of hidden and exposed terminal problems.
8. The protocol must be scalable to large networks.
9. It should have power control mechanisms.
10. The protocol should have mechanisms for adaptive data rate control.
11. It should try to use directional antennas.
12. The protocol should provide synchronization among nodes.

### 3.2.2 Routing

- Major challenges for routing protocol :
  1. Mobility : Node mobility results in path breaks, packet collision, difficulty in resource reservation and transient loop.

2. Bandwidth constraint : Channel is shared by all nodes, so bandwidth available per wireless link depends on the number of nodes and traffic they handle.
3. Error-prone and shared channel : Bit error rate in wireless channel is very high.
4. Location-dependent contention : High contention for the channel results in a high number of collisions and subsequent wastage of bandwidth.

- Major requirements of a routing protocol in ad hoc :
  a. Minimum route acquisition delay
  b. Quick route reconfiguration
  c. Loop-free routing
  d. Distributed routing approach
  e. Minimum control overhead
  f. Scalability
  g. Provisioning of QoS
  h. Support for time-sensitive traffic
  i. Security and privacy
- Routing's responsibilities are as follows :
  a. Exchanging the route information
  b. Finding a feasible path
  c. Gathering information about path breaks
  d. Mending the broken paths
  e. Utilizing minimum bandwidth

## 3.2.3 Multicasting

- Multicasting plays an important role in the typical applications of ad hoc wireless networks, namely, emergency search-and-rescue operations and military communication. Provisioning of multiple links among the nodes in ad hoc results in a mesh-shaped structure.
- The major issues in designing multicast
  a. Robustness : Multicast routing protocol must be able to recover and reconfigure quickly.
  b. Efficiency : Protocol should make minimum number of transmission for delivery data packet to all group members.
  c. Control overhead : Bandwidth availability demands minimal control overhead for multicast session.

d. Quality of service : It is required because of data transferred in multicast session in time sensitive.

e. Efficient group management : Maintain connectivity between all group member and minimal exchange of control messages.

f. Scalability : Must support for adding new node in large network.

g. Security : Authentication is required in some applications.

## 3.2.4 Transport Layer Protocols

- The function of the transport layer protocols include setting up and maintaining end-to-end connections, reliable end-to-end delivery of data packets, flow control, and congestion control.
- UDP protocol is used and it is connectionless transport layer protocol and neither perform flow control and congestion control.
- TCP is connection oriented protocol and it affect the performance of network because of frequent path breaks, presence of state routing information, high channel error rate etc.
- Wireless channel are inherently unreliable due to the high probability of errors caused by interference. When the TCP ACK is delayed more than the round trip timeout, congestion control algorithm is invoked.

## 3.2.5 Pricing Scheme

- Assume that an optimal route from node X to node Y passes through node Z, & node Z is not powered on. Then node X will have to set up a costlier & non-optimal route to Y.
- The non-optimal path consumes more resources & affects the throughput of the system.
- We need a pricing scheme for compensating relaying node for their consumption of resources such as battery charge and computing power.
- So pricing schemes that incorporate service compensation or service reimbursement are required.

## 3.2.6 Security

- The ad hoc networks are even more exposed to attacks than the infrastructure counterpart. Both active and passive attacks are possible.

- In active attack attacker tries to interrupt operations (control and data packets; reintroduces bogus control packets; damages the routing tables beyond repair; unleashes denial of service attacks, etc.).
- Passive attacks are unique in ad-hoc network and can be more hazardous than the active attack. The active attacker is eventually discovered and physically disabled.
- The passive attacker is never discovered by the network. It monitors data and control traffic patterns and thus infers the normal operation. Defense from passive attacks require powerful novel encryption techniques coupled with careful network protocol designs.
- Security threats that exist in an Ad hoc wireless networks are denial of service, resource consumption, information disclosure, host impersonation etc.
- Denial of service : The attacker can also try to perform Denial of Service on the network layer by saturating the medium with a storm of broadcast messages, reducing nodes' goodput and possibly impeding nodes from communicating.
- **Host impersonation :** When internal node is compromised, it can act as another node and respond with appropriate control packets to create wrong route entries, and can terminate the traffic meant for the intended destination node.
- **Information disclosure :** A compromised node can act as an informer by deliberate discloser of secret information to unauthorized nodes. Information like the amount and the periodicity of traffic between a selected pair of nodes and pattern of traffic changes can be very valuable for military applications.
- **Interference :** A common attack in defense applications is to jam the wireless communication be creating a wide-spectrum noise. This can be done by using a single wide-band jammer, sweeping across the spectrum.
- **Buffer overflow attack :** In this attack, routing table is filled by unwanted routing entries.

### 3.2.7 Scalability

- When size of ad hoc wireless network growing up, there are some problems such as install, latency, periodic routing overhead.
- Hierarchical topology system can improve this problem. Scalability is expected in ad hoc wireless networks.
- Periodic routing overhead involved in a table driven routing protocol may consume a significant amount of bandwidth in such large networks.

### 3.2.8 Energy Management

- Transmission power management : The Radio Frequency (RF) hardware design should ensure minimum power consumption.
- Battery energy management is aimed at extending the battery life.
- Processor power management : The CPU can be put into different power saving modes.
- Devices power management : Intelligent device management can reduce power consumption of a mobile node.

### 3.2.9 Quality of Service Provisioning

- QoS parameters based on different applications. QoS-aware routing uses QoS parameters to find a path.
- QoS framework is a complete system that aims at providing the promised services to each users.
- QoS provisioning often requires negotiation between host and network, call admission control, resource reservation and priority scheduling of packets.
- As different applications have different requirements, the services required by them and the associated QoS parameters differ from application to application.
- Applications such as group communication in a conference hall require that the transmissions among nodes consume as mini-mum energy as possible. Hence battery life is the key QoS parameter here.

### 3.2.10 Addressing and Service Discovery

- Addressing and Service Discovery is essential because of absence of a centralized coordinator. Each device in ad hoc wireless network should has unique address.
- With unique address for each device, location of each device and whole network configuration can be maintained. So we can discover the node offering service.

### 3.2.11 Deployment Considerations

- The deployment of a commercial ad hoc wireless network has the following benefits comparing to wired networks
  a. Low cost of deployment
  b. Incremental deployment
  c. Short deployment time
  d. Reconfigurability

- Issues of considering deployment of ad hoc
  1. Scenario of deployment
  2. Required longevity of network
  3. Area of coverage
  4. Service availability
  5. Operational integration with other infrastructure
  6. Choice of protocols

## 3.3 Ad hoc Network MAC Layer

### 3.3.1 Design Issues for Ad hoc Network MAC layer

- **Bandwidth efficiency** is defined at the ratio of the bandwidth used for actual data transmission to the total available bandwidth. The MAC protocol for ad-hoc networks should maximize it.
- **Quality of service** support is essential for time-critical applications. The MAC protocol for ad-hoc networks should consider the constraint of ad-hoc networks.
- **Synchronization** can be achieved by exchange of control packets. Some mechanism has to be found in order to provide synchronization among the nodes. Synchronization is important or regulating the bandwidth reservation.
- **Hidden and exposed terminal problems :** The reason for these two problems is the broadcast nature of the radio channel, namely, all the nodes within a node's transmission range receive its transmission.
- **Hidden terminal problem :** Two nodes that are outside each-other's range perform simultaneous transmission to a node that is within the range of each of them, hence, there is a packet collision.
- Exposed terminal problem - the node is within the range of a node that is transmitting, and it cannot transmit to any node.
- **Error-prone shared broadcast channel :** In radio transmission, a node can listen to all traffic within its range. Therefore, when there is communication going on no other node should transmit, otherwise there would be interferences. Access to the physical medium should be granted only if there is no session going on. Nodes will often compete for the channel at the same time; therefore, there is high probability of collisions. The aim of a MAC protocol will be to minimize them, while maintaining fairness.
- **No central coordination :** In ad hoc networks, there is no central point of coordination due to the mobility of the nodes. Therefore, the control of the access

to the channel must be distributed among them. In order for this to be coordinated, the nodes must exchange information. It is the responsibility of the MAC protocol to make sure this overhead is not a burden for the scarce bandwidth.

- **Mobility of nodes :** The mobility of the nodes is one of its key features. The QoS reservations or the exchanged information might become useless, due to node mobility. The MAC protocol must be such that mobility has as little influence as possible on the performance of the whole network.

## 3.3.2 Design Goals

1. Protocol operation should be distributed through all the nodes.
2. In real time traffic, the protocol should provide QoS.
3. The average delay for packet transmission should be as small as possible.
4. The bandwidth should be utilized efficiently.
5. Each node must have a fair share of the available bandwidth.
6. Control overhead should be minimized.
7. The hidden and exposed terminal problems should be minimized.
8. The protocol must be scalable to large networks.
9. Power control mechanisms are needed for efficient management of the energy consumption of the nodes.
10. Adaptive data rate control should be provided - a node controls the rate of outgoing traffic in relation also to the network load and to the status of the other nodes.
11. Directional antennas are encouraged, the advantages are reduced interference, increased spectrum reuse and reduced power consumption.
12. Time synchronization between the nodes should be provided.

## 3.3.3 Classification of MAC Protocol for Ad hoc Networks

- Several criteria can be used for the classification of MAC protocols, such as time synchronization, initiation approach and reservation approach. Ad hoc network protocols can be classified into three basic types :
  1. Contention-based protocols;
  2. Contention-based protocols with reservation mechanisms;
  3. Contention-based protocols with scheduling mechanisms;

**Contention-based protocols**

- The channel access policy is based on competition. Whenever a node needs to send a packet, it tries to get access to the channel. These protocols cannot provide QoS, since access to the network cannot be guaranteed beforehand.
- A node does not make any resource reservation a priori. It cannot provide QoS guarantee.
- Random access protocol can be divided into following types :
  1. Sender-initiated protocols : Packet transmissions are initiated by the sender node.
  2. Single-channel sender-initiated protocols : A node that wins the contention to the channel can make use of the entire bandwidth.
  3. Multichannel sender-initiated protocols : The available bandwidth is divided into multiple channels.
  4. 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.

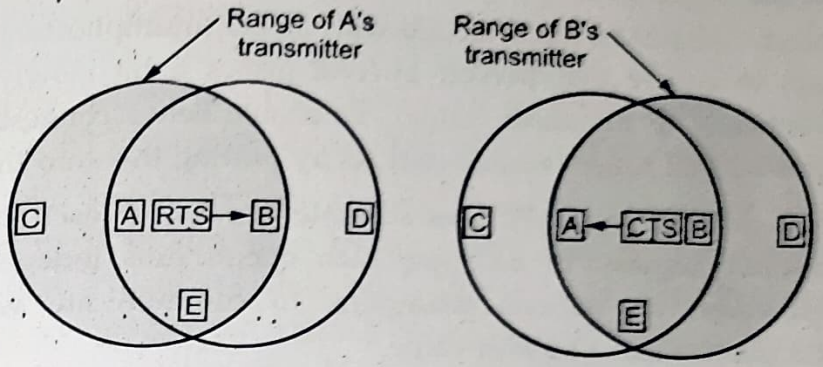
## 3.4 MACAW Protocol

**1. MACA protocol**

- Multiple Access Collision Avoidance protocol (MACA) proposed by Karn in 1990. It does not make use of carrier-sensing. It uses Request-To-Send (RTS) Clear-To-Send (CTS) and DATA messages.
- There is no acknowledgment packet (ACK) in MACA scheme. Before transmission of a packet, the nodes operate in RTS-CTS mode to reserve the channel by sending Request-to-send packet.

**2.**

- The destination node send a Clear-to-send frame to acknowledge the receipt of an RTS frame, then data is transmitted after successful exchange of RTS-CTS. his mechanism helps to solve problems only if the nodes are synchronized and packet sizes and data rates are same for both the transmitting nodes.
- Once the sender receives the CTS packet without any error, it starts transmitting the data packet.
- If a packet transmitted by a node is lost, the node uses the binary exponential back-off (BEB) algorithm to back off a random interval of time before retrying.
- The binary exponential back-off mechanism used in MACA might starves flows sometimes. The problem is solved by MACAW. Fig. 3.4.1 shows MACA protocol.




(a) Node A sending RTS to node B

(b) Node B responding with a CTS to node A

**Fig. 3.4.1 : MACA protocol**

- Both the RTS and CTS packets carry the expected duration of the data packet transmission.
- Since the collision may occur on RTS packet and it is detected by lack of CTS response. The packet is scheduled for retransmission in the future. RTS-CTS mechanism increases the system performance by reducing collision. It is suited to combat Hidden terminal problem in CSMA.
- This MACA is not fully solve the hidden node and exposed terminal problem and nothing is done regarding receiver blocked problem.
- The binary exponential back-off mechanism used in MACA might starves flows sometimes. The problem is solved by MACAW.

### 2. MACAW protocol

- A Media Access Protocol for Wireless LANs is based on MACA (Multiple Access Collision Avoidance) Protocol.
- This protocol uses an RTS-CTS-DS-DATA-ACK message exchange and a backoff algorithm. MACAW protocol uses one more control packet RRTS

(Request-for-Request-to-Send). This control packet is transmitted by a receiver on behalf of sender to save it from starvation.

- The design of MACAW is based on four observations :
  1. Relevant contention occurs at the receiver; sensing carrier at the sender (as in CSMA) is inappropriate.
  2. Congestion is location dependent.
  3. For fair allocation, collision (congestion) information must be shared among devices.
  4. Information related to contention period must be synchronized among devices to promote fair contention.
- Backoff algorithm : MACAW replaces BEB with MILD (multiplicative increase and linear decrease) to ensure that backoff interval grows a bit slowly and shrinks really slowly (linearly to minimum value). To enable better congestion detection, MACAW shares backoff timers among stations by putting this info in headers.
- Multiple stream model : MACAW uses separate queues for each stream in each node for increased fairness. In addition, each queue runs independent backoff algorithms. However, all stations attempting to communicate with the same receiver should use the same backoff value.
- *Fig. 3.4.2 shows the operation of the MACAW protocol.*

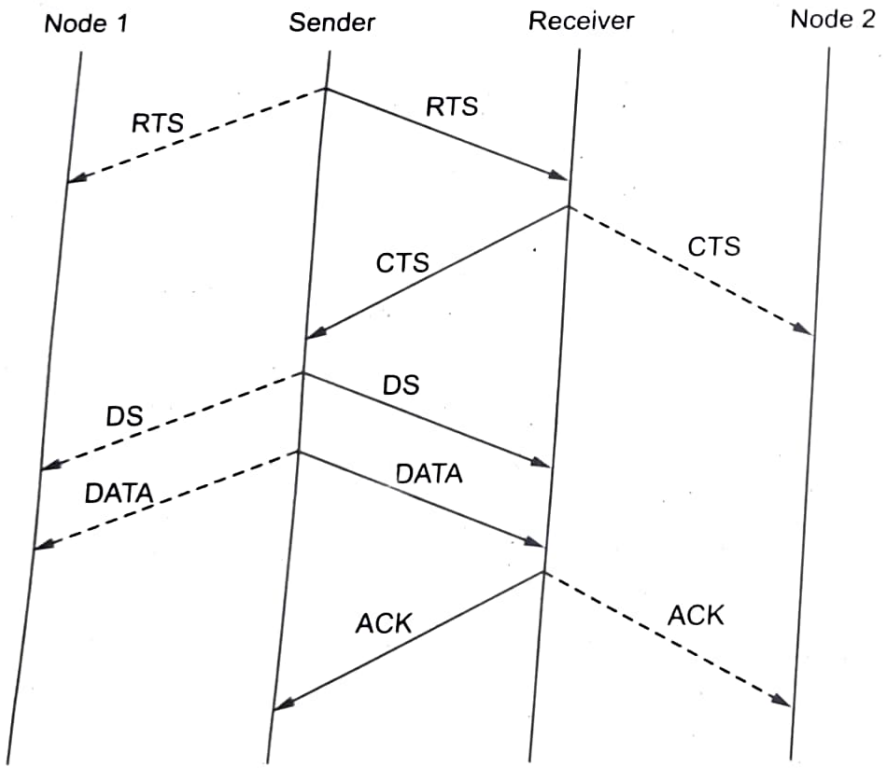



**Fig. 3.4.2 : Operation of the MACAW protocol**

- When RTS transmitted by sender is overhead by node 1, it refrains from transmitting until sender receives the CTS.
- When CTS transmitted by receiver is heard by neighbor node 2, it defers its transmission until data packet is received by receiver.
- On receiving this CTS packet, sender immediately transmits the DS message carrying the expected duration of the data packet transmission.
- On hearing this packet, node 1 back off until the data packet is transmitted. Finally after receiving the data packet, receiver acknowledges the reception by sending sender an ACK packet.
- Basic exchange : MACAW replaces RTS-CTS-DATA to RTS-CTS-DS-DATA-ACK with the following extensions :

1. ACK : An extra ACK at the end ensures that errors can be recovered in the link layer, which is much faster than transport layer recovery. If an ACK is lost, next RTS can generate another ACK for the previous transmission.
2. DS : This signal ensures a 3-way handshake between sender and receiver (similar to TCP) so that everyone within hearing distance of the two stations know that a data transmission is about to happen. Without the DS packet, stations vying for the shared media cannot compete properly and one is always starved due to the lack of its knowledge of the contention period. In short, DS enables synchronization.
3. RRTS : RRTS is basically a proxy RTS, when the actual RTS sender is too far away to fight for the contention slot. However, there is one scenario where even RRTS cannot guarantee fair contention.
4. Multicast : Multicast is handled by sending data right away after the RTS packet, without waiting for CTS. It suffers from the same problems as in CSMA, but the authors leave it as an open challenge.

## 3.5 Ad hoc Network Routing Layer

**SPPU : Dec.-15, May-16, 17**

- Routing protocols used in wired networks cannot be directly applied to ad hoc wireless networks.
  1. Highly dynamic topology.
  2. No infrastructure for centralized administration.
  3. Bandwidth constrained - Bandwidth constrained.
  4. Energy constrained.
- For the above reasons, we need to design new routing protocols for ad hoc networks.

### 3.5.1 Issues in Designing a Routing Protocol for Ad hoc Wireless Networks

1. **Mobility :** Ad hoc is highly dynamic due to the movement of nodes. The node movement causes frequent path breaks. The path repair in wired network has slow convergence.
2. **Bandwidth constraint :** Wireless has less bandwidth due to the limited radio band. Wireless has less bandwidth due to the limited radio band. Less data rate are difficult to maintain topology information. Frequent change of topology causes more overhead of topology maintenance. For that purpose, bandwidth optimization and design topology update mechanism with less overhead is required.
3. **Error-prone shared broadcast radio channel :** Wireless links have time varying characteristics in terms of link capacity and link-error probability. So it is necessary to interact with MAC layer to find better-quality link. Hidden terminal problem causes packet collision.
4. **Resource constraints :** Because of limited battery life and limited processing power, necessary to optimally manage these resources.

### 3.5.2 Classifications of Routing Protocols

- Routing protocols for Ad Hoc networking can be classified based on four different criteria. They can be classified based on the routing information update mechanism.
- Another classification can be done based on the use of temporal information for routing. A third option is to classify such protocols based on the routing topology. Finally, they can be also classified based on the utilization of specific resources.
- Ad-hoc routing protocols can be classified into three major groups based on the routing strategy.
  1. Pro-active or table driven,
  2. Reactive or on-demand,
  3. Hybrid
- In proactive routing protocols routes to a destination are determined when a node joins the networks or changes its location and are maintained by periodic route updates.
- In reactive routing protocols routes are discovered when needed and expire after a certain period.
- Hybrid routing protocols combine the features of both proactive and reactive routing protocols to scale well with network size and node density. Each of these

groups can be further divided into two sub-groups based on the routing structure: flat and hierarchical.

- In flat routing protocols nodes are addressed by a flat addressing scheme and each node plays an equal role in routing. On the other hand, different nodes have different routing responsibilities in hierarchical routing protocols. These protocols require a hierarchical addressing system to address the nodes.
- Classification of ad-hoc routing protocols based on routing strategy and network structure.
- Proactive routing protocols require each node to maintain up-to-date routing information to every other node in the network. The various routing protocols in this group differ in how topology changes are detected, how routing information is updated and what sort of routing information is maintained at each node.
- These routing protocols are based on the working principles of two popular routing algorithms used in wired networks. They are known as link-state routing and distance vector routing.
- In the link-state approach, each node maintains at least a partial view of the whole network topology. To achieve this, each node periodically broadcasts link-state

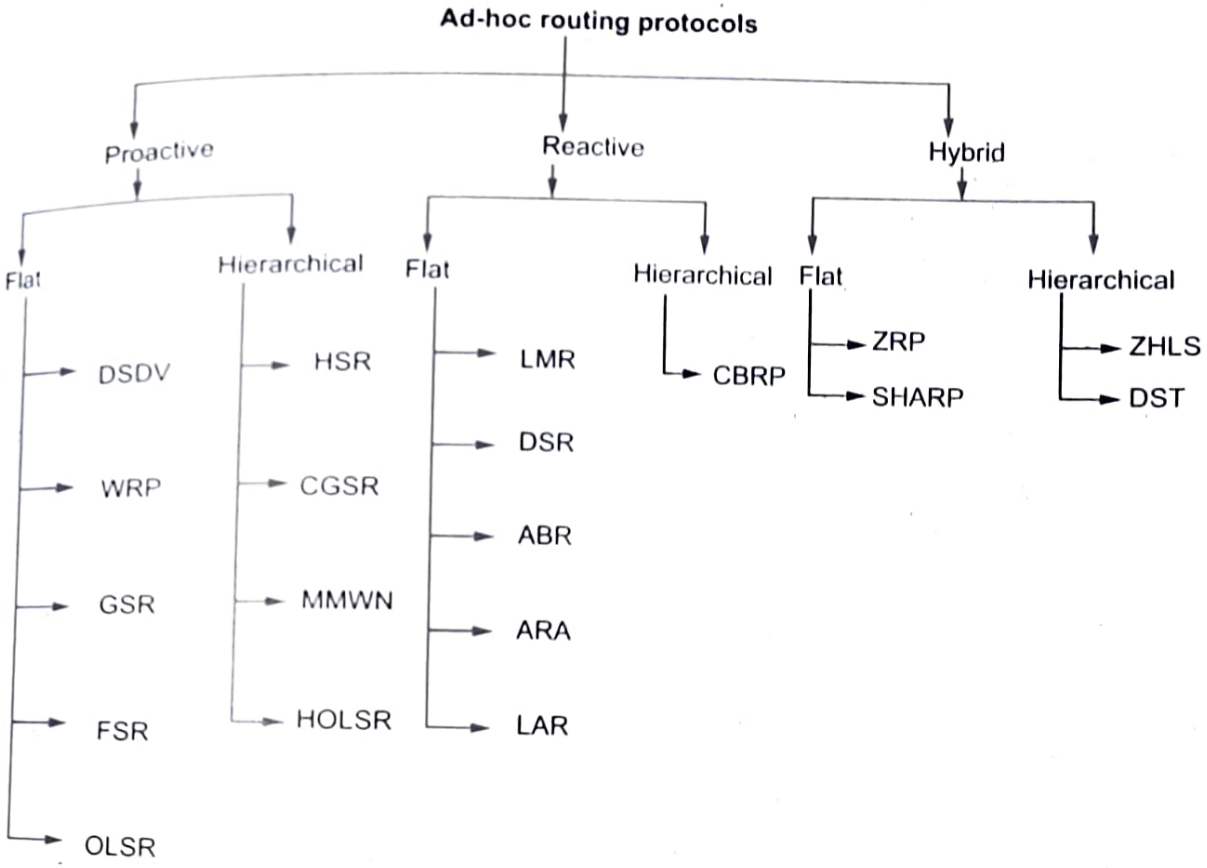



**Fig. 3.5.1 Classification of routing protocols**

information such as link activity and delay of its outgoing links to all other nodes using network-wide flooding.

- When a node receives this information, it updates its view of the network topology and applies a shortest-path algorithm to choose the next hop for each destination.
- The welknown routing protocol OSPF is an example of a link-state routing protocol. On the other hand, each node in distance vector routing periodically monitors the cost of its outgoing links and sends its routing table information to all neighbours.
- The cost can be measured in terms of the number of hops or time delay or other metrics. Each entry in the routing table contains at least the ID of a destination, the ID of the next hop neighbour through which the destination can be reached at minimum cost, and the cost to reach the destination.
- Thus, through periodic monitoring of outgoing links, and dissemination of the routing table information, each node maintains an estimate of the shortest distance to every node in the network.
- Distributed Bellman Ford and RIP is classic examples of distance vector routing algorithms.

### 3.5.3 Comparison between Proactive and Reactive

| Parameters | Proactive routing | Reactive routing |
|---|---|---|
| Availability of routing information | Available when needed | Always available regardless of need |
| Routing philosophy | Flat | Mostly flat except for CSGR |
| Periodic route mobility | Not required | Required |
| Signaling traffic generated | Grows with increasing mobility of active routes | Greater than that of on-demand routing |
| Examples | DSDV, CGSR and WRP | AODV, DSR, TORA, ABR and SSR |
| Route | Always maintain routes | Lower overhead since routes are determined on demand |
| Name | It is also called table driven routing | It is also called on-demand routing |
| Definition | Proactive protocols are based on periodic exchange of control messages and maintaining routing tables. | In a reactive protocol, a route is discovered only when it is necessary. |

## 3.5.4 DSDV

- DSDV was one of the first proactive routing protocols available for Ad-hoc networks.

**Algorithm**

- DSDV is based on the Bellman-Ford algorithm.
- With DSDV, each routing table will contain all available destinations, with the associated next hop, the associated metric (numbers of hops) and a sequence number originated by the destination node.
- Tables are updated in the topology per exchange between nodes.
- Each node will broadcast to its neighbors entries in its table. This exchange of entries can be made by dumping the whole routing table or by performing an incremental update, that means exchanging just recently updated routes.
- Nodes who receive this data can then update their tables if they received a better route, or a new one.
- Updates are performed on a regular basis and are instantly scheduled if a new event is detected in the topology.
- If there are frequent changes in topology, full table exchange will be preferred whereas in a stable topology, incremental updates will cause less traffic.
- The route selection is performed on the metric and sequence number criteria. The sequence number is a time indication sent by the destination node. It allows the table update process, as if two identical routes are known, the one with the best sequence number is kept and used, while the other is destroyed (considered as a stale entry).

**Illustration**

- Consider the two following topologies. At t = 0, the network is organized as shows Fig. 3.5.2 (a). Let at this time the network is stable, each node has a correct routing table of all destinations.
- Then, we suppose node-A is moving and at t + 1, the topology is as shown in Fig. 3.5.2 (b). At this stage, the following events are detected and actions are taken :
  1. **On node B :** Link with A is broken, the route entry is deleted and updates are sent to node C.
  2. **On node F :** A new link is detected, the new entry is added to the routing table and updates are sent to neighbors.

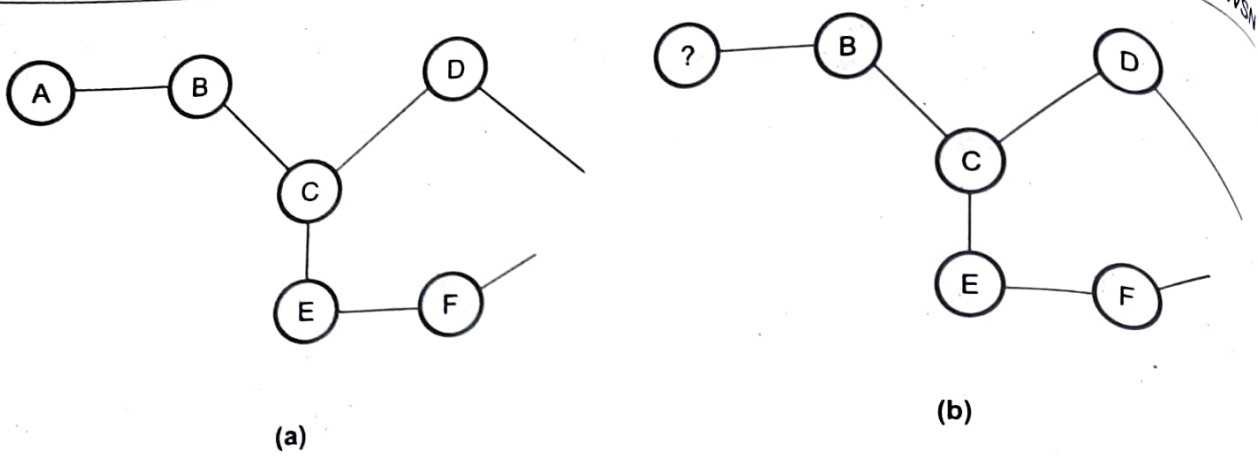



Fig. 3.5.2

3. **On node A :** Two new links are detected (to F) and one is broken (to B), the routing table is updated and a full dump is sent to neighbors (as the routing table is entirely changed, a full dump equals an incremental update).

### 3.5.4.1 Advantages and Disadvantages of DSDV

**Advantages**

1. DSDV was one of the early algorithms available. It is quite suitable for creating ad hoc networks with small number of nodes. Since no formal specification of this algorithm is present there is no commercial implementation of this algorithm.
2. DSDV guarantees for loop free path.

**Disadvantages**

1. DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle.
2. Whenever the topology of the network changes, a new sequence number is necessary before the network re-converges; thus, DSDV is not suitable for highly dynamic networks.

## 3.5.5 AODV

- Ad-hoc on demand distance vector routing (AODV) is a stateless on-demand routing protocol. Two major functions of AODV protocols are: route discovery and route maintenance. The performance of protocol is improved by keeping the routing information in each node.
- AODV is a distance vector routing protocol, which means routing decisions will be taken depending on the number of hops to destination. A particularity of this network is to support both multicast and unicast routing.

**Algorithm**

- When a route is needed to some destination, the protocol starts route discovery. Then the source node sends route request message (RREQ) to its neighboring nodes (flooding). And if those nodes do not have any information about the destination node, they will send the message to all its neighboring nodes and so on.
- If any neighbor node has the information about the destination node, the node sends route reply message to the route request message initiator. The path is recorded in the intermediate nodes. This path identifies the route and is called the reverse path.
- Since each node forwards route request message to all of its neighbors, more than one copy of the original route request message can arrive at a node. A unique ID is assigned, when a route request message is created. When a node received, it will check this ID and the address of the initiator and discarded the message if it had already processed that request.
- Node that has information about the path to the destination sends route reply message to the neighbor from which it has received route request message. This neighbor does the same. Due to the reverse path it can be possible. Then the route reply (RREP) message travels back using reverse path. When a route reply message reaches the initiator the route is ready and the initiator can start sending data packets.
- When a node detects the link failure to its next hop, it propagates a link failure notification message, Route-Error (RERR) to each of its active upstream neighbours to inform them to erase that part of the route. These nodes in turn propagate the link failure notification message to their upstream neighbours and so on, until the source node is reached.
- When the source node receives the link failure notification message, it will re-initiate a route discovery for the destination if a route is still needed. A new destination sequence number is used to prevent routing loops formed by the entangling of stale and newly established paths.
- AODV saves bandwidth and performs well in a large MANET since a data packet does not carry the whole path information.

**Route maintenance**

- Another part of this algorithm is the **route maintenance**.
- While a neighbour is no longer available, if it was a hop for a route, this route is not valid anymore.

- AODV uses HELLO packets on a regular basis to check if they are active neighbours. Active neighbours are the ones used during a previous route discovery process. If there is no response to the HELLO packet sent to a node, then the originator deletes all associated routes in its routing table.
- HELLO packets are similar to ping requests. While transmitting, if a link is broken (a station did not receive acknowledgment from the layer 2), a ROUTE ERROR packet is unicast to all previous forwarders and to the sender of the packet.

**Illustration**

- In the example illustrated in Fig. 3.5.3, node-A needs to send a packet to node-I. A route request () packet will be generated and sent to B and D.

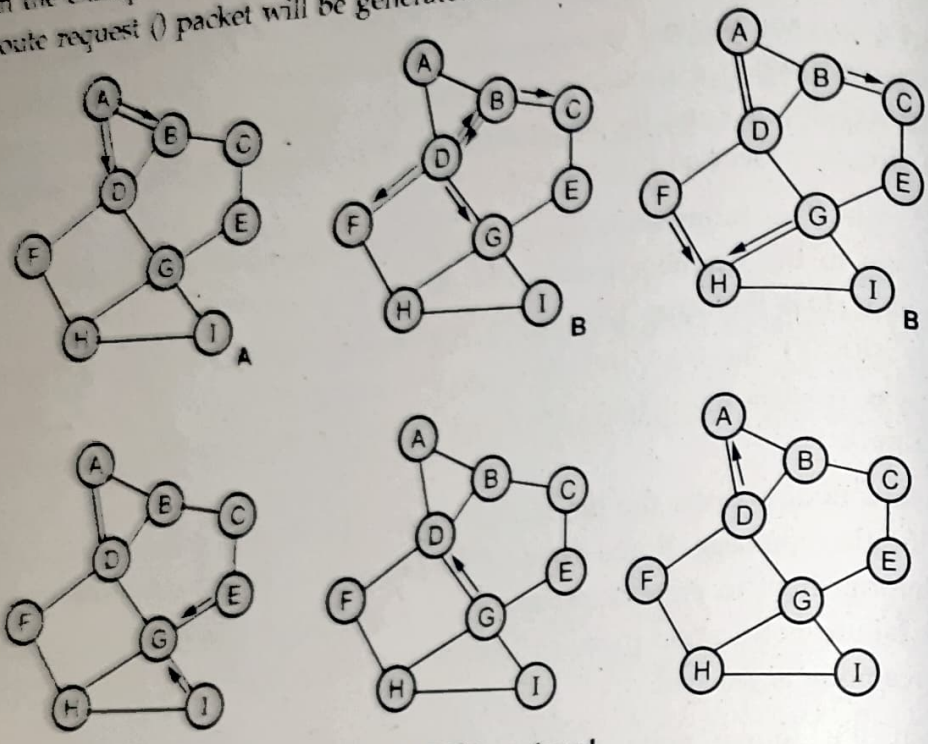



**Fig. 3.5.3 AODV protocol**

- B and D add A in their routing table, as a reverse route and forward a route request (RREQ) packet to their neighbours.
- B and D ignored the packet they exchanged each others (as duplicates). The forwarding process continues while no route is known.
- Once node-I receives the route request (RREQ) from G, it generates then a route reply (RREP) packet and sends it to the node it received from. Duplicate packets continue to be ignored while the route reply (RREP) packet goes on the shortest way to A, using previously established reverse routes.
- The reverse routes created by the other nodes that have not been used for the route reply (RREP) are deleted after a delay. G and D will add the route to I once they receive the route reply (RREP) packet.

### 3.5.5.1 Characteristics of AODV

1. AODV support unicast, broadcast and multicast communication.
2. AODV performs on-demand route establishment with small delay.
3. Multicast trees connecting group members maintained for lifetime of multicast group.
4. Link breakages in active routes efficiently repaired.
5. All routes are loop-free through use of sequence numbers.
6. Use of Sequence numbers to track accuracy of information.
7. Only keeps track of next hop for a route instead of the entire route.
8. Use of periodic HELLO messages to track neighbors.

### 3.5.5.2 Advantages and Disadvantages of AODV

- The main advantage of AODV protocol is that routes are established on demand and destination sequence numbers are used to find the latest route to the destination. The connection setup delay is lower.
- One of the disadvantages of AODV protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also multiple RouteReply packets in response to a single RouteRequest packet can lead to heavy control overhead.
- Another disadvantage of AODV is that the periodic beaconing leads to unnecessary bandwidth consumption.

## 3.5.6 DSR

- The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes.
- DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration.
- It is a reactive protocol and all aspects of the protocol operate entirely on-demand basis.
- DSR protocol uses the concept of source routing approach (every data packet carries the whole path information in its header) to forward packets.
- The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance". DSR requires each node to maintain a route cache of all known self to destination pairs. If a node has a packet to send, it attempts to use this cache to deliver the packet.

- In source routing technique the sender of a packet determines the complete sequence of nodes through which, the packets are forwarded. Otherwise, it will initiate a route discovery phase by flooding a Route REQuest (RREQ) message.
- The RREQ message carries the sequence of hops it passed through in the message header. Any nodes that have received the same RREQ message will not broadcast it again.
- Once an RREQ message reaches the destination node, the destination node will reply with a Route REPly (RREP) packet to the source. The RREP packet will carry the path information obtained from the RREQ packet.
- When the RREP packet traverses backward to the source, the source and all traversed nodes will know the route to the destination. Each node uses a route cache to record the complete route to desired destinations.
- The advantage of source routing is: intermediate nodes do not need to maintain up to date routing information in order to route the packets they forward.
- Route failure is detected by the failure of message transmissions. Such a failure will initiate a route error message to the source. When the source and the intermediate nodes receive the error message, they will erase all the paths that use the broken link from their route cache.
- If the destination does not exist in the cache, then a route discovery phase is initiated to discover a route to destination, by sending a route request (RREQ). The RREQ request includes the destination address, source address and a unique identification number.
- If a route is available from the route cache, but is not valid any more, a route maintenance procedure may be initiated.
- A node processes the route request packet only if it has not previously processes the packet and its address is not present in the route cache.
- A route reply is generated by the destination or by any of the intermediate nodes when it knows about how to reach the destination.

### 3.5.6.1 Advantages and Disadvantages of DSR

**Advantages**

1. DSR uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead.
2. DSR is simple and loop-free.

**Disadvantages**

1. The disadvantage of DSR is that the route maintenance mechanism does not locally repair a broken down link.
2. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility.
3. Considerable routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length.
4. The loop free feature may waste bandwidth if every data packet carries the entire path information.

**Review Questions**

1. *Write short note on : i) AODV ii) DSR.* **SPPU : Dec.-15 (End Sem), May-16, Marks 10**
2. *Describe DSDV routing protocols.* **SPPU : May-17, Marks 8**

## 3.6 Ad hoc Transport Layer

- Ad hoc wireless networks pose a big challenge for transport layer protocol and transport layer protocols designed for wired networks like TCP are not suitable for ad hoc wireless networks.
- The objectives of a transport layer protocol include setting up of End-to-end connection, End-to-end delivery of data packets, Flow control and Congestion control.

### 3.6.1 Issues in Designing a Transport Layer Protocol for Ad hoc Wireless Networks

- **Induced traffic :** Ad hoc wireless networks use multi-hop radio relaying, and a link-level transmission affects neighbor nodes of both sender and receiver of the link. This induced traffic affects throughput of the transport layer protocol.
- **Induced throughput unfairness :** Some MAC protocols, like IEEE 802.11 DCF, may add throughput unfairness to the transport layer. A transport layer protocol needs to take this into account to provide a fair throughput for contesting flows.
- **Separation of congestion control, reliability and flow control :** The throughput may be improved if the transport controls protocol handles congestion control, reliability and flow control separately. Congestion is usually a local activity that

affects only neighboring nodes while reliability and flow control are end-to-end issues. Separation of these should not produce significant control overhead.

- **Misinterpretation of congestion :** Commonly used methods of detecting the congestion by measuring packet loss and retransmission timeout are not suitable for ad hoc wireless networks. Packet loss occurs in wireless networks relatively frequently for several reasons. Bit error rates are much higher than in wired networks and path breaks occur frequently because nodes are constantly moving and they may fail e.g. after draining a battery. Thus, a better method for detecting congestion must be used.
- **Completely decoupled transport layer :** In wired networks, transport layer is usually almost completely decoupled from lower network layers. In wireless networks, cross-layer interaction would help transport layer protocol to adapt to the changes in the network.
- **Power and bandwidth constraints :** Ad hoc wireless networks are constrained by available power and bandwidth. These constraints affect the performance of transport layer protocol.
- **Dynamic topology :** Topology of ad hoc wireless network may change rabidly and this leads to path breaks and partitioning of network. A transport layer protocol should be able to adapt to these changes.

### 3.6.2 Design Goals of a Transport Layer Protocol for Ad hoc Wireless Networks

1. Per connection throughput should be maximum.
2. It should provide throughput fairness across contending flows.
3. It should incur minimum connection set up and connection maintenance overheads.
4. It should have mechanisms for congestion control and flow control in the network.
5. It should be able to provide both reliable and unreliable connections as per the requirements of the application layer.
6. It should be able to adapt to the dynamics of the network such as rapid changes in topology.
7. Bandwidth must be used efficiently.
8. It should be aware of resource constraints such as battery power and buffer sizes and make efficient use of them.

9. It should make use of information from the lower layers for improving network throughput.
10. Cross-layer interaction framework is defined properly.
11. End-to-End Semantics should be maintained.

### 3.6.3 Classification of Transport Layer Solutions

- Fig. 3.6.1 shows a classification tree the transport layer protocols. The solutions for TCP over ad hoc wireless networks can further be classified into split approaches and end-to-end approaches.

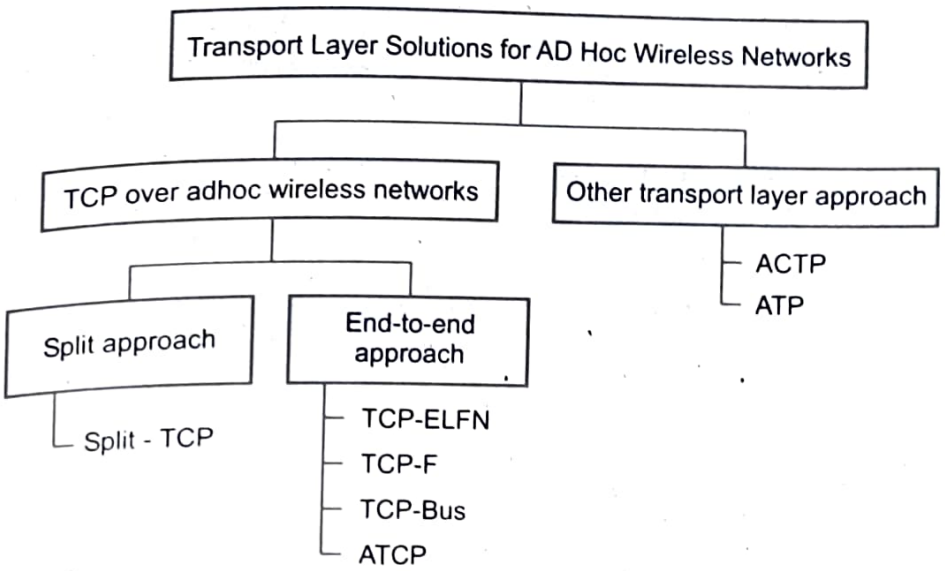



**Fig. 3.6.1 : Classification of transport layer solutions**

## 3.7 TCP over Adhoc Wireless Networks

- TCP is reliable, end-to-end, connection-oriented transport layer protocol that provides a byte stream based service.
- Major responsibilities of TCP include congestion control, flow control, in-order delivery of packets and reliable transportation of packets.

### 3.7.1 Traditional TCP

- TCP handles the congestion control in the following way.
- TCP regulates the number of packets sent to the network by changing the size of the congestion window. Initially, at the beginning of the TCP session, the size of congestion window is set to one maximum segment size (MSS).
- If the acknowledgment (ACK) is received during the retransmission time out period (RTO), size of the congestion window is doubled until the size reaches slow-start threshold.

- After the slow-start threshold is reached, congestion window increases linearly, by one MSS for every received ACK. If the ACK is not received in time, TCP assumes that the packet is lost and invokes congestion control mechanism, slow-start threshold is halved and the size of congestion window is decreased to one MSS.
- The congestion handling is the biggest single issue that makes the traditional TCP a poor choice for ad hoc wireless networks. TCP has been designed for wired networks that have very low bit error rates, thus when the packet loss is encountered, TCP assumes that there is significant problem in the network and initiates aggressive congestion control.
- In ad hoc wireless networks packet loss can frequently occur for many reasons.
  1. The bit error rates are generally much higher in wireless network.
  2. The nodes are constantly moving and path breaks can occur frequently.
- If the packet loss occurs frequently, the size of congestion window in TCP will stay at very low level most of the time and this naturally decreases the throughput of the network significantly. In addition, after a route reconfiguration, new route may accept higher throughput.

b. However, TCP does not take this into account. The problem worsens when the path length increases, since the increased path length increases the probability that a path break occurs somewhere along the path. With a path length of just 4 hops and link break probability of 10 % for each link, throughput of TCP decreases to about 20 % of the original.

## 3.7.2 Why does TCP Not Perform Well in Ad hoc Wireless Networks ?

- The following reasons are behind the poor performance of TCP in ad-hoc networks :

| Reasons | Remarks |
|---|---|
| Misinterpretation of packet loss | • Wired networks: packets losses are mainly due to congestions; |
| | • Ad-hoc wireless networks: high packet loss due to high BER; collisions due to hidden terminal problem; interference, large-scale and small-scale propagation phenomenons. |
| Frequent path breaks | • Due to topology changes, route reconfigurations.<br>• Slow start because of inefficient use of the resources. |
| Effects of contention | With the increase in the number of hops in the path throughput decreases xponentially. |

| | |
|---|---|
| Misinterpretation of congestion window | • Congestion window is the rate that is acceptable for the network and the receiver. |
| Asymmetric link behavior | • Sometimes wireless links are directional in ad-hoc networks leading to :<br>a. Delivery of a packet to a node and failure in the delivery of ACK back;<br>b. Congestion control algorithm could be invoked due to this;<br>c. Some routing protocols require the forward and backward paths to be the same. |
| Resource contention | • Both DATA and ACK require RTS-CTS-DATA-ACK at the data-link layer;<br>• Contention for resources in the same link at forward and backward paths; |
| Multipath routing | • Some routing protocols use multiple paths between the source and destination leading to high number of out-of-order packets leading to DUPACKs. |

## 3.7.3 Feedback-based TCP (TCP-F)

- TCP-F requires the following to enhance performance :
  a. Support of reliable data-link layer protocols;
  b. Routing support to inform the TCP sender about path breaks;
  c. Routing protocol is expected to repair the broken path within a reasonable time.
- The aim of TCP-F is to minimize the throughput degradation resulting from path breaks. Fig. 3.7.1 shows link break in ad-hoc network.

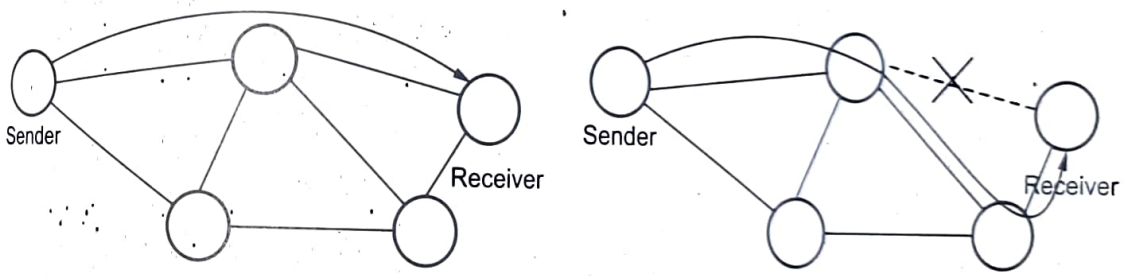



**Fig. 3.7.1 : Link break in ad-hoc network**

- In TCP-F an intermediate node upon detection of the link break, following things occurs :
  a. Obtains information from TCP-F sender's packets routed via this node;
  b. Generates a route failure notification (RFN) packet;

c. Routes this packet to the TCP-F sender;

d. Does not forward any packet from this connection;

e. Updates its routing table;

f. Stores information about generation of a RFN packet.

- Any intermediate node that forwards the RFN packet :
  a. If this node has an alternative route to destination then discards the RFN packet and uses this path to forward other packets. This allows to reduce an overhead involved in route re-establishment.
  b. If this node does not alternate route to destination then updates its routing table and forwards the RFN packet to the source.
- When TCP-F sender receives the RFN packet it enters the so-called snooze state then stops sending packet to the destination; cancels all the timers; freezes the congestion window and sets up a route failure timer. When failure timer expires TCP-F enters the connected state.
- If the broken links rejoins or intermediate node obtains a new path to destination then route reestablishment notification (RRN) is sent to TCP-F sender.
- Fig. 3.7.2 shows operation of TCP-F.

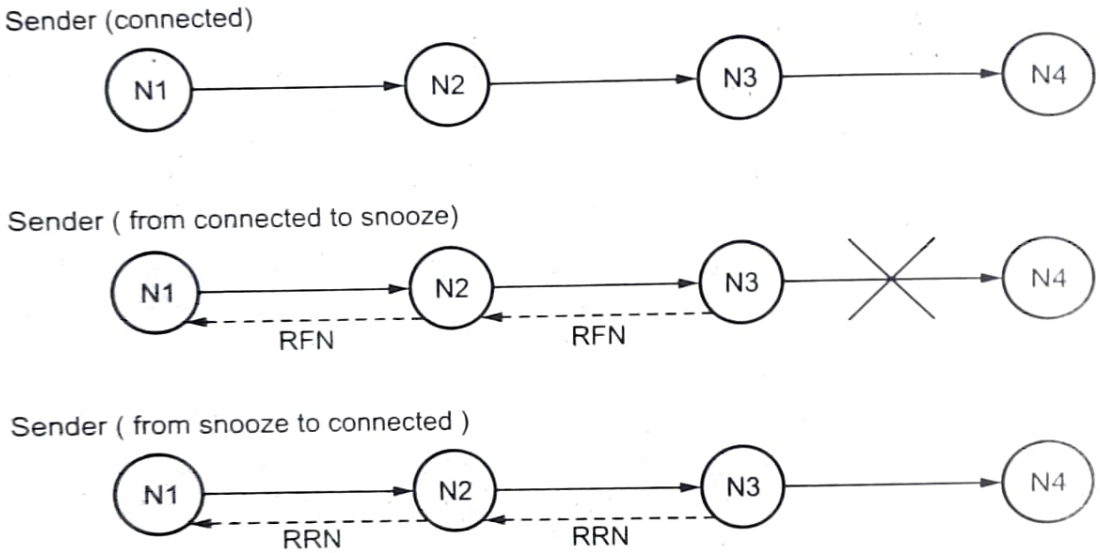



**Fig. 3.7.2 : Operation of TCP-F**

- When the sender receives RRN packet :
  a. Reactivates all timers and congestion window assuming that the network is back;
  b. Starts transmitting data available in the buffer;
  c. Takes care of packets lost due to path break.

**Advantages :**

1. Provides simple feedback to minimize problems due to link breaks;
2. Still allows congestion control occurring due to buffer overflows;

**Disadvantages :**

a. Requires merging of transport and network layer features;
b. Requires ability of nodes to detect path breaks;
c. Requires ability of routing protocols to repair a link within a reasonable time;
d. Requires ability of node to determine the TCP-F sender;
e. Reactivated congestion window may not reflect allowed network rate.

## 3.7.4 TCP with Explicit Link Failure Notification (TCP-ELFN)

- It handles explicit link failure notification.
- When an intermediate node detects a link failure then it sends an explicit link failure notification (ELFN) to TCP-ELFN sender. Either sending an ICMP destination unreachable message (DUR) or inserting info regarding link break in RouteError message of the routing protocol.
- Once the TCP-ELFN sender receives the ELFN packet, it disables its retransmission timer and CW and enters a standby state. Fig. 3.7.3 shows example of TCP-ELFN.

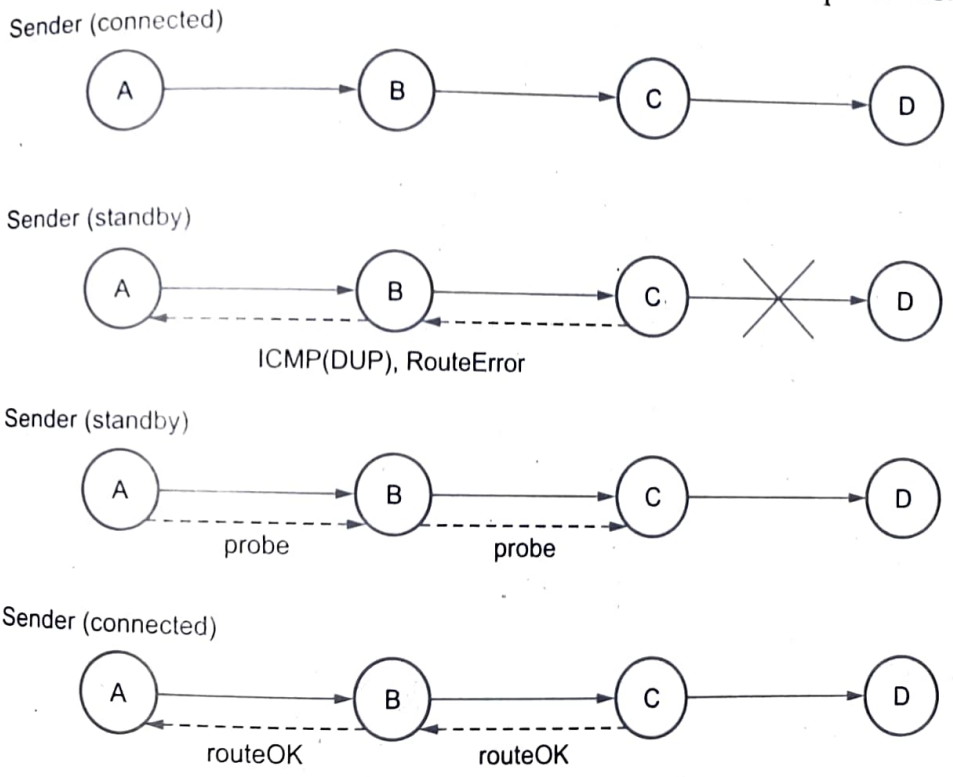



**Fig. 3.7.3 : Example of TCP-ELFN**

- Being in standby state the TCP-ELFN sender :
  a. Periodically originates probe packets to see if a new route is established;
  b. When ACK for a probe packet is received TCP-ELFN continues to perform as usual.

**Advantages :**

a. Improves the TCP performance by decoupling the path break information from the congestion information by the use of ELFN.

b. Less dependent on the routing protocol and requires only link failure notification.

**Disadvantages**

1. When the network is partitioned, the path failure may last longer.
2. The congestion window after a new route is obtained may not reflect the achievable transmission rate acceptable to the network and TCP receiver.

## 3.7.5 TCP with Buffering Capability and Sequence Information (TCP-BuS)

- **Characteristics :**
  a. Protocol tries to notify the source about the path breaks using the feedback info;
  b. This protocol is more dependent on routing protocol compared to TCP-F and TCP-ELFN.
- TCP-BuS was proposed for usage with Associativity-Based Routing (ABR) and uses localized query (LQ) message of ABR; REPLY message of ABR.
- Both these messages are modified to carry TCP connection and segment information. Fig. 3.7.4 shows basic definitions for TCP-BuS protocol.

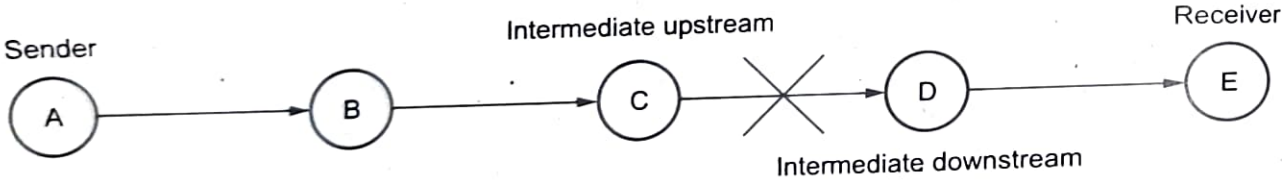



**Fig. 3.7.4 : Basic definitions for TCP-BuS protocol**

- When a link break is detected, **intermediate downstream node** generates a route notification (RN) message to TCP-BuS receiver. Route notification includes the sequence number of packet belonging to that flow in the head of its queue. All packets belonging to this flow are discarded at all intermediate nodes that forward RN.

- When a link break is detected, **intermediate upstream node :**
  a. Generate explicit route disconnection notification (ERDN);
  b. When ERDN is received by the sender, it stops sending and freezes timers CW;
  c. All packets in transit nodes are buffered, till new partial path is found by source of ERDN;
  d. Tries to find a new (partial) route to the TCP-BuS receiver;
  e. If it finds, explicit route successful notification packet (ERSN) to the sender is sent.
- Fig. 3.7.5 shows operation of TCP-BuS connection.

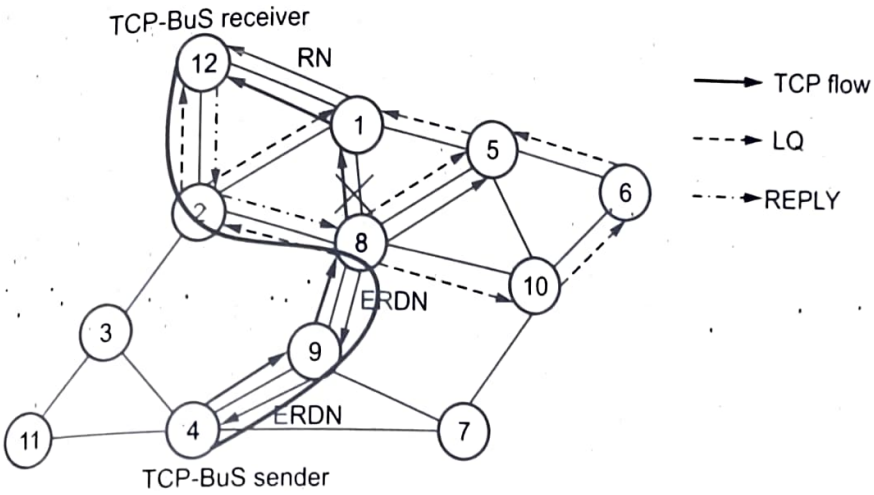



**Fig. 3.7.5 : Operation of TCP-BuS connection**

**Advantages**

1. Performance improvement and avoidance of fast retransmission.
2. Use on-demand routing protocol.

**Disadvantages**

i. Increased dependency on the routing protocol and the buffering at the intermediate nodes.

ii. The failure of intermediate nodes may lead to loss of packets.

iii. The dependency of TCP-BuS on the routing protocol many degrade its performance.

## 3.7.6 Ad hoc TCP

- Ad hoc TCP (ATCP) relies on a network layer feedback to make the TCP sender aware of the status of the network path. ATCP takes advantage of Explicit Congestion Notification (ECN) flags and ICMP destination unreachable (DUR) messages to detect network congestion and path breaks.
- ATCP is not a full replacement to the TCP, instead it operates between the TCP and the network layer. Thus, ATCP is fully compatible with the traditional TCP and the ATCP support is only required for the sender.
- When packet loss is detected or packets arrive out-of-order to the destination, ATCP simply retransmits missing packets without invoking congestion control mechanism. This provides a performance advantage against traditional TCP that invokes congestion control every time the packet loss or out-of-order packets are detected.
- When the ATCP sender receives ECN message, it moves to the congested state where it lets TCP invoke congestion control normally.
- When DUR packets are received, ATCP moves in to disconnect state where it ceases to send packets. After the connection is re-established, ATCP sets the size of the congestion window to one in order to make TCP to determine optimal congestion window size for a new connection.

**Advantages**

1. Compatible with traditional TCP;
2. Maintains the end-to-end semantics of TCP;

**Disadvantages**

1. Requires support from routing protocol (route changes, partition detection);
2. Requires changes to interface functions.

## 3.7.7 Split TCP

- The following are two major problems with TCP.
  1. Degradation of throughput with increase in the path length :
  2. Unfairness among TCP flows.
- Split-TCP provides a solution to this problem by separating transport layer objectives into congestion control and end-to-end reliability. The idea is that the congestion control is mostly a local phenomenon and thus it requires local solution. The reliability is a end-to-end requirement and thus it requires end-to-end acknowledgments.

- Split-TCP also splits TCP connection into a set of shorter concatenated TCP connections, intermediate nodes, also called as proxy nodes, are end point of these short connections. The number of proxies is determined by the path length, longer paths will have a higher amount of proxies to keep the length of individual connection short.

**Advantages**

1. Improved throughput.
2. Improved throughput fairness.
3. Lessened impact of mobility.

**Disadvantages**

1. It requires modifications to TCP protocol.
2. The end-to-end connection handling of traditional TCP is violated.
3. The failure of proxy nodes can lead to throughput degradation.

## 3.8 Wireless Sensor Network

**SPPU : Dec.-16**

- A wireless sensor network consists of group of sensor nodes to perform distributed sensing task using wireless medium.
- Sensor is one type of transducer. It converts one form of energy into electrical energy. Sensing capabilities should be distributed and coordinated amongst the sensor nodes.
- Sensing units consists of two subunits : Sensors and anlog-to-digital converters. The analog signal produced by the sensors are converted to digital signals by the ADC, and fed into the processing unit.
- A wireless sensor network is a collection of nodes organized into a cooperative network. Each node consits of processing capability. It consists of multiple types of memory with an RF transceiver, power source and various sensors.
- Large number of sensors forms a network to cooperatively monitor large or complex physical enviroments.
- Sensor node acquired information and sends to base station using wireless communication. Base station propagates the information to remote devices for storage, analysis and processing.
- Location finding system is needed to determine the location of sensor nodes with high accuracy; mobilizer may be needed to move sensor nodes when it is required to carry out the task.

- To provide data to remote end-users, the base station includes WAN connectivity and persistent data storage for the collection of sensor patches.
- Power management is only problem with wireless sensor network. Battery is used for provide power to the sensor node.

### 3.8.1 Functions

- A wireless sensor network is a collection of nodes organized into a co-operative network. Each node consists of processing capability, may contain multiple types of memory, have a RF transceiver and a power source and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad-hoc fashion.
- WSN is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations.
- A communication network is composed of nodes, each of which has computing power and can transmit and receive messages over communication links, wireless or cabled.
- The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation and traffic control.
- Possible applications
  1. **Military :** Battlefield surveillance, biological attack detection, targeting.
  2. **Ecological :** Fire detection, flood detection, agricultural uses.
  3. **Health related :** Human physiological data monitoring.
  4. **Miscellaneous :** Car theft detection, inventory control, home applications.
- Sensor network development rely on advances in sensing, communication and computing. To manage scarce WSN resources adequately, routing protocols for WENs need to be energy-aware.
- Data-centric routing and in-network processing are important concepts that are associated intrinsically with sensor networks. The end-to-end routing schemes that have been proposed in the literature for mobile ad-hoc networks are not appropriate WSNs; data-centric technologies are needed that perform in-network aggregation of data to yield energy efficient dissemination.
- A sensor node typically has embedded processing capabilities and onboard storage; the node can have one or more sensors operating in the acoustic, seismic,

radio (radar), infrared, optical, magnetic and chemical or biological domains. The node has communication interfaces, typically wireless links, to neighbouring domains. The sensor node also often has location and positioning knowledge that is acquired through a Global Positioning System (GPS) or local positioning algorithm.

- Sensor nodes are scattered in a special domain called a sensor field. Each of the distributed sensor nodes typically has the capability to collect data, analyze them and route them to a designated sink point.
- Fig. 3.8.1 shown a typical WSN arrangement.

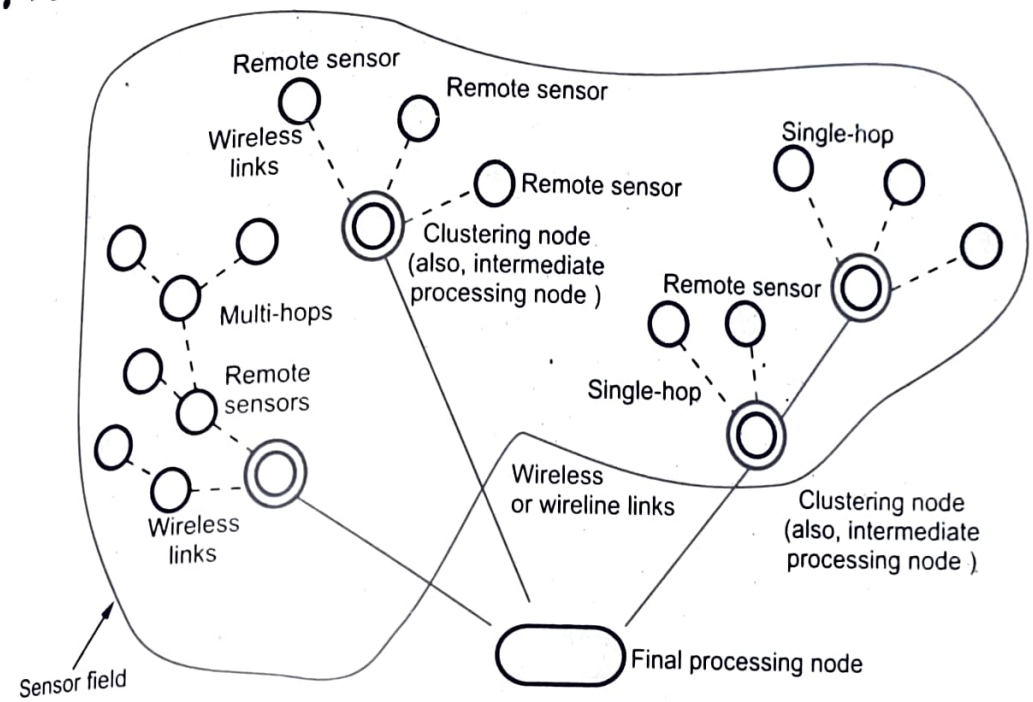



**Fig. 3.8.1 WSN arrangement**

- Node location and fine grained time are essential for proper operation of a sensor network; this is almost the opposite of the prevalent Internet architecture, where server location is immaterial to a large degree and where latency is often not a key consideration or explicit design objective.
- In sensor networks, fine grained time synchronization and localization are needed to detect events of interest in the environment under observation. Location needs to be assess detection levels across a related set of sensors.
- Localization is used for functionality such as beam forming for localization of target and events, geographical forwarding and geographical addressing.

## 3.8.2 Sensor Node Architecture

Some of the **characteristic features of sensor networks** include the following :

- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network changes very frequently.
- Sensor nodes are limited in power, computational capacities and memory.
- Sensor nodes may not have global identification because of the large amount of overhead and the large number of sensors.
- Sensor networks require sensing systems that are long-lived and environmentally resilient. Unattended, self-powered low-duty-cycle systems are typical.

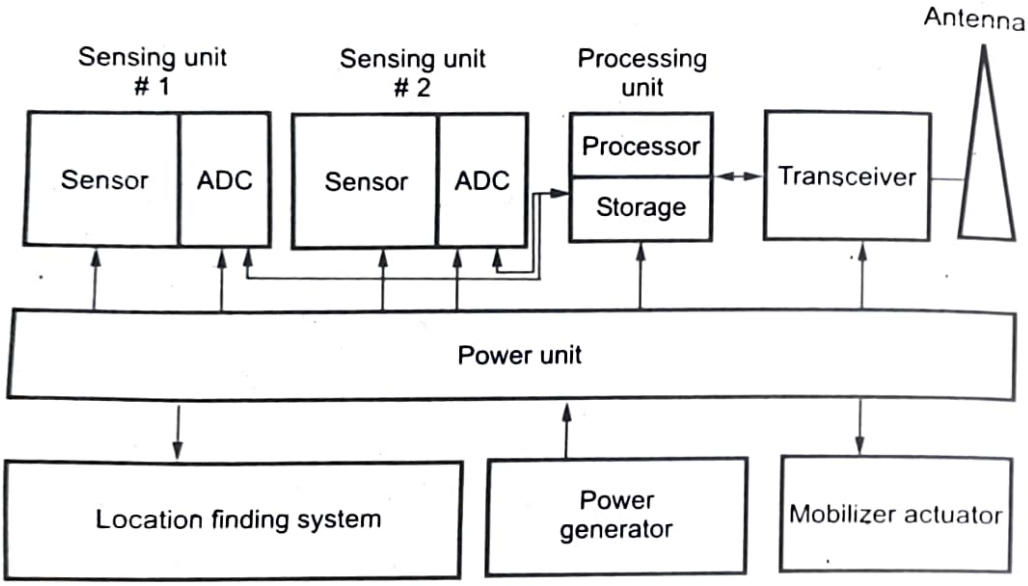



**Fig. 3.8.2 Typical sensing node**

- Fig. 3.8.2 shows a typical sensing node. The components of a sensing node include the following :
  1. A sensing and actuation unit (single element or array)
  2. A processing unit
  3. A communication unit
  4. A power unit
  5. Other application-dependent units.
- *Power consumption* is often an issue that needs to be taken into account as a *design constraint*. In most instances, communication circuitry and antennas are the *primary elements* that draw most of the energy. Sensors are either passive or *active devices*. Passive sensors in element form include seismic, acoustic, strain,

humidity and temperature-measuring devices. Passive sensors in array form include optical and biochemical measuring devices. Passive sensors tend to be low-energy devices. Active sensors include radar and sonar; these tend to be high-energy systems. Basic sensor node comprises five main components.

1. Controller
2. Memory
3. Sensors and actuators
4. Communication
5. Power supply.

Fig. 3.8.3 shows the overview of main sensor node hardware components.

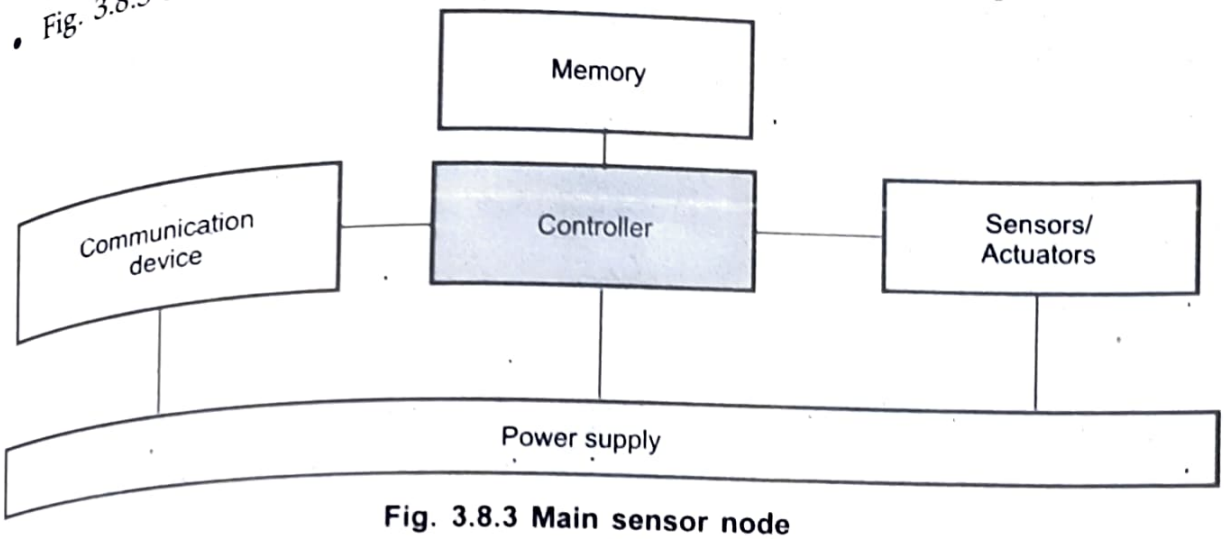



**Fig. 3.8.3 Main sensor node**

1. **Controller** : A controller to process all the relevant data, capable of executing arbitrary code.
2. **Memory** : Some memory to store programs and intermediate data; usually, different types of memory are used for programs and data.
3. **Sensors and actuators** : The actual interface to the physical world, the device that can observe or control physical parameters of the environment.
4. **Communication** : Turning nodes into a network requires a device for sending and receiving information over a wireless channel.
5. **Power supply** : Some forms of batteries are necessary to provide energy.

The energy consumed by an interface depends on its operating mode :

1. **Sleep Mode** : An interface can neither transmit nor receive. It is very low energy consumption.
2. **Idle Mode** : An interface can transmit or receive data at any time. it consumes more energy than it does in the sleep state.
3. **Receive Mode and Transmit Mode** : The energy consumption is of the same order of magnitude than idle state. Transmitting requires more energy than receiving, but the difference is generally less than a factor of two.

**Review Question**

1. *Describe each component in sensor node architecture.*

**SPPU : Dec.-16 (End Sem), Marks 8**

## 3.9 Sensor Network Architecture

**SPPU : Dec.-14**

- Sensor network architectures uses two main concept **source and sink.**
- **Source** provides information to network and **sink** receive information from network. Sink receives the information from source entity. Example of source is sensor node acts as source entity. Examples of sink are sensor network, PDA and entity outside home network. Fig. 3.9.1 shows three types of sink.

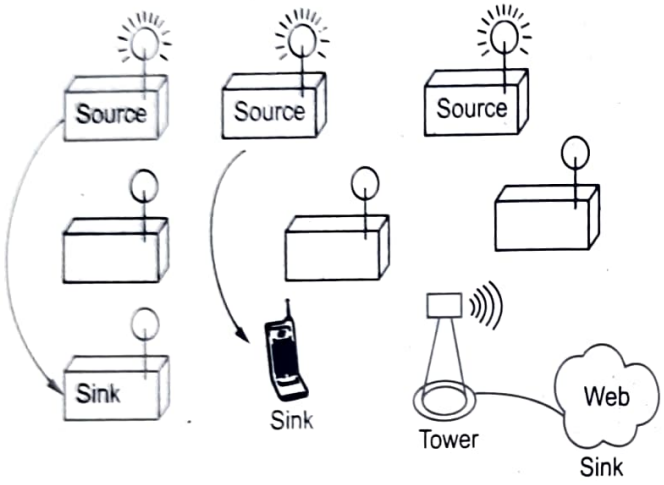



**Fig. 3.9.1 Types of sink**

- If direct communication is not possible because of distance limit or obstacles, then multihop communication method is used. Multihop communication uses store and forward fashion. Node has to receive a packet properly before it can forward next entity.
- Proper placing of intermediate sensor node is necessary. Fig. 3.9.2 shows multihop communication network.

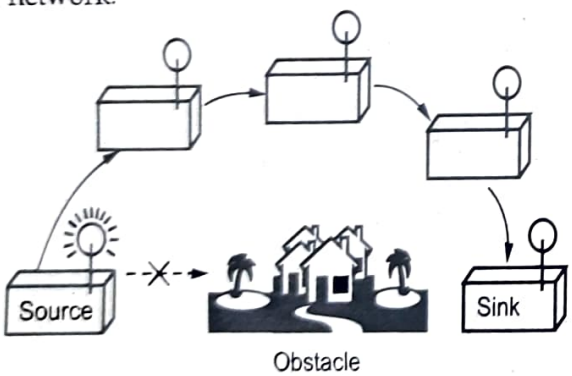



**Fig. 3.9.2 Multihop communication**

- Traditional transport protocols such as UDP and TCP cannot be directly implemented in sensor networks because if a sensor node is far away from the sink then the flow and congestion control mechanism cannot be applied for those nodes.
- UDP on the other hand has a reputation of not providing reliable data delivery and has no congestion or flow control mechanisms which are needed for sensor networks.

## 3.9.1 Types of Mobility

- Wireless communication is its ability to support mobile participants. Three type mobility supported by wireless network.

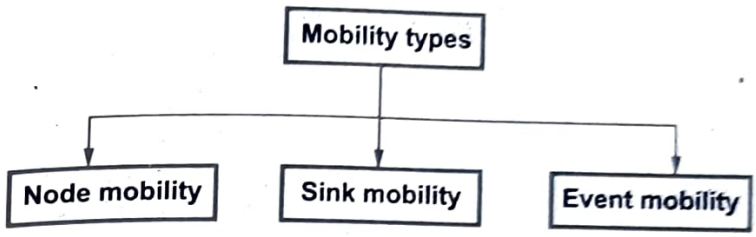



**Fig. 3.9.3**

1. **Node mobility :** Sensor node is best example of node mobility. Most of the applications are dependent on node mobility. Placement and node movement is also important factor. In video surveillance, node mobility is important but in environmental control application it not matters that much. Node must be performing correct functions.
2. **Sink mobility :** Here we consider information sink as a mobile. Suppose you are walking on the street and your PDA is connected to network and request for some information. PDA will interact with one of the access point nearby and you will get the information. Most of the time, consecutive interactions can be treated as separate, unrelated requests. If required information is not available at local place then it must be retrieved from some remote part of the network. Even if the user moves from one place, then also information is given to user in new place.
3. **Event mobility :** Event mobility is used in tracking applications. Numbers of sensors are used for this purpose.

Different WSN nodes become "responsible" for surveillance of such an event.

## 3.9.2 Topologies

- Wireless sensor networks use three basic networking topologies;
  1. Point-to-point
  2. Star
  3. Mesh

### Point-to-Point Topology

- Point-to-point topology is simply a dedicated link between two points. Networks allow each node to communicate directly with another node without needing to go through a centralized communications hub.
- Fig. 3.9.4 shows point-to-point topology.

**Fig. 3.9.4 Point-to-point topology**

Each device is act as both a "client" and a "server" to the other nodes on the network.

- This topology is most reliable because there is only one single point of failure in the topology.

### Star Topology

- Star topology is also called point-to-multipoint or Multi-drop networks. Fig. 3.9.5 shows star topology.

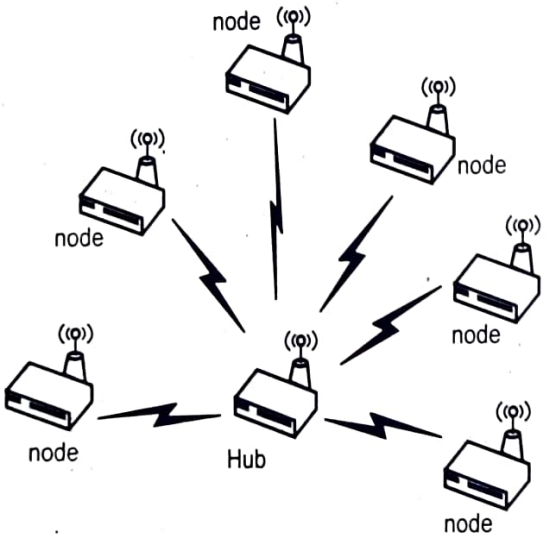



**Fig. 3.9.5 Star topology**

- Nodes are connected to a centralized communications hub. There is no direct communication between two nodes. The all communications must be routed through the centralized hub.
- In this topology, hub acts as a server and node as a client. One of the drawbacks of a star topology is that the central hub is a single point of failure; if a hub fails, the entire sub-network fails.
- Hybrid topology is possible by using point-to-point and star topology. It is also called tree topology.

Fig. 3.9.6 shows tree topology.

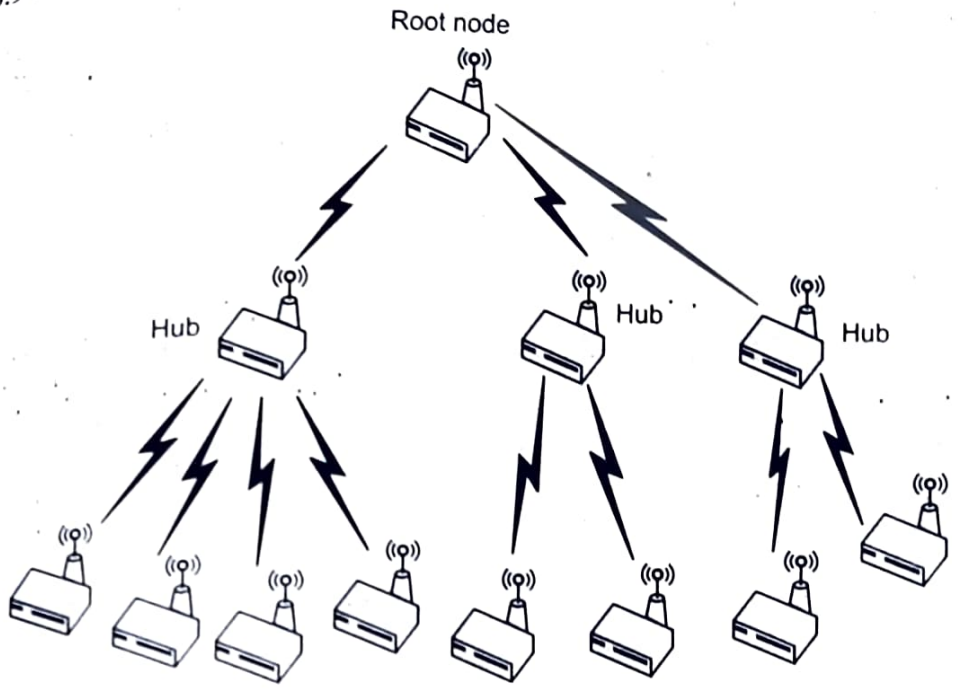



**Fig. 3.9.6 Tree topology**

**Mesh Topology**

- In the mesh topology, every node has multiple pathways to every other node.
- Each node is then able to communicate with each other as data is routed from node to node until it reaches the desired location.
- Fig. 3.9.7 shows mesh topology.

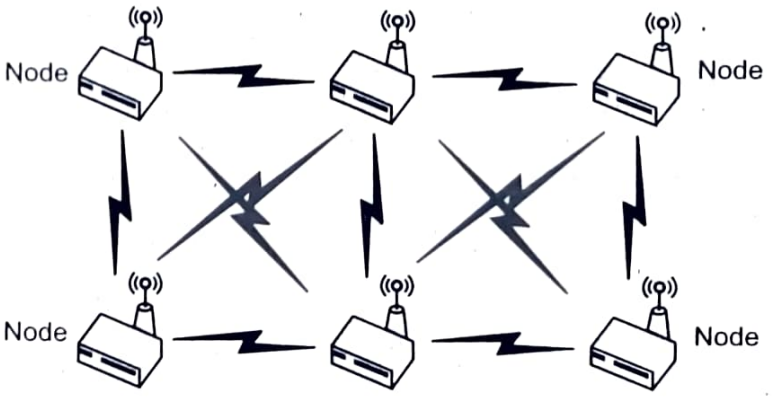



**Fig. 3.9.7 Mesh topology**

- This topology uses multi-hop routing algorithm that can be optimized for the lowest latency or lowest power.
- This type of network is one of the most complex and costly.

### 3.9.3 Issues and Challenges in Designing a Sensor Network

- Sensor nodes are randomly deployed and hence do not fit into any regular topology so it uses dynamic topology. Once deployed, they usually do not require any manual interaction. Operation like setup and maintenance of the network should be entirely autonomous.
- Sensor networks are dependent on infrastructure. So all routing algorithm and maintenance algorithms need to be distributed.
- Energy problem is the major factor because network uses battery for power supply for sensor node.
- Multihop networking may be adapted among sensor nodes to reduce communication link range and also density of sensor nodes should be high.
- Long range communication is typically point to point and requires high transmission power, with the danger of being eavesdropped. So we should consider short range transmission to minimize the possibility of being eavesdropped.
- Hardware device and software should be designed to save power.
- Sensor nodes should be able to synchronize with each other in a completely distributed manner, so that TDMA schedules can be imposed.
- 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.
- It is necessary to provide security for communication. Provision must be made for secure communication over sensor networks, especially for military applications which carry sensitive data.

1. **Centralized versus Distributed :** In centralized approach, center controller fails then network operation fails. Communication range is also limited so controlling of communication is big problem. Distributed approach is suitable for radio network. In this approach, all nodes operate cooperatively. There is problem with

distributed approach also. To combine centralized and distributed approach. For any local network operation, centralized approach is used.

2. **Inside network processing :** When network is design in distributed approach, then the sensor nodes take part in operating the network. Information processing is happens at node level.

3. **Aggregation :** Example of aggregation is inside network processing. Sink collect the information from the network and process it. Data Aggregation is defined as the process of aggregating the data from multiple sensors to eliminate redundant transmission and estimating the desired answer about the sensed environment, then providing fused information to the base station. Mechanisms for combining data at forwarding intermediate nodes so as to propagate only useful and not redundant information should be considered. Data aggregation is aimed at aggregating data coming from multiple sensors into useful non redundant fused data.

- **Distributed and collaborative signal processing :** For complex computations on a certain amount of data requires more energy. A sensor node has limited processing power. It affect on communication of sensor nodes. Instead of doing communication with other node, inode is busy with data processing. To avoid this, we uses distributed computation of a Fast Fourier Transform (FFT). Depending on where the input data is located, there are different algorithms available to compute an FFT in a distributed fashion.

- The concept of mobile code or agent-based networking is used executing program code. Code is sent from node to node so it is small in size. This program code is executed locally.

- **Exploit temporal and spatial correlation :** Signals are vary slowly. There is no need to transmit data at full speed all the time. Observe the neighbouring nodes signal and compare it. Only to transmit changed signals.

4. **Adaptive fidelity and Accuracy :** Accuracy is increases if we taken more and more samples. For function approximation application more sample is required. To collect the samples, large numbers of sensor nodes are used. For collecting samples, more energy is required. Consider the example of event detection. When there is no event, then send only short "all OK" messages. If any event occurs, increase rate of message exchanges.

5. **Data centric networking**

- In typical networks, network transactions are addressed to the identities of specific nodes. It is called a "node-centric" or "address-centric" networking paradigm.

- Unlike traditional networks, a sensor node may not need an identity. The sensor network applications are unlikely to ask the question : *What is the temperature at*

*sensor number13* ? Rather, applications focus on the data generated by sensors. Data is named by attributes and applications request data matching certain attribute values. The communication primitive in this system is a request : *Where are nodes whose temperatures recently exceeded 41 degrees* ? This approach decouples data from the sensor that produced it. This allows for more robust application design : Even if sensor number13 dies, the data it generates can be cached in other sensors for later retrieval.

- Thus focus networking transactions on the data directly instead of their senders and transmitters.
- Data-centric networking is implements in many ways.
  1. Overlay networks and distributed hash tables.
  2. Publish/Subscribe.
  3. Databases.

**Review Question**

1. *Explain WSN architecture in details.* **SPPU : Dec.-14, Marks 4**

## 3.10 Cluster Architecture Management

- Cluster management manages cluster quorum and cluster membership. Cluster manager (CMAN) performs cluster management. It is a distributed cluster manager and runs in each cluster node; cluster management is distributed across all nodes in the cluster.
- CMAN keeps track of cluster quorum by monitoring the count of cluster nodes. If more than half the nodes are active, the cluster has quorum. If half the nodes (or fewer) are active, the cluster does not have quorum, and all cluster activity is stopped.
- Cluster quorum prevents the occurrence of a "split-brain" condition - a condition where two instances of the same cluster are running. A split-brain condition would allow each cluster instance to access cluster resources without knowledge of the other cluster instance, resulting in corrupted cluster integrity.
- Quorum is determined by communication of messages among cluster nodes via Ethernet. Optionally, quorum can be determined by a combination of communicating messages via Ethernet and through a quorum disk. For quorum via Ethernet, quorum consists of 50 percent of the node votes plus 1. For quorum via quorum disk, quorum consists of user-specified conditions.

- CMAN keeps track of membership by monitoring messages from other cluster nodes. When cluster membership changes, the cluster manager notifies the other infrastructure components, which then take appropriate action.
- For example, if node A joins a cluster and mounts a GFS file system that nodes B and C have already mounted, then an additional journal and lock management is required for node A to use that GFS file system.
- If a cluster node does not transmit a message within a prescribed amount of time, the cluster manager removes the node from the cluster and communicates to other cluster infrastructure components that the node is not a member. Again, other cluster infrastructure components determine what actions to take upon notification that node is no longer a cluster member. For example, Fencing would fence the node that is no longer a member.

## 3.11 LEACH Clustering Protocol

- Low Energy Adaptive Clustering Hierarchy (LEACH) takes a hierarchical approach and organizes nodes into clusters. Within each cluster, nodes take turns to assume the role of a cluster head.
- LEACH uses TDMA to achieve communication between nodes and their cluster head.
- The cluster heads forwards to the base station messages received from its cluster nodes. The cluster head node sets up a TDMA schedule and transmits this schedule to all nodes in its cluster.
- The schedule prevents collisions among data messages. Furthermore, the schedule can be used by the nodes to determine the time slots during which they must be active. This allows each cluster node, except for the head cluster, to turn-off their radio components until its allocated time slots.
- LEACH assumes that cluster nodes start the cluster setup phase at the same time and remain synchronized thereafter one possible mechanism to achieve synchronization is to have the base station send out synchronization pulses to the all the nodes.
- To reduce inter-cluster interference, LEACH uses a transmitter-based code assignment scheme. Communications between a node and its cluster head are achieved using Direct-Sequence Spread Spectrum (DSSS), whereby each cluster is assigned a unique spreading code, which is used by all nodes in the cluster to transmit their data to the cluster head.

- Spreading codes are assigned to cluster heads on a first-in first-served basis, starting with the first cluster head to announce its position, followed by subsequent cluster heads.
- Nodes are also required to adjust their transmit powers to reduce interference with nearby clusters. Upon receiving data packets form its cluster nodes, the cluster head aggregates the data before sending them to the base station.
- The communication between a cluster head and a base station is achieved using fixed spreading code and CSMA.
- Before transmitting data to the base station, the cluster head must sense the channel to ensure that no other cluster head is currently transmitting data using the base station spreading code.
- If the channel is sensed busy, the cluster head delays the data transmission until the channel becomes idle. When this event occurs, the cluster head sends the data using the base station spreading code.
- In general, schedule-based protocols are contention free and as such, they eliminate energy waste caused by collisions. Furthermore, sensor nodes need only turn their radios on during those slots where data are to be transmitted or received.
- In all other slots, the sensor node can turn-off its radio, thereby avoiding overhearting. This results in low-duty-cycle node operations, which may extend the network lifetime significantly.
- Schedule based MAC protocols have several disadvantages, however, which limit their use in WSNs. The use of TDMA requires the organization of nodes into clusters. This hierarchical structure often restricts nodes to communicate only with their cluster head.
- Consequently, peer-to-peer communication cannot be supported directly, unless nodes are required to listen during all times slot. Most of the schedule based schemes depend on distributed, to align slots boundaries.
- Achieving time synchronization among distributed sensor nodes is difficult and costly, especially in energy-constrained wireless networks.
- Schedule-based schemes also require additional mechanisms such as FADMA or CDMA to overcome inter-cluster communications and interference.
- Finally, TDMA-based MAC-layer protocols have limited scalability and are not easily adaptable to node mobility and changes in network traffic and topology.

## 3.12 Short Answered Questions

**Q.1 What are the challenging issues in ad hoc network maintenance ?**

**Ans. : The challenging issues in ad hoc network are -**

1. Medium access scheme
2. Routing
3. Multicast routing
4. Transport layer protocol
5. Pricing schemes
6. Quality of service provisioning
7. Self-organization
8. Security
9. Addressing and service discovery
10. Energy management
11. Scalability

**Q.2 Why are ad hoc networks needed ?**

**Ans. : Need of Ad hoc network**

- Ad hoc networking is often needed where an infrastructure network cannot be deployed and managed.
- The presence of dynamic and adaptive routing protocols enables quick formation of ad hoc networks and is suitable for emergency situations like natural disasters, spontaneous meetings or military conflicts.

**Q.3 List the table driven protocols.**

**Ans. : The table driven protocols are -**

1. Destination-Sequenced Distance Vector (DSDV).
2. Cluster Head Gateway Switch Routing (CHGSR).
3. Wireless Routing Protocol (WRP).

**Q.4 List the source-initiated on-demand routing protocols.**

**Ans. : The source-initiated on-demand routing protocols are -**

1. Adhoc On-Demand Distance Vector Routing (AODV).
2. Dynamic Source Routing (DSR).
3. Temporarily Ordered Routing Algorithm (TORA).
4. Associativity Based Routing (ABR).
5. Signal Stability Based Routing (SSR).

**Q.5 Why does TCP not work well in ad hoc network ?**

**Ans. :** The TCP does not work well in ad hoc network because of the following reasons -

1. Misinterpretation of packet loss.
2. Frequent path breaks.
3. Effect of path length.
4. Misinterpretation of congestion window.
5. Asymmetric link behavior.
6. Unidirectional path.
7. Multipath routing.
8. Network partitioning and reemerging.
9. Use of sliding-window-based transmission.

## 3.13 Multiple Choice Questions

**Q.1 In ____an adversary node advertises routes to non-existent nodes, to the authorized nodes present in the network.**

a. routing table poisoning
b. route cache poisoning
c. routing table overflow
d. packet replication

**Q.2 The wireless transmission is divided into _____ .**

a. 3 broad groups
b. 6 broad groups
c. 9 broad groups
d. 8 broad groups

**Q.3 BTMA protocol comes under which mechanism ?**

a. Contention based protocols
b. Contention based protocols with reservation mechanisms
c. MAC protocols
d. Contention based protocols with scheduling

**Q.4 Classification of routing protocol is based on _____ .**

a. routing information update mechanism
b. protocol (DSDV) routing topology
c. utilization of specific resources
d. processing utilization

**Q.5 Which one is the first protocol proposed for ad hoc wireless networks ?**

a Wireless Routing Protocol (WRP)

b Destination sequenced distance-vector routing

c Source-Tree Adaptive Routing protocol (STAR)

d Dynamic Source Routing protocol (DSR)

**Q.6 In wireless ad-hoc network ____.**

a access point is must

b access point is not required

c nodes are not required

d all nodes are access points

**Answer Keys for Multiple Choice Questions :**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Q.1 | c | Q.2 | a | Q.3 | a | Q.4 | d |
| Q.5 | b | Q.6 | b | | | | |

❑❑❑