Unit III

3 Adhoc and WSN

3.1 : Infrastructure Network and Infrastructure-less Wireless Networks

Q.1 What is adhoc network ? List characteristic.

Ans. : • 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.

Q.2 Differentiate between infrastructure network and infrastructure-less networks ? What are issues in Adhoc wireless network ? ☞ **[SPPU : May-18, Dec.-19, End Sem, Marks 8]**

Ans. : • In Infrastructure network topology is static and infrastructure less network topology is dynamic.

- No bandwidth problem in infrastructure network but infrastructure less network may face bandwidth constrained.
- Limited physical security in infrastructure less network whereas proper security in infrastructure network.
- In Infrastructure network, planning of network is required before installation of components. In infrastructure less network automatically forms network and easy to change.

Also Refer Q.4

Q.3 Differentiate between infrastructure network and infrastructure-less networks ? What are the MAC layer and routing layer design goals ? ☞ **[SPPU : Dec.-18, End Sem, Marks 8]**

Ans. : Refer Q.2, Q.9 and Q.12

3.2 : Design Issues in Adhoc Wireless Network

Q.4 List the issues in adhoc wireless network.

Ans. : • Following are the main issues which affect design, implementation and performance of Adhoc 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

Q.5 Explain medium access scheme for adhoc wireless network.

Ans. : 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.

Q.6 Explain energy management and quality of service provisioning in adhoc network.

Ans. : 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.

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.

Q.7 What are the major challenges for routing protocol and requiremet in adhoc network.

Ans. : • 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 adhoc :
  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

3.3 : Adhoc Network MAC Layer

Q.8 Describe design goals for adhoc network MAC layer.

Ans. :

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.

Q.9 Explain design issues for adhoc network MAC layer.

Ans. : • **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 ofa 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 adhoc 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.

Q.10 Explain design issues and design goal in Adhoc network MAC layer. ☞ [SPPU : Dec.-22, End Sem, Marks 6]

OR Comment on adhoc network MAC layer with design issues, design goal. ☞ [SPPU : June-22, End Sem, Marks 9]

Ans. : Refer Q.8 and Q.9.

3.4 : MACAW Protocol

Q.11 Write short note on MACAW protocol.

☞ [SPPU : May-18,19, Dec.-19, End Sem, Marks 8]

Ans. : • 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. Q.11.1 shows the operation of the MACAW protocol.

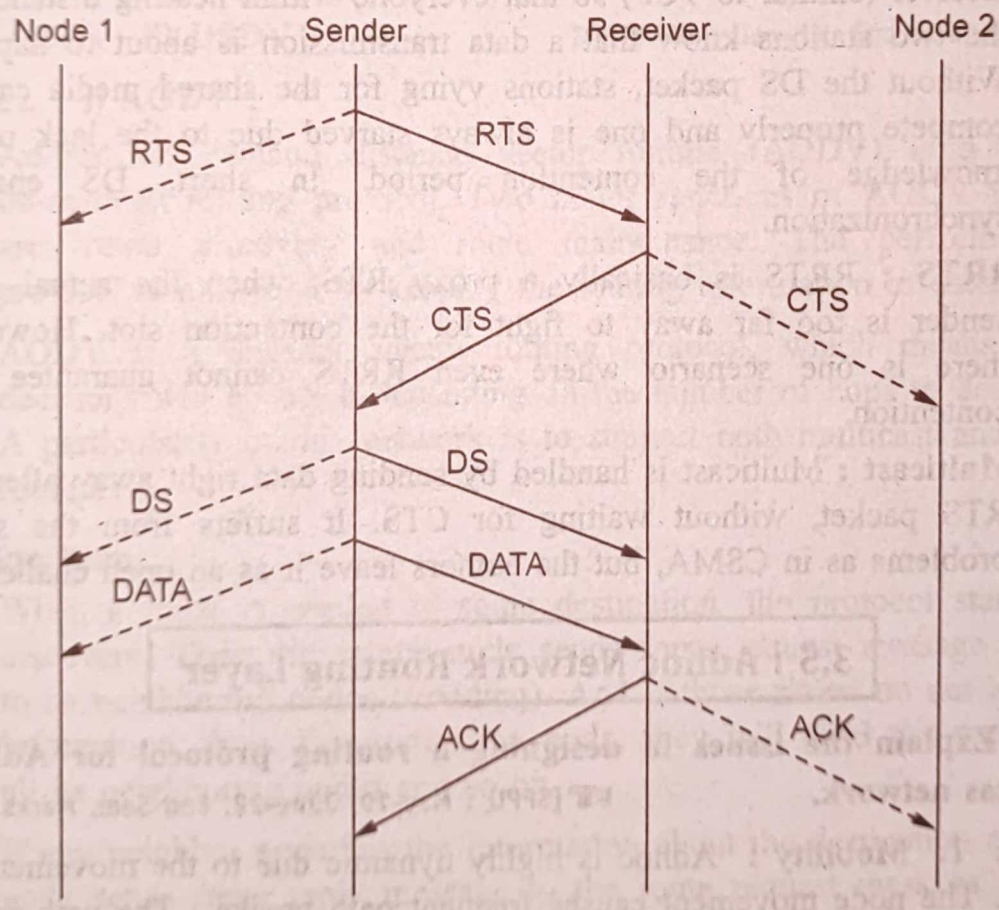


Fig. Q.11.1 Operation of the MACAW protocol

- 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 : Adhoc Network Routing Layer

Q.12 Explain the issues in designing a routing protocol for Adhoc wireless network. ☞ **[SPPU : May-19, June-22, End Sem, Marks 9]**

Ans. : 1. Mobility : Adhoc 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.

Q.13 Explain DSDV and AODV protocol in detail.

☞ [SPPU : May-19, Dec.-19, 22, End Sem, Marks 9]

OR Explain the connection establishment and data transfer phase in the following routing protocols with suitable diagram.

i) AODV ii) DSDV ☞ [SPPU : Dec.-18, End Sem, Marks 8]

Ans. : i) 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. Q.13.1, node-A needs to send a packet to node-I. A route request () packet will be generated and sent to B and D.
- B and D add A in their routing table, as a reverse route and forward a route request (RREQ) packet to their neighbours.

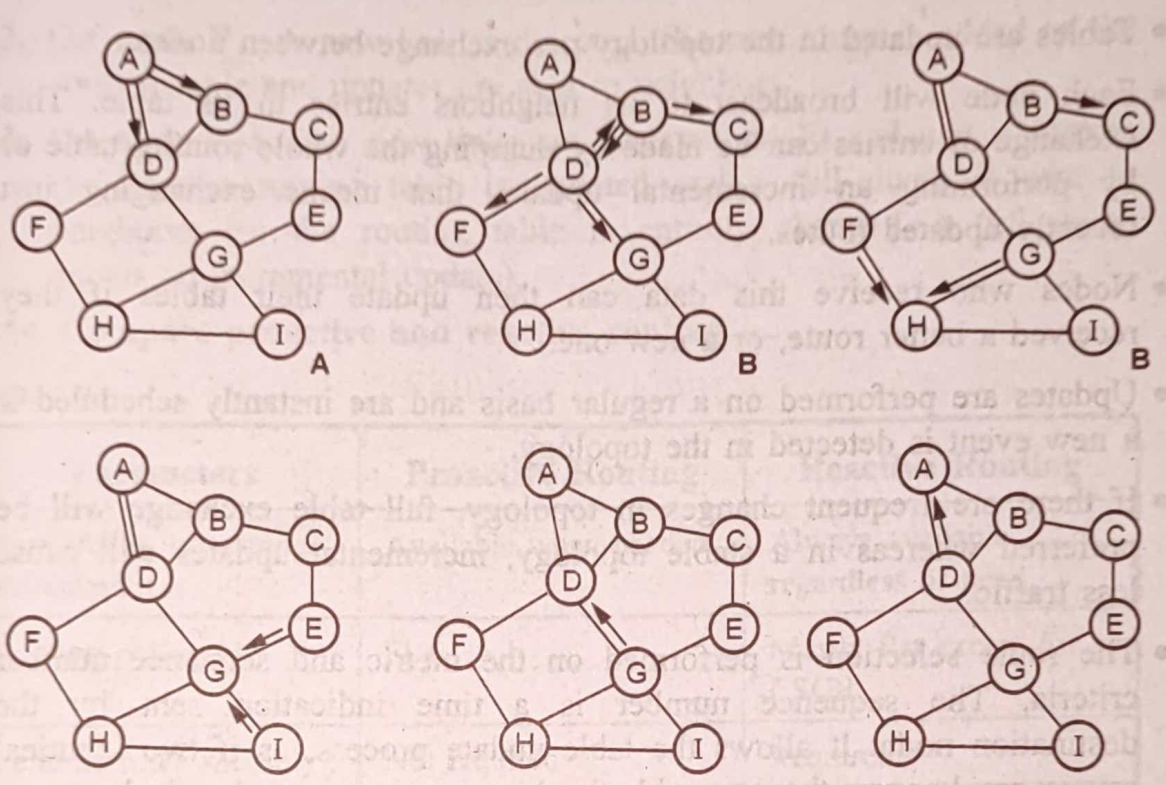


Fig. Q.13.1 AODV protocol

- 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.

ii) DSDV :

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

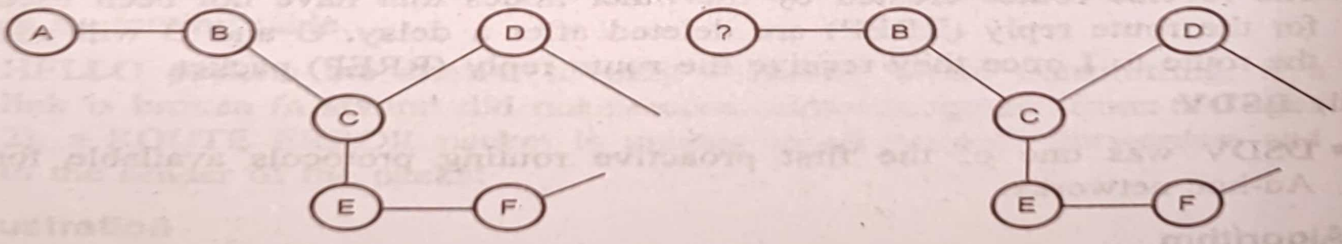
Algorithm

- 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. Q.13.2 (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. Q.13.2 (b). At this stage, the following events are detected and actions are taken :



(a) (b)

Fig. Q.13.2

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.
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).

Q.14 Compare proactive and reactive routing.

Ans. :

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.

Q.15 Explain routing protocols in detail.

☞ **[SPPU : May-18, End Sem, Marks 8]**

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

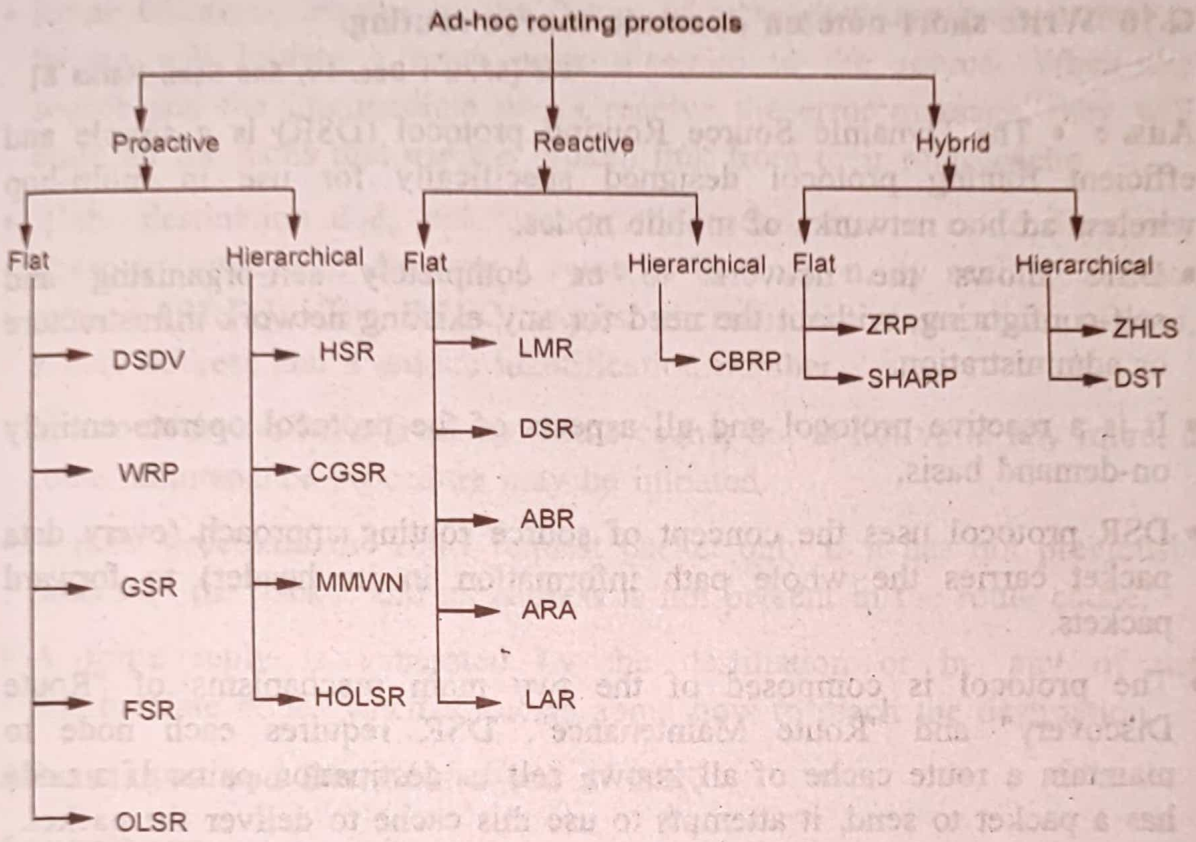


Fig. Q.15.1 Classification of routing protocols

- 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.

Q.16 Write short note on dynamic source routing.

☞ [SPPU : Dec.-19, End Sem, Marks 8]

Ans. : • 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.

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.

Q.17 Explain characteristics of AODV routing algorithm protocol.

☞ [SPPU : Dec.-22, End Sem, Marks 6]

Ans. :

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.

3.6 : Adhoc Transport Layer

Q.18 Explain issues in designing a transport layer protocol for adhoc wireless networks.

Ans. : • **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.

Q.19 List design goals of a transport layer protocol for adhoc wireless networks

Ans. :

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.

Q.20 Given classification of transport layer solutions in adhoc wireless network. Explain operation of TCP-F.

☞ **[SPPU : Dec.-18, End Sem, Marks 8]**

Ans. : Fig. Q.20.1 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.

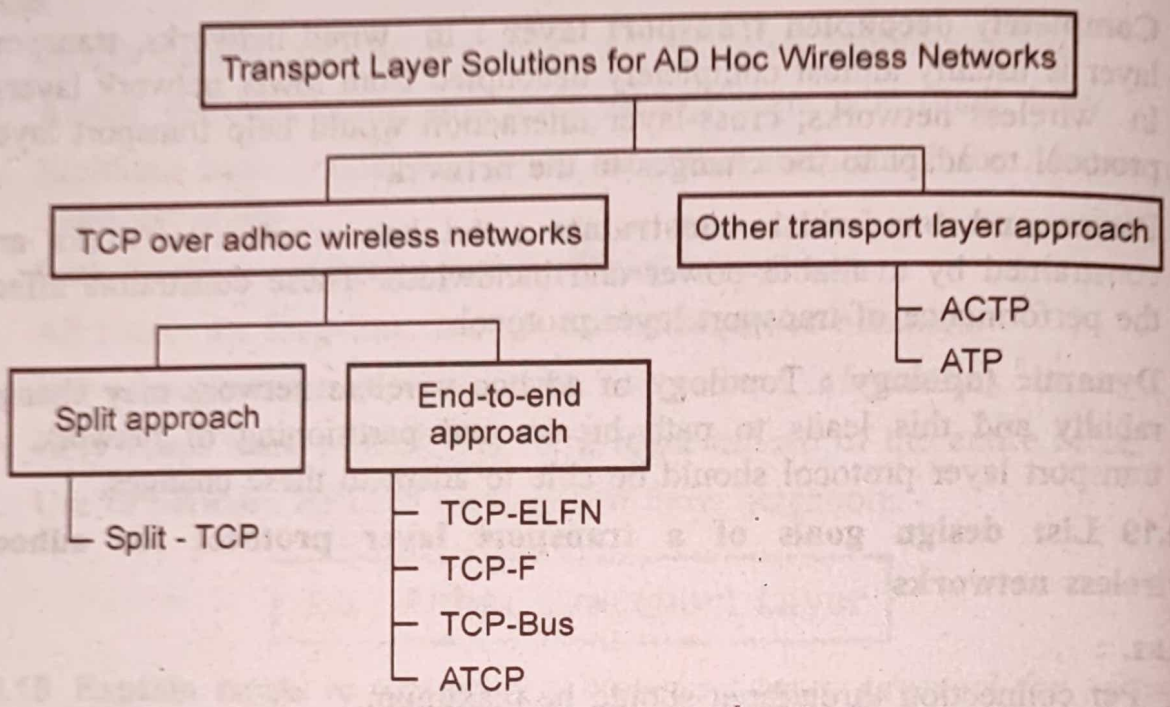


Fig. Q.20.1 Classification of transport layer solutions

Also Refer Q.21

3.7 : TCP Over Adhoc Wireless Network

Q.21 Explain operation of TCP-F. ☞ **[SPPU : May-18, End Sem, Marks 8]**

Ans. : • 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. Q.21.1 shows link break in ad-hoc network.

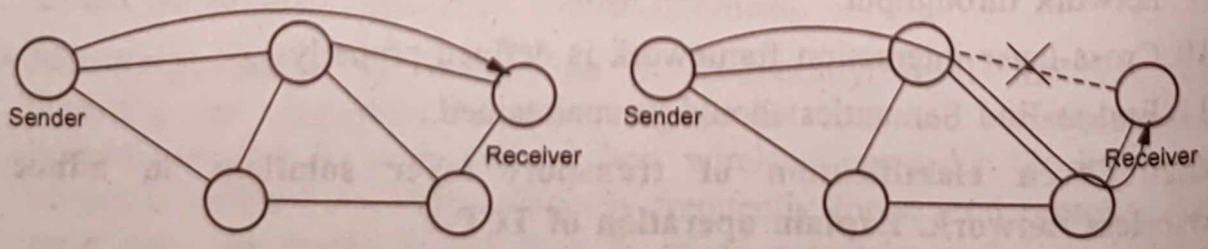


Fig. Q.21.1 Link break in ad-hoc network

- 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. Q.21.2 shows operation of TCP-F.

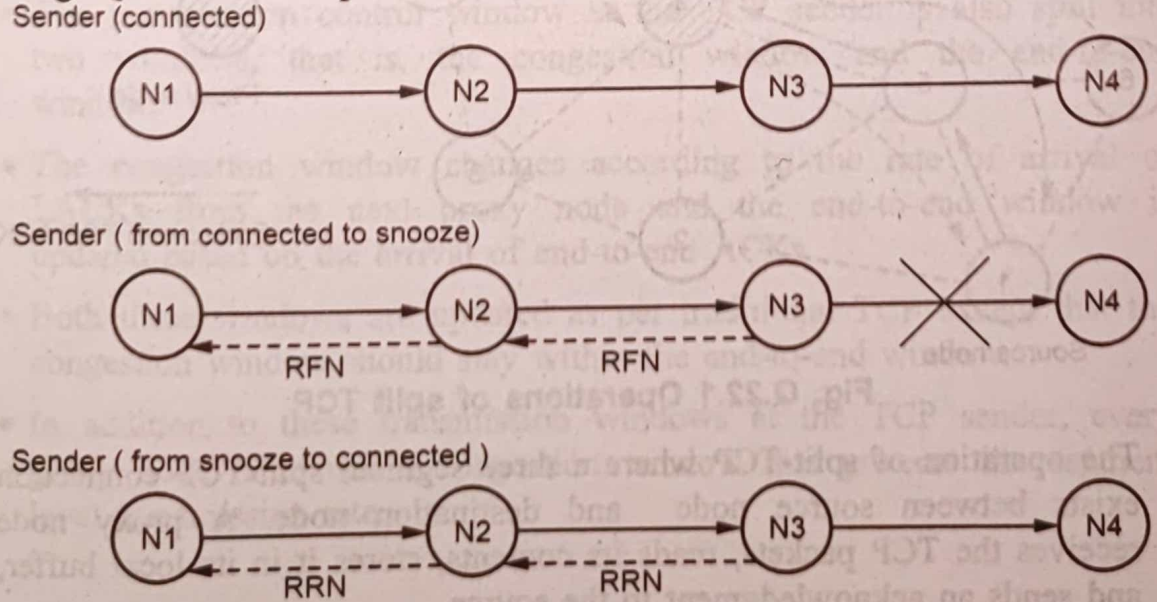


Fig. Q.21.2 Operation of TCP-F

- 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.

Q.22 Explain operations of split TCP. Explain its advantages and disadvantages. ☞ **[SPPU : May-19, End Sem, Marks 8]**

Ans. : • Split-TCP provides a unique solution to channel capture problem by splitting the transport layer objectives into congestion control and end-to-end reliability.

• Fig. Q.22.1 shows operations of split TCP.

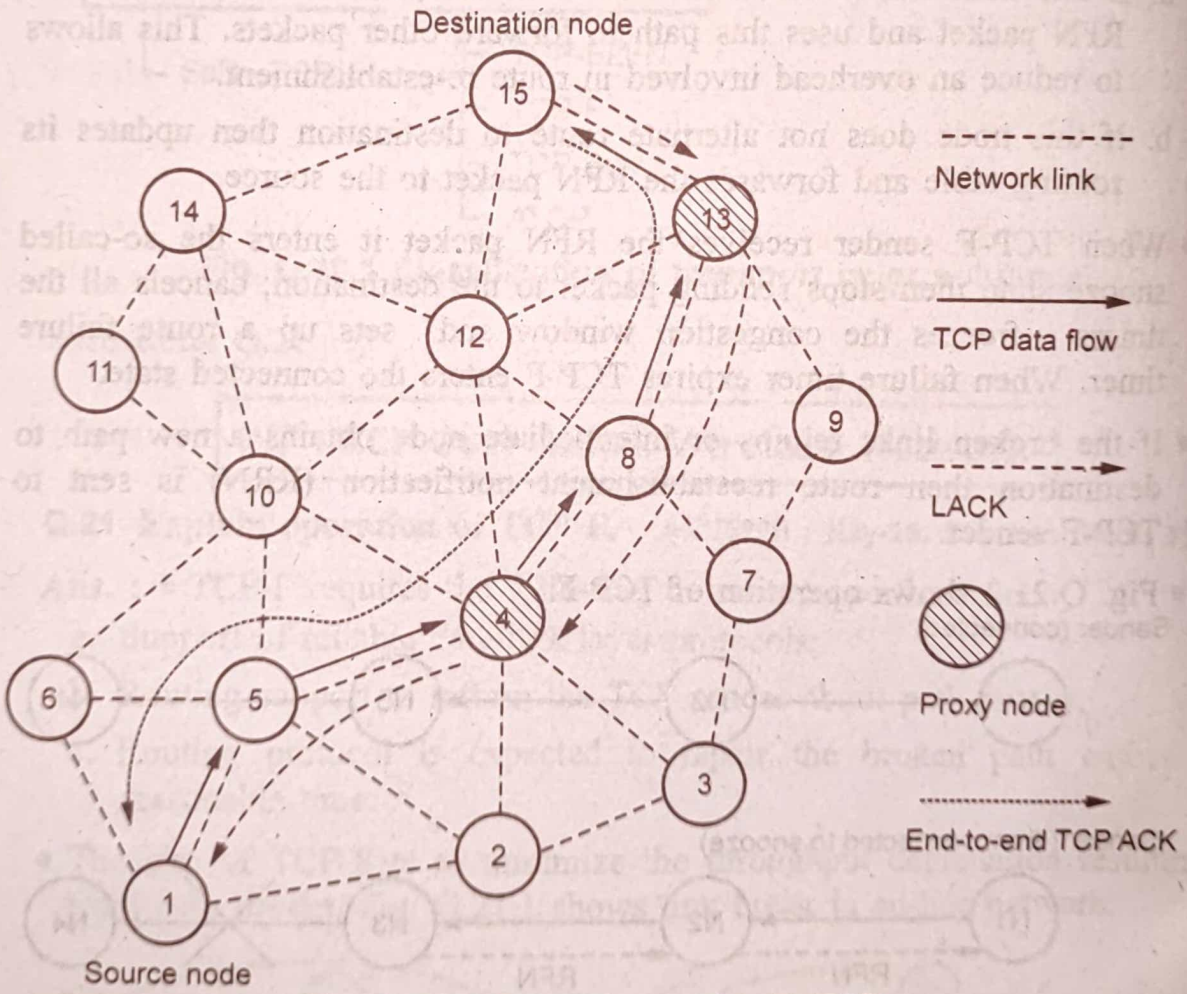


Fig. Q.22.1 Operations of split TCP

- The operation of split-TCP where a three segment split-TCP connection exists between source node and destination node. A proxy node receives the TCP packets, reads its contents, stores it in its local buffer, and sends an acknowledgment to the source.

- This acknowledgment called local acknowledgment (LACK) does not guarantee end-to-end delivery. The responsibility of further delivery of packets is assigned to the proxy node.
- A proxy node clears a buffered packet once it receives LACK from the immediate successor proxy node for that packet.
- Split-TCP maintains the end-to-end acknowledgment mechanism intact, irrespective of the addition of zone-wise LACKs. The source node clears the buffered packets only after receiving the end-to-end acknowledgment for those packets.
- Source Node initiates a TCP session to destination node. Node 4 and node 13 are chosen as proxy nodes. The number of proxy nodes in a TCP session is determined by the length of the path between source and destination nodes.
- Based on a distributed algorithm, the intermediate nodes that receive TCP packets determine whether to act as a proxy node or just as a simple forwarding node.
- In Fig. Q.22.1 the path between node 1 and node 4 is the first zone (segment), the path between nodes 4 and 13 is the second zone (segment), and the last zone is between node 13 and 15.
- The proxy node 4, upon receipt of each TCP packet from source node 1, acknowledges it with a LACK packet, and buffers the received packets. This buffered packet is forwarded to the next proxy node (in this case, node 13) at a transmission rate proportional to the arrival of LACKs from the next proxy node or destination.
- The transmission control window at the TCP sender is also split into two windows, that is, the congestion window and the end-to-end window.
- The congestion window changes according to the rate of arrival of LACKs from the next proxy node and the end-to-end window is updated based on the arrival of end-to-end ACKs.
- Both these windows are updated as per traditional TCP except that the congestion window should stay within the end-to-end window.
- In addition to these transmission windows at the TCP sender, every proxy node maintains a congestion window that governs the segment level transmission rate.

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.

Adhoc TCP :

- Adhoc 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

Q.23 Write short note on TCP-Bus.

Ans. : • 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. Q.23.1 shows basic definitions for TCP-BuS protocol.

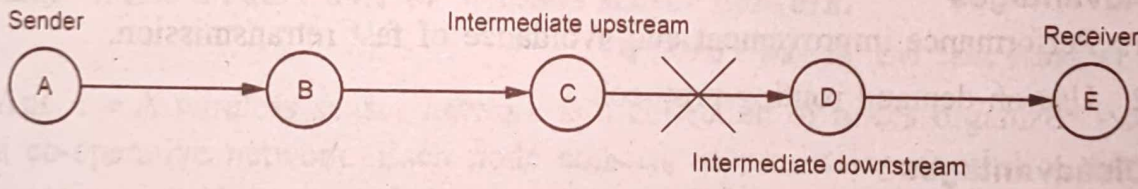


Fig. Q.23.1 : Basic definitions for TCP-BuS protocol

- 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. Q.23.2 shows operation of TCP-BuS connection.

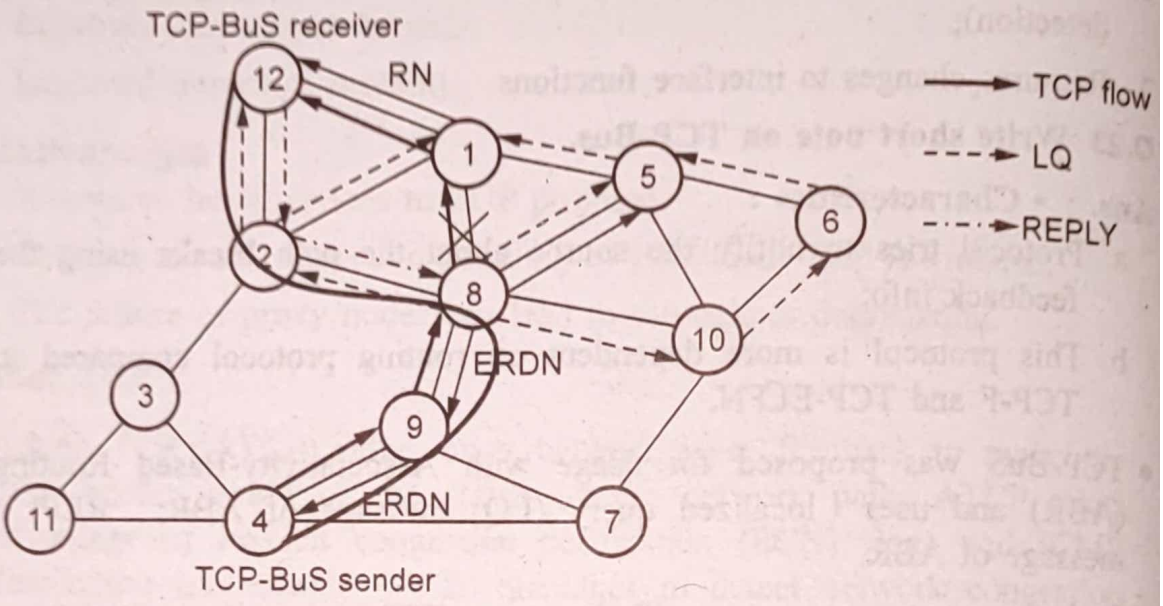


Fig. Q.23.2 : Operation of TCP-BuS connection

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.

3.8 : Wireless Sensor Network

Q.24 What are the design issues in wireless sensor network ?

☞ [SPPU : Dec.-18, End Sem, Marks 8]

Ans. : Design issues in WSN are as follows :

1. **Fault tolerance :** Possibility of node failure and change of topology of network is quite high in case of WSN. Hence the designer of network should make the network robust and reliable even in case of node failures and topology changes.

2. **Scalability** : The design of WSN should support addition of new nodes any time and also the design should support large number of nodes.
3. **Environment** : The design of WSN should be such that WSN should be able to survive regardless of the conditions in which WSN s deployed.
4. **Heterogeneity support** : The protocols designed for WSN should support different kinds of sensor nodes and also be able to support variety of applications.
5. **Autonomous operations** : The WSN should be able to organize , reorganize and operate autonomously because sometimes WSN deployed in places where human habitation is not possible.
6. **Limited memory and processing capability** : The sensor nodes have very limited memory, power and processing capabilities , so all designs of WSN should not be demanding in terms of processing requirements or memory requirements

Q.25 Write a short note on wireless sensor network.

☞ **[SPPU : May-18, End Sem, Marks 4]**

Ans. : • 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.

Q.26 Describe each component in sensor node architecture.

☞ [SPPU : May-18, End Sem, Marks 10]

Ans. : 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. Q.26.1 shows a typical sensing node. The components of a sensing node include the following :

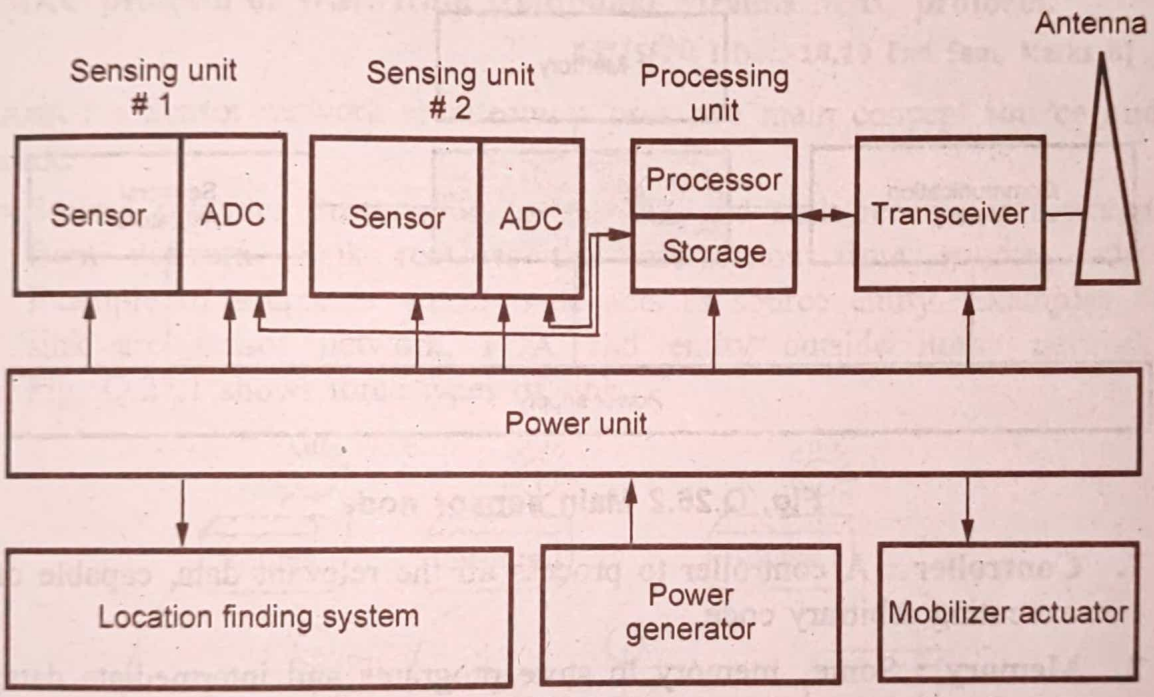


Fig. Q.26.1 Typical sensing node

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. Q.26.2 shows the overview of main sensor node hardware components.

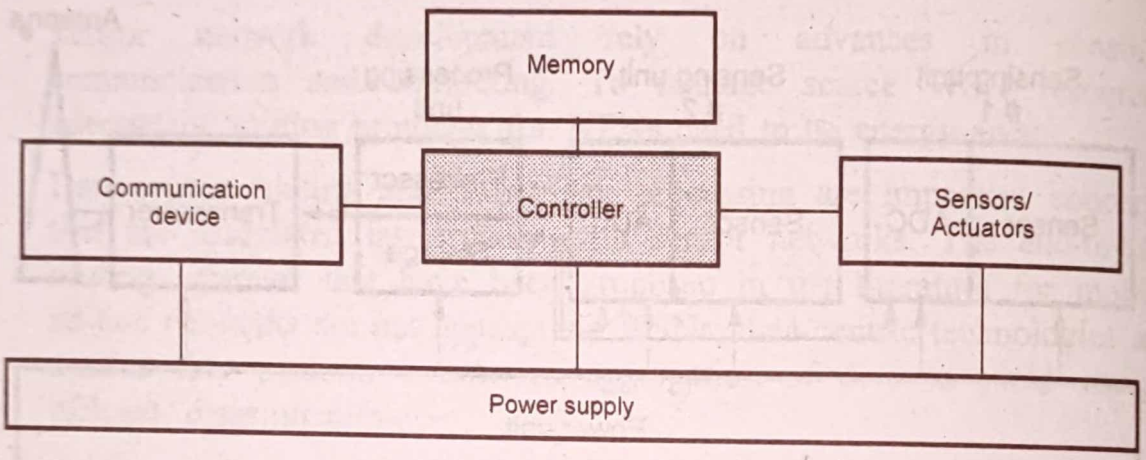


Fig. Q.26.2 Main sensor node

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.

3.9 : Sensor Network Architecture

Q.27 What are the elements of sensor networks? Differentiate the MAC protocol of WSN from traditional wireless MAC protocol.

☞ [SPPU : Dec.-18,19 End Sem, Marks 8]

Ans. : • 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. Q.27.1 shows three types of sink.

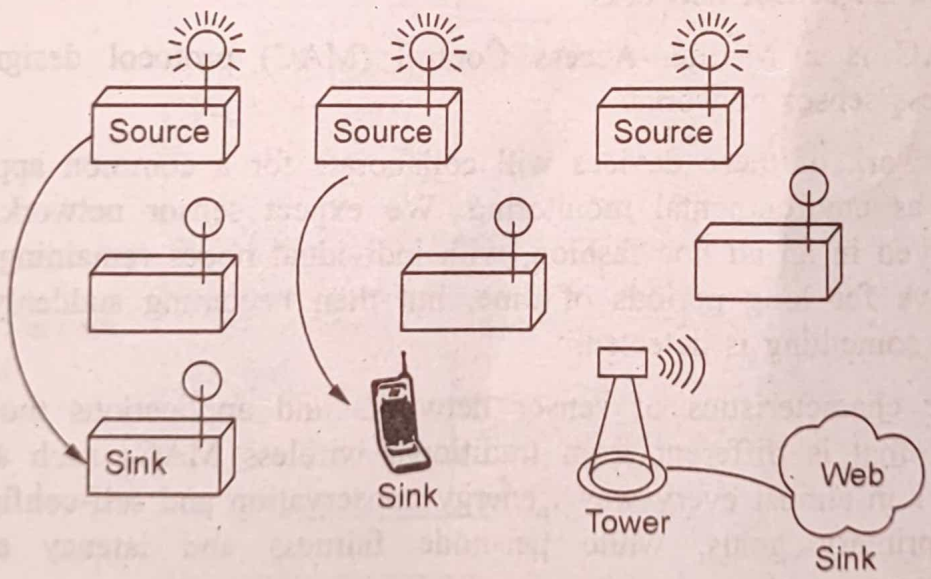


Fig. Q.27.1 Types of sink

• 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. Q.27.2 shows multihop communication network.

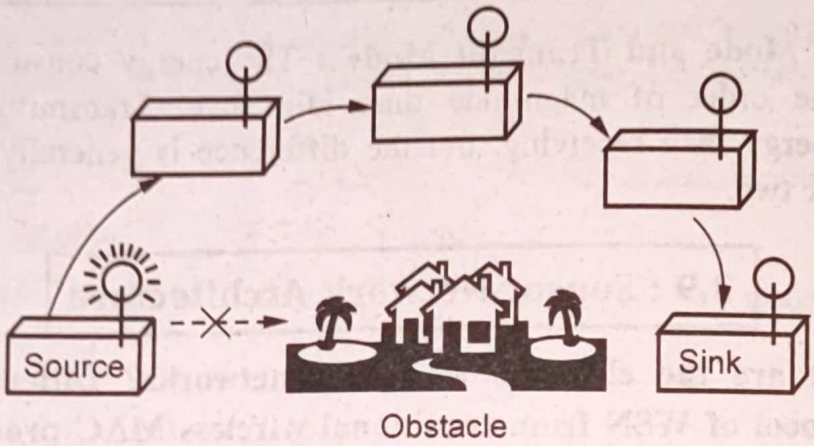


Fig. Q.27.2 Multihop communication

- 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.
- S-MAC is a Medium-Access Control (MAC) protocol designed for wireless sensor networks.
- A network of these devices will collaborate for a common application such as environmental monitoring. We expect sensor networks to be deployed in an ad hoc fashion, with individual nodes remaining largely inactive for long periods of time, but then becoming suddenly active when something is detected.
- These characteristics of sensor networks and applications motivate a MAC that is different from traditional wireless MACs such as IEEE 802.11 in almost every way : energy conservation and self-configuration are primary goals, while per-node fairness and latency are less important.
- S-MAC uses three novel techniques to reduce energy consumption and support self-configuration. To reduce energy consumption in listening to an idle channel, nodes periodically sleep. Neighboring nodes form virtual clusters to auto-synchronize on sleep schedules.
- Inspired by PAMAS, S-MAC also sets the radio to sleep during transmissions of other nodes. Unlike PAMAS, it only uses in-channel signaling.

- Finally, S-MAC applies message passing to reduce contention latency for sensor-network applications that require store-and-forward processing as data move through the network.

Q.28 Write a short note on sensor network with classification of protocols used. ☞ [SPPU : Dec.-22, End Sem, Marks 9]

Ans. : Classification of protocols used :

Sensor Network Protocol	Architecture	Layered	UNPF
		Clustered	LEACH
	Data Handling	Data Dissemination	Flooding
			SAR
			SPIN
			SMECN
			Gossiping
		Data Gathering	Direct Transmission
			Binary Scheme
			FEGASIS
	Medium Access Control	SMACS	
		Hybrid FDMA	
		CSMA	
	Location Discovery	Indoor Localization	
		Multi-lateration	

	Miscellaneous	Quality of network coverage	Breach Path
			Maximum support path
		Security	LEAP
			INSENS
			SPINS
		Real time communication	SPEED
			RAP
		Other Solutions	Transport Layer
			Synchronizations
			Energy efficient hardware design

Also Refer Q.27

Q.29 Explain different issues and challenges in designing sensor network. ☞ [SPPU : June-22, End Sem, Marks 9]

Ans. : Issues and challenges in designing sensor network are as follows :

1. Sensor networks are infrastructure-less. Therefore, all routing and maintenance algorithms need to be distributed.
2. Energy : The operation of sensor nodes is depends on 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.
3. 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.
4. Sensor nodes should be able to synchronize with each other in a completely distributed manner.

5. 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.
6. Real-time communication over sensor networks must be supported through provision of guarantees on maximum delay, minimum bandwidth, or other QoS parameters.

Q.30 Compare sensor network with Adhoc wireless network.

☞ [SPPU : Dec.-22, End Sem, Marks 6]

Ans. : • 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.
- 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.
- Sensor networks is data fusion/aggregation, whereby the sensor nodes aggregate the local information before relaying.

3.10 : Cluster Architecture Management

Q.31 Explain with diagram layered architecture & clustered architecture for sensor network. ☞ [SPPU : June-22, End Sem, Marks 9]

Ans. : 1. Layered architecture :

- 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.
- Fig. Q.31.1 shows layered architecture.

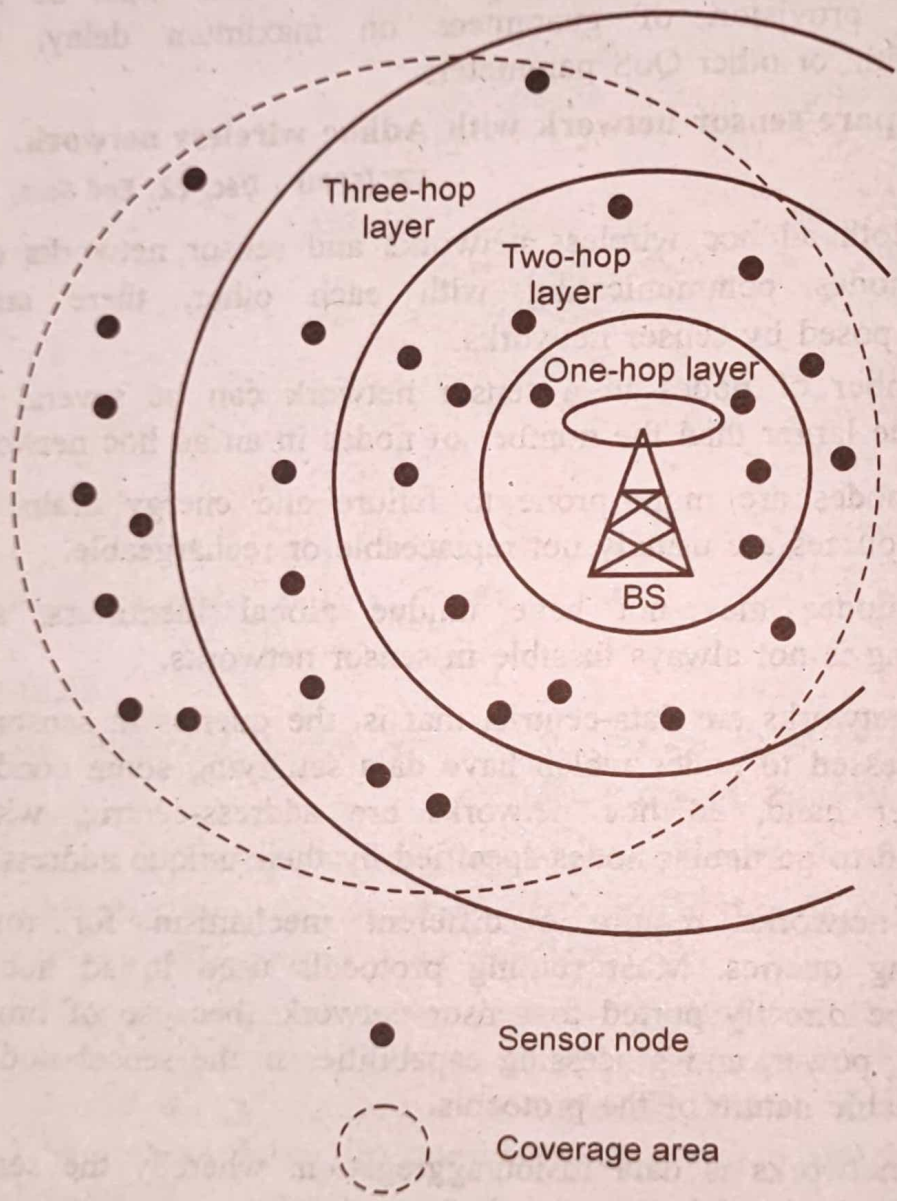


Fig. Q.31.1

- 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).
- Unified Network Protocol Framework (UNPF) is a set of protocols for complete implementation of a layered architecture for sensor networks.

- UNPF integrates three operations in its protocol structure : network initialization and maintenance, MAC, and routing protocols.
- Network Initialization and Maintenance Protocol : The network initialization protocol organizes the sensor nodes into different layers, using the broadcast capability of the BS. The BS can reach all nodes in a one-hop communication over a common control channel. The BS broadcasts its identifier using a known CDMA code on the common control channel. All nodes which hear this broadcast then record the BS ID.
- MAC Protocol : Network initialization is carried out on a common control channel. During the data transmission phase, the Distributed TDMA Receiver Oriented Channel (DTROC) assignment MAC protocol is used. Each node is assigned a reception channel by the BS, and channel reuse is such that collisions are avoided.
- Routing Protocol : Downlink from the BS is by direct broadcast on the control channel. The layered architecture enables multi-hop data forwarding from the sensor nodes to the BS.

2. Clustered Architecture :

- A clustered architecture organizes the sensor nodes into clusters, each governed by a clusterhead. The nodes in each cluster are involved in message exchanges with their respective clusterheads, and these heads send messages to a BS, which is usually an access point connected to a wired network.
- Fig. Q.31.2 shows clustered architecture.
- Clustered architecture is specially 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).

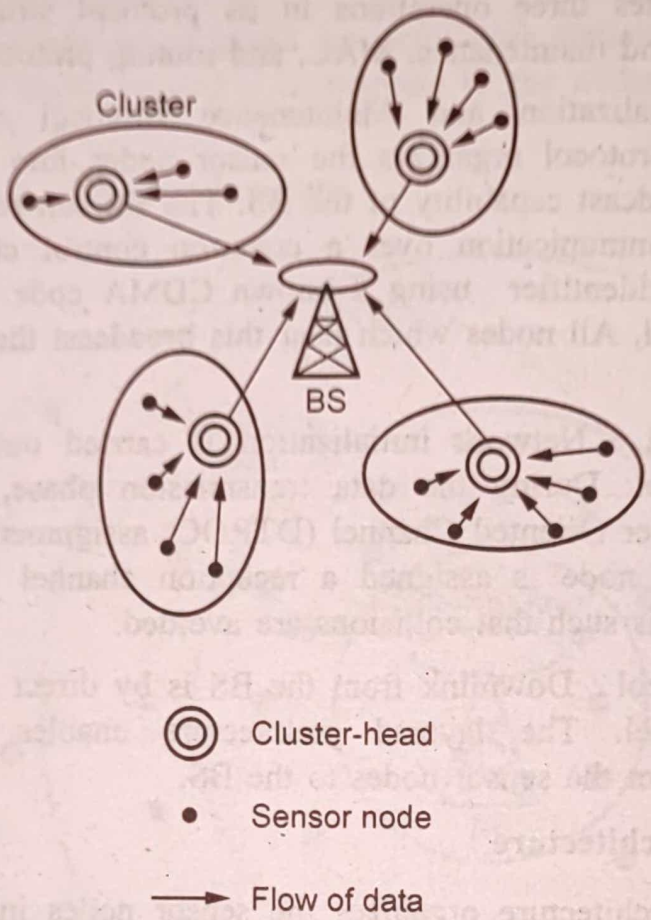


Fig. Q.31.2 clustered architecture

Q.32 Explain with diagram clustered architecture for sensor network.

☞ [SPPU : Dec.-22, End Sem, Marks 6]

Ans. : Refer Q.31

Q.33 Explain in detail LEACH algorithm.

☞ [SPPU : May-18, End Sem, Marks 10]

Ans. : • 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.

END...