SRI MUTHUKUMARAN INSTITUTE OF TECHNOLOGY

(Approved by AICTE, Accredited by NBA and Affiliated to Anna University, Chennai)
Chikkarayapuram (Near Mangadu), Chennai- 600 069.

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

EC8702 - ADHOC AND WIRELESS SENSOR NETWORKS
(REGULATION – 2017)

YEAR: IV **SEM: VII**

UNITI: - ADHOCNETWORKS–INTRODUCTIONANDROUTINGPROTOCOLS

PART – A

1. What is an Ad hoc network?

An Ad hoc network is a multi hop, infrastructure less network which has no centralized server to control the communication between the nodes and resources cannot be reserved beforehand. It is used in battlefields and military applications.

2. Why are Ad hoc networks needed?

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.

3. What do you mean by routing ?

Routing is a process of establishing a path between the sender and receiver nodes for transmitting the packet along the path.

4. What are the design constraints of a routing protocol ?

The design constraints of a routing protocol are,

- Node mobility
- Highly dynamic topology
- No infrastructure for centralized administration
- Bandwidth constrained
- Energy constrained
- Establishing end-to-end path.

5. What are the types of ad hoc routing protocols ?

Ad hoc routing protocols can be broadly classified into three categories :

- Proactive or table driven routing protocols
- Reactive or on-demand routing protocols
- Hybrid routing protocols.

6. What do you mean by proactive routing protocols ?

Proactive routing protocols are also called as **table-driven** routing protocols in which each node maintains a routing table. Routing table contains up-to-date routing information of the entire network.

7. List the advantages and disadvantages of proactive routing protocols.

Advantage

- Minimum time is required to find out a route for data transmission.

Disadvantages

- Due to the frequent change of network topology, the exchange of up-to-date information has to be done periodically.
- Network overload is high.

- Bandwidth consumption is high in large networks.
- This type of protocol is not suited for large networks.

8. Define reactive routing protocols.

Reactive routing protocols are also called as **on-demand** routing protocols. In this type of routing protocols, each node determines the routing path whenever it is ready for transmitting data to other node in the network.

9. List the advantages and disadvantages of reactive routing protocols.

Advantages

- Needs to broadcast less control messages for discovering route when required
- Network overhead is low
- Suitable for large networks
- Bandwidth wastage is low.

Disadvantage

- Time taken to discover a route is non-predictable.

10. What is hybrid routing protocols?

Hybrid routing protocols combine the features of both proactive and reactive routing protocols. In this protocol, the network is divided into zones.

11. What is the basic principle of an Ad hoc Network?

Mobile device communicate in peer-to-peer fashion, Self organizing network without the need of fixed network infrastructure, Multi-hop communication, Decentralized, mobility-adaptive operation.

12. Define Scalability.

Scalability is the ability of the routing protocol to scale a network with a large number of nodes.

13. Differentiate Cellular and Ad hoc Network.

Cellular Network	Ad hoc Network
• Fixed Infrastructure	• Infrastructure less
• Single hop Network	• Multihop Network
• Circuit Switched	• Packet switched
• Centralized routing	• Distributed routing

14. Mention few applications of Ad hoc Network.

Ad hoc networks are widely used in

- Military applications and battlefields
- Collaborative and distributed computing
- Emergency search and rescue operations
- Wireless sensor and mesh networks.

15. Define QoS.

Quality of service (QoS) is the performance level of services offered by a service provider or a network to the user. In Adhoc wireless network to achieve QoS the following factors must be taken into account, QoS parameters, QoS- aware routing, and QoS framework.

16. What is Hidden terminal Problem?

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

17. Mention the types of security attacks in ad hoc networks.

The lack of any central coordination and shared medium of ad hoc networks makes them vulnerable to security attacks. The types of security attacks are

- **Passive attacks:** Attacks attempted by malicious nodes to perceive the nature of activities and obtain the information transacted in the network without disturbing the network.
- **Active attacks:** Active attacks disturb the operation of networks. Types are external attack and internal attack.

18. What is Denial of service?

The attack affected by making the network resource unavailable for service to other nodes, either by consuming the bandwidth or by overloading the system.

19. What are the types of wireless networks ?

The wireless networks can be broadly classified into two types :

- Infrastructure based network
- Infrastructure less network.

20. Define security issue.

Security is a challenging one in Ad hoc wireless networks, especially in military areas. The attacks in Ad hoc wireless network is broadly classified into two types:

- Passive attack
- Active attack.

21. Define a Wireless Sensor Network (WSN).

Wireless Sensor Networks (WSNs) are distributed networks which are formed by small, lightweight wireless nodes. Each sensor node is also called as **mote**.

22. What are the types of wireless sensor networks ?

The types of WSNs are listed below,

- Terrestrial WSNs
- Underground WSNs
- Underwater WSNs
- Multimedia WSNs
- Mobile WSNs.

23. List some design challenges posed by sensor networks.

1. Fault-tolerant communication
2. Low latency
3. Scalability
4. Transmission media
5. Speed
6. Energy
7. Storage capacity
8. Coverage problems

24. Illustrate the issues in Adhoc networks.

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

25. Differentiate proactive and reactive routing protocols. Write examples for each.

Proactive or table-driven routing protocols: In table-driven routing protocols, every node maintains the network topology information in the form of routing tables by periodically exchanging routing information. Routing information is generally flooded in the whole network. Whenever a node requires a path to a destination, it runs an appropriate path-finding algorithm on the topology information it maintains.

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

PART – B

1. Differentiate between cellular Network and Adhoc Network.

Cellular Networks	Ad Hoc Wireless Networks
Fixed infrastructure-based	Infrastructure-less
Single-hop wireless links	Multi-hop wireless links
Guaranteed bandwidth (designed for voice traffic)	Shared radio channel (more suitable for best-effort data traffic)
Centralized routing	Distributed routing
Circuit-switched (evolving toward packet switching)	Packet-switched (evolving toward emulation of circuit switching)
Seamless connectivity (low call drops during handoffs)	Frequency path break due to mobility
High cost and time of deployment	Quick and cost-effective deployment
Reuse of frequency spectrum through geographical channel reuse	Dynamic frequency reuse based on carrier sense mechanism

Easier to achieve time synchronization	Time synchronization is difficult and consumes bandwidth
Easier to employ bandwidth reservation	Bandwidth reservation requires complex medium access control protocols
Application domains include mainly civilian and commercial sector	Application domains include battlefields, emergency search and rescue operation, and collaborative computing
High cost of network maintenance (backup power source, staffing, etc.)	Self-organization and maintenance properties are built into the network
Mobile hosts are of relatively low complexity	Mobile hosts require more intelligence (should have a transceiver as well as routing/switching capacity)
Major goals of routing and call admission are to maximize the call acceptance ratio and minimize the call drop ratio	Man aim of routing is to find paths with minimum overhead and also quick reconfiguration of broken paths
Widely deployed and currently in the third generation	Several issues are to be addressed for successful commercial deployment even though widespread use exists in defense

2. Draw the schematic diagram of an ad hoc wireless Internet and discuss the issues to be considered for the successful ad hoc wireless Internet.

Ad hoc wireless internet extends the services of the internet to the end users over an ad hoc wireless network. Some of the applications of ad hoc wireless internet are:

- Wireless mesh network.
- Provisioning of temporary internet services to major conference venues.
- Sports venues.
- Temporary military settlements.
- Battlefields &
- Broadband internet services in rural regions.

The major issues to be considered for a successful ad hoc wireless internet are the following:

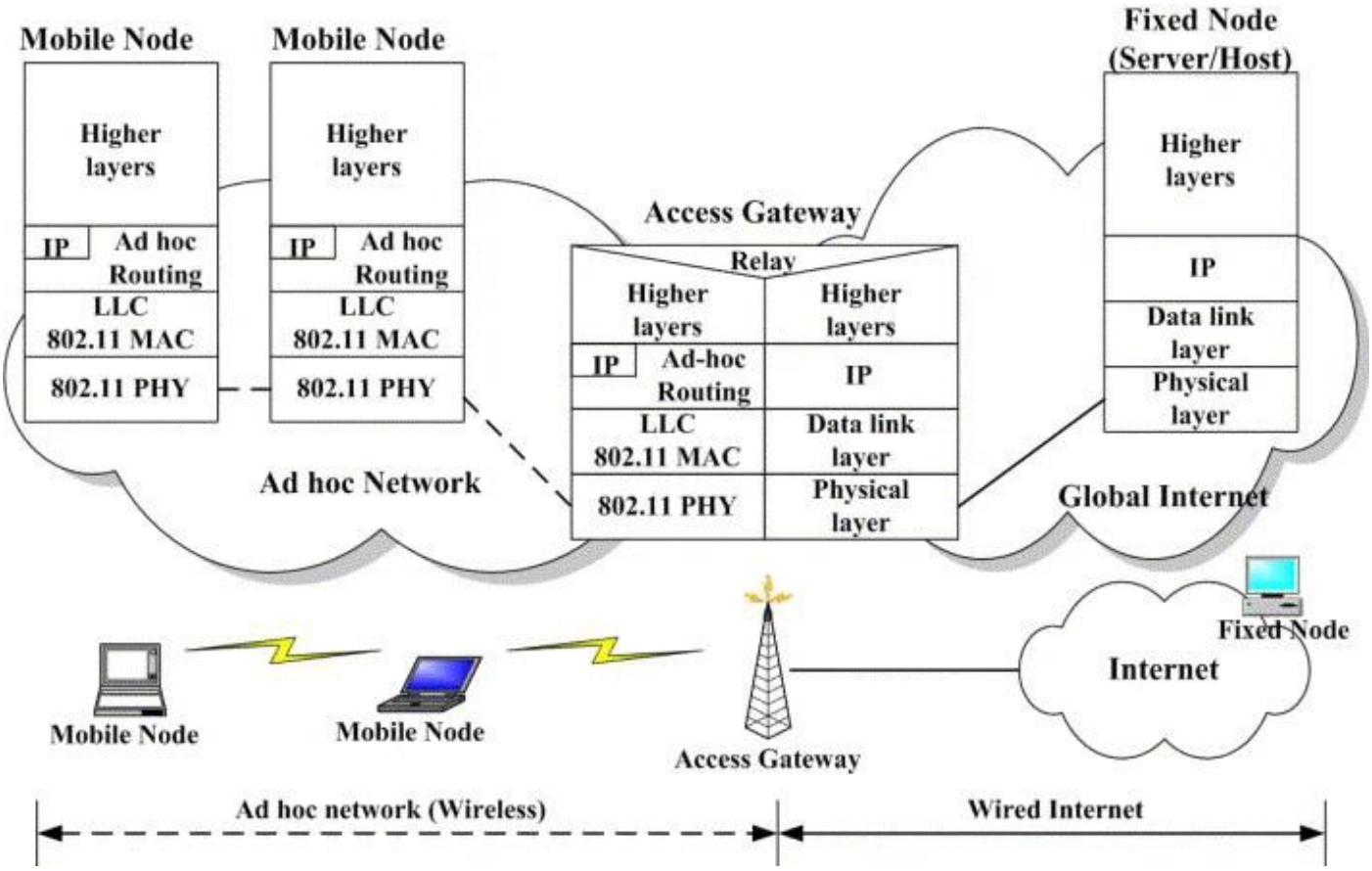
Gateway:

- They are the entry points to the wired internet.
- Generally owned & operated by a service provider.

They perform following tasks,

- Keeping track of end users.
- Bandwidth management.

- Load balancing.
- Traffic shaping.
- Packet filtering.
- Width fairness &
- Address, service & location discovery.



Address mobility:
This problem is worse here as the nodes operate over multiple wireless hops.
Solution such as Mobile IP can provide temporary alternative.
Routing:

- It is a major problem in ad hoc wireless internet, due to dynamic topological changes, the presence of gateways, multi-hop relaying, & the hybrid character of the network.
- Possible solution is to use separate routing protocol for the wireless part of ad hoc wireless internet.

Transport layer protocol:
Several factors are to be considered here, the major one being the state maintenance overhead at the gateway nodes.
Load balancing:
They are essential to distribute the load so as to avoid the situation where the gateway nodes become bottleneck nodes.
Pricing / Billing:
Since internet bandwidth is expensive, it becomes very important to introduce pricing/billing strategies for the ad hoc wireless internet.
Provisioning of security:
Security is a prime concern since the end users can utilize the ad hoc wireless internet infrastructure to make e-commerce transaction.
QoS support:
With the widespread use of voice over IP(VOIP) & growing multimedia applications over the internet, provisioning of QoS support in the ad hoc wireless internet becomes a very important issue.

Service, address & location discovery:

- Service discovery refers to the activity of discovering or identifying the party which provides service or resource.
- Address discovery refers to the services such as those provided by Address Resolution Protocol (ARP) or Domain Name Service (DNS) operating within the wireless domain.
- Location discovery refers to different activities such as detecting the location of a particular mobile node in the network or detecting the geographical location of nodes.

3. Describe the issues and challenges in Ad hoc wireless networks.

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

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

1. Medium Access Scheme

The primary responsibility of a Medium Access Control (MAC) protocol in adhoc wireless networks is the distributed arbitration for the shared channel for transmission of packets. **The major issues to be considered in designing a MAC protocol for adhoc wireless networks are as follows:**

1. Distributed Operation:

The ad hoc wireless networks need to operate in environments where no centralized coordination is possible. The MAC protocol design should be fully distributed involving minimum control overhead.

2. Synchronization:

The MAC protocol design should take into account the requirement of time synchronization. Synchronization is mandatory for TDMA-based systems for management of transmission and reception slots.

3. Hidden Terminals:

Hidden terminals are nodes that are hidden(or not reachable) from the sender of a data transmission session, but are reachable to the receiver of the session.

4. Exposed terminals:

Exposed terminals, the nodes that are in the transmission range of the sender of an on-going session, are prevented from making a transmission.

5. Throughput:

The MAC protocol employed in adhoc wireless networks should attempt to maximize the throughput of the system.

The important considerations for throughput enhancement are

- Minimizing the occurrence of collisions.
- Maximizing channel utilization and
- Minimizing control overhead.

6. Access delay:

The average delay that any packet experiences to get transmitted. The MAC protocol should attempt to minimize the delay.

7. Fairness:

Fairness refers to the ability of the MAC protocol to provide an equal share or weighted share of the bandwidth to all competing nodes. Fairness can be either node-based or flow-based.

8. Real-time Traffic support:

In a contention-based channel access environment, without any central coordination, with limited bandwidth, and with location-dependent contention, supporting time- sensitive traffic such as voice, video, and real-time data requires explicit support from the MAC protocol.

9. Resource reservation:

The provisioning of QoS defined by parameters such as bandwidth, delay, and jitter requires reservation of resources such as bandwidth, buffer space, and processing power.

10. Ability to measure resource availability:

In order to handle the resources such as bandwidth efficiently and perform call admission control based on their availability, the MAC protocol should be able to provide an estimation of resource availability at every node. This can also be used for making congestion control decisions.

11. Capability for power control:

The transmission power control reduces the energy consumption at the nodes, causes a decrease in interference at neighboring nodes, and increases frequency reuse.

12. Adaptive rate control:

This refers to the variation in the data bit rate achieved over a channel. A MAC protocol that has adaptive rate control can make use of a high data rate when the sender and receiver are nearby & adaptively reduce the data rate as they move away from each other.

13. Use of directional antennas:

This has many advantages that include

- Increased spectrum reuse.
- Reduction in interference and
- Reduced power consumption.

2. Routing **

The responsibilities of a routing protocol include exchanging the route information; finding a feasible path to a destination. **The major challenges that a routing protocol faces are as follows:**

1. Mobility:

The Mobility of nodes results in frequent path breaks, packet collisions, transient loops, stale routing information, and difficulty in resource reservation.

2. Bandwidth constraint:

Since the channel is shared by all nodes in the broadcast region, the bandwidth available per wireless link depends on the number of nodes & traffic they handle.

3. Error-prone and shared channel:

The Bit Error Rate (BER) in a wireless channel is very high [10^{-5} to 10^{-3}] compared to that in its wired counterparts [10^{-12} to 10^{-9}]. Consideration of the state of the wireless link, signal-to-noise ratio, and path loss for routing in ad hoc wireless networks can improve the efficiency of the routing protocol.

4. Location-dependent contention:

The load on the wireless channel varies with the number of nodes present in a given geographical region. This makes the contention for the channel high when the number of nodes increases.

The high contention for the channel results in a high number of collisions & a subsequent wastage of bandwidth.

5. Other resource constraints:

The constraints on resources such as computing power, battery power, and buffer storage also limit the capability of a routing protocol.

The major requirements of a routing protocol in adhoc wireless networks are the following.

1. Minimum route acquisition delay:

The route acquisition delay for a node that does not have a route to a particular destination node should be as minimal as possible. The delay may vary with the size of the network and the network load.

2. Quick route reconfiguration:

The unpredictable changes in the topology of the network require that the routing protocol be able to quickly perform route reconfiguration in order to handle path breaks and subsequent packet losses.

3. Loop-free routing:

This is a fundamental requirement to avoid unnecessary wastage of network bandwidth. In adhoc wireless networks, due to the random movement of nodes, transient loops may form in the route thus established. A routing protocol should detect such transient routing loops & take corrective actions.

4. Distributed routing approach:

An adhoc wireless network is a fully distributed wireless network & the use of centralized routing approaches in such a network may consume a large amount of bandwidth.

5. Minimum control overhead:

The control packets exchanged for finding a new route, and maintaining existing routes should be kept as minimal as possible.

6. Scalability:

Scalability is the ability of the routing protocol to scale well in a network with a large number of nodes. This requires minimization of control overhead & adaptation of the routing protocol to the network size.

7. Provisioning of QoS:

The routing protocol should be able to provide a certain level of QoS as demanded by the nodes or the category of calls. The QoS parameters can be bandwidth, delay, jitter, packet delivery ratio, & throughput.

8. Support for time-sensitive traffic:

Tactical communications & similar applications require support for time-sensitive traffic. The routing protocol should be able to support both hard real-time & soft real-time traffic.

9. Security and privacy:

The routing protocol in adhoc wireless networks must be resilient to threats and vulnerabilities. It must have inbuilt capability to avoid resource consumption, denial-of-service, impersonation, and similar attacks possible against an ad hoc wireless network.

3. Multicasting

It plays important role in emergency search & rescue operations & in military communication. Use of single- link connectivity among the nodes in a multicast group results in a tree-shaped multicast routing topology. Such a tree-shaped topology provides high multicast efficiency, with low packet delivery ratio due to the frequency tree breaks. The major issues in designing multicast routing protocols are as follows:

1. **Robustness:**

• The multicast routing protocol must be able to recover & reconfigure quickly from potential mobility-induced link breaks thus making it suitable for use in high dynamic environments.

2. **Efficiency:**

• A multicast protocol should make a minimum number of transmissions to deliver a data packet to all the group members.

3. **Control overhead:**

• The scarce bandwidth availability in ad hoc wireless networks demands minimal control overhead for the multicast session.

4. **Quality of Service:**

• QoS support is essential in multicast routing because, in most cases, the data transferred in a multicast session is time-sensitive.

5. **Efficient group management:**

• Group management refers to the process of accepting multicast session members and maintaining the connectivity among them until the session expires.

6. **Scalability:**

• The multicast routing protocol should be able to scale for a network with a large number of node

7. **Security:**

• Authentication of session members and prevention of non-members from gaining unauthorized information play a major role in military communications.

4. Transport Layer Protocol

The main objectives of the transport layer protocols include:

- Setting up & maintaining end-to-end connections,
- Reliable end-to-end delivery of packets,
- Flow control &
- Congestion control.

Examples of some transport layers protocols are,

a. UDP (User Datagram Protocol) :

- It is an unreliable connectionless transport layer protocol.
- It neither performs flow control & congestion control.
- It do not take into account the current network status such as congestion at the intermediate links, the rate of collision, or other similar factors affecting the network throughput.

b. TCP (Transmission Control Protocol):

- It is a reliable connection-oriented transport layer protocol.
- It performs flow control & congestion control.
- Here performance degradation arises due to frequent path breaks, presence of stale routing information, high channel error rate, and frequent network partitions.

5. Pricing Scheme

• Assume that an optimal route from node A to node B passes through node C, & node C is not powered on.

• Then node A will have to set up a costlier & non-optimal route to B.

• The non-optimal path consumes more resources & affects the throughput of the system.

• As the intermediate nodes in a path that relay the data packets expend their resources such as battery charge & computing power, they should be properly compensated.

• Hence, pricing schemes that incorporate service compensation or service reimbursement are required.

6. Quality of Service Provisioning (QoS)

QoS is the performance level of services offered by a service provider or a network to the user. QoS provisioning often requires ,

- Negotiation between host & the network.
- Resource reservation schemes.
- Priority scheduling &
- Call admission control.

QoS parameters :

Applications	Corresponding QoS parameter
1. Multimedia application	1. Bandwidth & Delay.
2. Military application	2. Security & Reliability.
3. Defense application	3. Finding trustworthy intermediate hosts & routing
4. Emergency search and rescue operations	4.Availability.
5. Hybrid wireless network	5. Maximum available link life, delay, bandwidth & channel utilization.
6. Communication among the nodes in a sensor network	6. Minimum energy consumption, battery life & energy conservation

QoS-aware routing :

i. Finding the path is the first step toward a QoS-aware routing protocol.

ii. The parameters that can be considered for routing decisions are,

- Network throughput.
- Packet delivery ratio.
- Reliability.
- Delay.
- Delay jitter.
- Packet loss rate.
- Bit error rate.
- Path loss.

QoS framework :

I. A framework for QoS is a complete system that attempts to provide the promised services to each user or application.

II. The key component of QoS framework is a QoS service model which defines the way user requirements are served.

7. Self-Organization

• One very important property that an ad hoc wireless network should exhibit is organizing & maintaining the network by itself.

• The major activities that an ad hoc wireless network is required to perform for self-organization are,

- Neighbour discovery.
- Topology organization &
- Topology reorganization (updating topology information)

8. Security

1) Security is an important issue in ad hoc wireless network as the information can be hacked.

2) Attacks against network are of 2 types :

I. Passive attack → Made by malicious node to obtain information transacted in the network without disrupting the operation.

II. Active attack → They disrupt the operation of network. Further active attacks are of 2 types :

- External attack: The active attacks that are executed by nodes outside the network.
- Internal attack: The active attacks that are performed by nodes belonging to the same network.

3) The major security threats that exist in ad hoc wireless networks are as follows :

Denial of service – The attack affected by making the network resource unavailable for service to other nodes, either by consuming the bandwidth or by overloading the system.

Resource consumption – The scarce availability of resources in ad hoc wireless network makes it an easy target for internal attacks, particularly aiming at consuming resources available in the network.

The major types of resource consumption attacks are,
Energy depletion :
- Highly constrained by the energy source
- Aimed at depleting the battery power of critical nodes.

Buffer overflow :
- Carried out either by filling the routing table with unwanted routing entries or by consuming the data packet buffer space with unwanted data.
- Lead to a large number of data packets being dropped, leading to the loss of critical information.

Host impersonation – A compromised internal node 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 disclosure of confidential information to unauthorized nodes.

Interference – A common attack in defense applications to jam the wireless communication by creating a wide spectrum noise.

9. Energy Management

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

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

Energy management can be classified into the following categories :

a. Transmission power management:

The power consumed by the Radio Frequency (RF) module of a mobile node is determined by several factors such as

- The state of operation.
- The transmission power and
- The technology used for the RF circuitry.

The state of operation refers to transmit, receive, and sleep modes of the operation. The transmission power is determined by

- Reach ability requirement of the network.
- Routing protocol and
- MAC protocol employed.

b. Battery energy management:

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

c. Processor power management:

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

d. Devices power management:

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

10. Scalability

- Scalability is the ability of the routing protocol to scale well in a network with a large number of nodes.
- It requires minimization of control overhead & adaptation of the routing protocol to the network size.

11. Deployment Considerations

The deployment of a commercial ad hoc wireless network has the following benefits when compared to wired networks

a) Low cost of deployment:

- The use of multi-hop wireless relaying eliminates the requirement of cables & maintenance in deployment of communication infrastructure.
- The cost involved is much lower than that of wired networks.

b) Incremental deployment:

- Deployment can be performed incrementally over geographical regions of the city.
- The deployed part of the network starts functioning immediately after the minimum configuration is done.

c) Short deployment time:

Compared to wired networks, the deployment time is considerably less due to the absence of any wired links.

d) Reconfigurability:

The cost involved in reconfiguring a wired network covering a Metropolitan Area Network(MAN) is very high compared to that of an ad hoc wireless network covering the same service area.

12. Addressing and service discovery

- Addressing & service discovery assume significance in ad hoc wireless network due to the absence of any centralised coordinator.
- An address that is globally unique in the connected part of the ad hoc wireless network is required for a node in order to participate in communication.
- Auto-configuration of addresses is required to allocate non-duplicate addresses to the nodes.

4. Explain in detail about the applications of Adhoc Wireless Networks.

1. Military Application

- Adhoc wireless networks can be very useful in establishing communication among a group of soldiers for tactical operations.
- Setting up of a fixed infrastructure for communication among group of soldiers in enemy territories or in inhospitable terrains may not be possible.
- In such a case, adhoc wireless networks provide required communication mechanism quickly.
- The primary nature of the communication required in a military environment enforces certain important requirements on adhoc wireless networks namely, Reliability, Efficiency, Secure communication & Support for multicast routing.

2. Collaborative & Distributed computing

- Adhoc wireless network helps in collaborative computing, by establishing temporary communication infrastructure for quick communication with minimal configuration among a group of people in a conference.
- In distributed file sharing application reliability is of high importance which would be provided by adhoc network.
- Other applications such as streaming of multimedia objects among participating nodes in ad hoc wireless networks require support for soft real-time communication
- Devices used for such applications could typically be laptops with add-on wireless interface cards, enhanced personal digital assistants (PDAs) or mobile devices with high processing power

3. Emergency Operations

- Ad hoc wireless networks are very useful in emergency operations such as search and rescue, crowd control and commando operations
- The major factors that favour ad hoc wireless networks for such tasks are self-configuration of the system with minimal overhead, independent of fixed or centralised infrastructure, the freedom and flexibility of mobility, and unavailability of conventional communication infrastructure.
- In environments, where the conventional infrastructure based communication facilities are destroyed due to a war or due to natural calamities, immediate deployment of adhoc wireless networks would be a good solution for co-ordinating rescue activities.
- They require minimum initial network configuration with very little or no delay

4. Wireless Mesh Network

- Wireless mesh networks are adhoc wireless network that are formed to provide an alternate communication infrastructure for mobile or fixed nodes/users, without the spectrum reuse constraint & requirement of network planning of cellular network.
- It provides many alternate paths for a data transfer session between a source & destination, resulting in quick reconfiguration of the path when the existing path fails due to node failure.
- Since the infrastructure built is in the form of small radio relaying devices, the investment required in wireless mesh networks is much less than what is required for the cellular network counterpart.
- The possible deployment scenarios of wireless mesh networks include: residential zones, highways, business zones, important civilian regions and university campuses
- Wireless mesh networks should be capable of self-organization and maintenance.
- It operates at license-free ISM band around 2.4 GHz & 5 GHz.
- It is scaled well to provide support to large number of points.
- Major advantage is the support for a high data rate, quick & low cost of deployment, enhanced services, high scalability, easy extendibility, high availability & low cost per bit.

5. Analyze the destination sequenced distance-vector routing protocol with an example.

- It is an enhanced version of the distributed Bellman-Ford algorithm where each node maintains a table that contains the shortest distance and the first node on the shortest path to every other node in the network.
- It incorporates table updates with increasing sequence number tags to prevent loops, to counter the count-to-infinity problem, and for faster convergence.
- As it is a table-driven routing protocol, routes to all destinations are readily available at every node at all times.
- The tables are exchanged between neighbors at regular intervals to keep an up-to-date view of the network topology.

The table updates are of two types:

- ***Incremental updates:*** Takes a single network data packet unit (NDPU). These are used when a node does not observe significant changes in the local topology.
- ***Full dumps:*** Takes multiple NDPUs. It is done either when the local topology changes significantly or when an incremental update requires more than a single NDPU.
- Table updates are initiated by a destination with a new sequence number which is always greater than the previous one.
- Consider the example as shown in figure one. Here node 1 is the source node and node 15 is the destination. As all the nodes maintain global topology information, the route is already available as shown in figure two.
- Here the routing table node 1 indicates that the shortest route to the destination node is available through node 5 and the distance to it is 4 hops, as depicted in figure two.
- The reconfiguration of a path used by an on-going data transfer session is handled by the protocol in the following way.
- The end node of the broken link initiates a table update message with the broken link's weight assigned to infinity (∞) and with a sequence number greater than the stored sequence number for that destination.
- Each node upon receiving an update with weight ∞, quickly disseminates it to its neighbors in order to propagate the broken-link information to the whole network.
- A node always assign an odd number to the link break update to differentiate it from the even sequence number generated by the destination.
- Figure shows the case when node 11 moves from its current position.

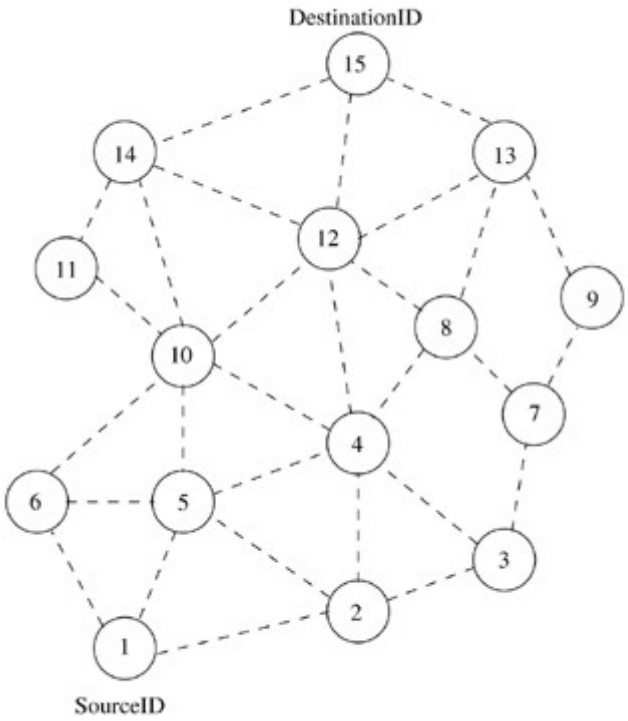
Advantages

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

Disadvantages

- The updates due to broken links lead to a heavy control overhead during high mobility.
- Even a small network with high mobility or a large network with low mobility can completely choke the available bandwidth.
- Suffers from excessive control overhead.
- In order to obtain information about a particular destination node, a node has to wait for a table update message initiated by the same destination node.
- This delay could result in state routing information at nodes.

Route establishment in DSDV

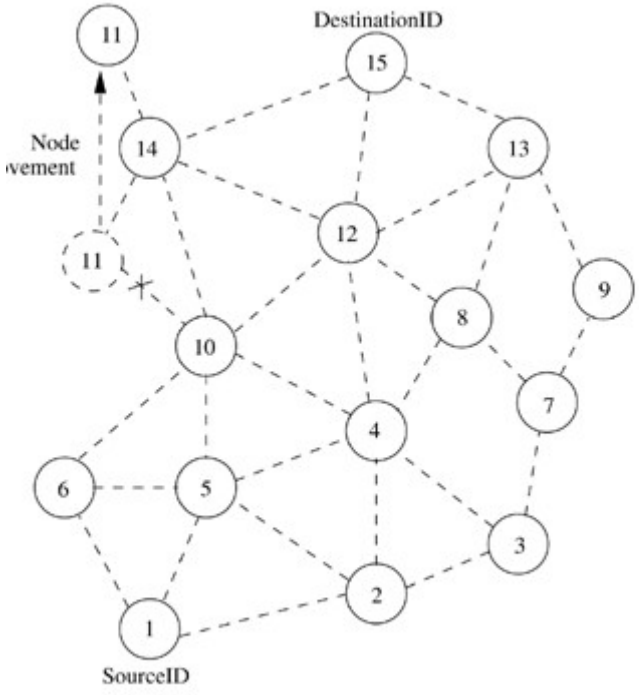


(a) Topology graph of the network

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

(b) Routing table for Node 1

Route maintenance in DSDV



Routing Table for Node 1

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	5	4	180
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

6. Demonstrate how route is established and maintained in an ad hoc network using AODV routing protocol.

- Route is established only when it is required by a source node for transmitting data packets
- It employs destination sequence numbers to identify the most recent path
- Source node and intermediate nodes store the next hop information corresponding to each flow for data packet transmission

- Uses DestSeqNum to determine an up-to-date path to the destination
- A RouteRequest carries the source identifier, the destination identifier, the source sequence number, the destination sequence number, the broadcast identifier and the time to live field
- DestSeqNum indicates the freshness of the route that is accepted by the source
- When an intermediate node receives a RouteRequest, it either forwards it or prepares a RouteReply if it has a valid route to the destination
- The validity of the intermediate node is determined by comparing the sequence numbers
- If a RouteRequest is received multiple times, then duplicate copies are discarded
- Every intermediate node enters the previous node address and its BcastID
- A timer is used to delete this entry in case a RouteReply packet is not received
- AODV does not repair a broken path locally
- When a link breaks, the end nodes are notified
- Source node re-establishes the route to the destination if required

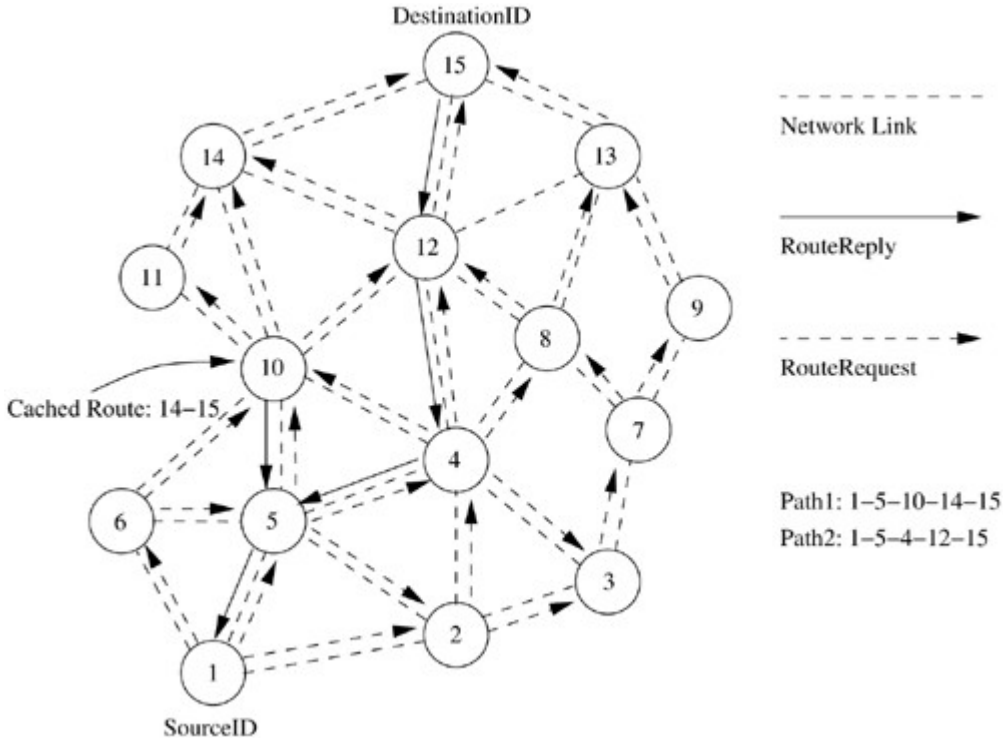
Advantage

- Routes are established on demand and DestSeqNum are used to find latest route to the destination
- Connection setup delay is less

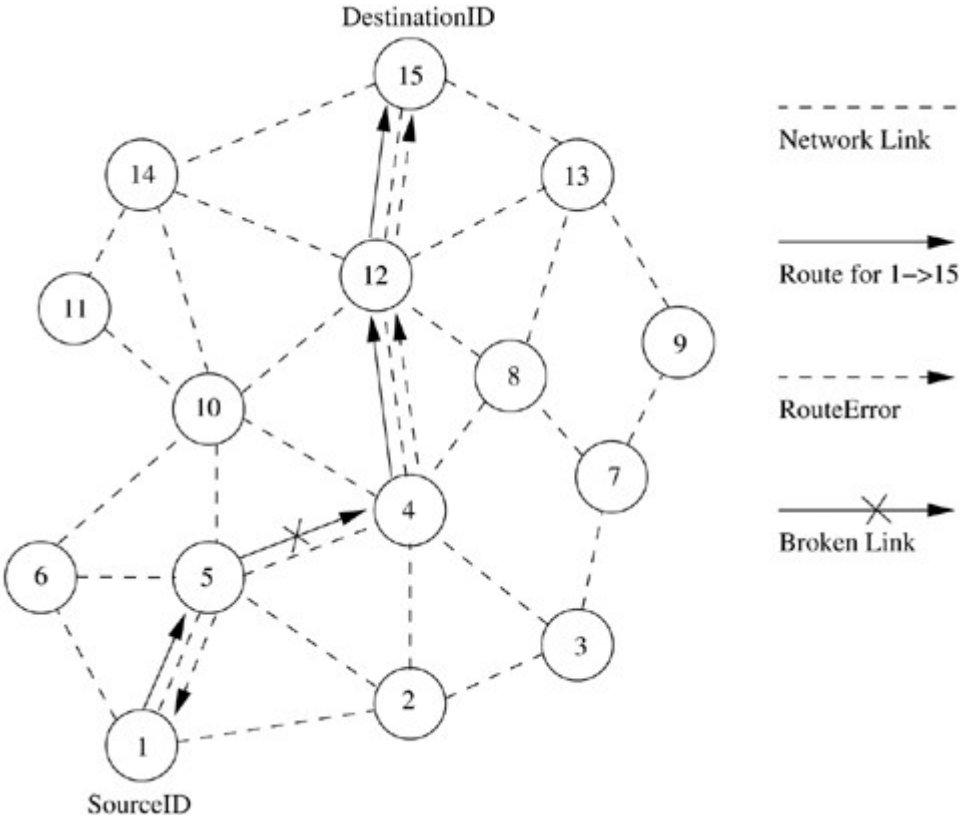
Disadvantages

- Intermediate nodes can lead to inconsistent routes if the source sequence number is very old
- Multiple RouteReply packets to single RouteRequest packet can lead to heavy control overhead
- Periodic beaconing leads to unnecessary bandwidth consumption

Route establishment in AODV



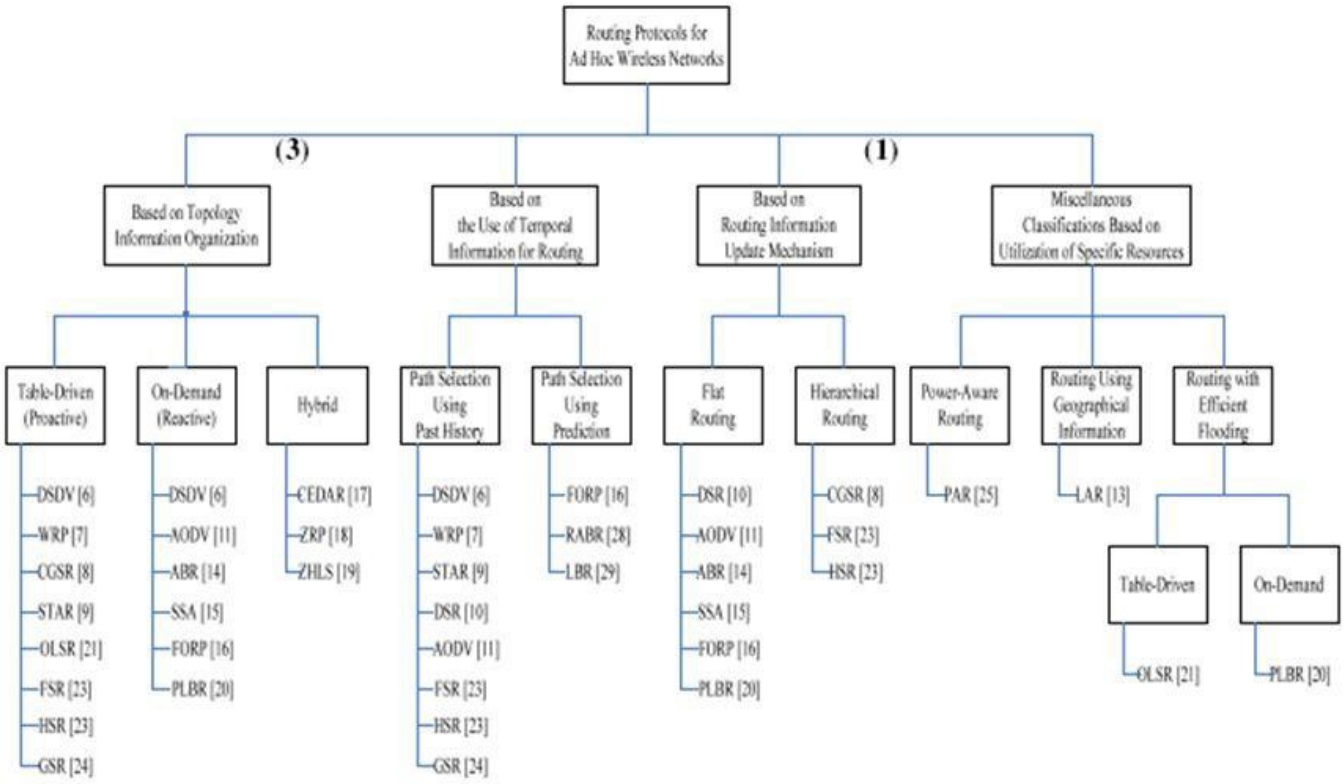
Route maintenance in AODV



7. Explain in detail about the classification of routing protocol.

The routing protocols for ad hoc wireless networks can be broadly classified into four categories based on

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



Based on the Routing Information Update Mechanism

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

1. **Proactive or table-driven routing protocols:** In table-driven routing protocols, every node maintains the network topology information in the form of routing tables by periodically exchanging routing information. Routing information is generally flooded in the whole network. Whenever a node requires a path to a destination, it runs an appropriate path-finding algorithm on the topology information it maintains.
2. **Reactive or on-demand routing protocols:** Protocols that fall under this category do not maintain the network topology information. They obtain the necessary path when it is required, by using a connection establishment process. Hence these protocols do not exchange routing information periodically.
3. **Hybrid routing protocols:** Protocols belonging to this category combine the best features of the above two categories. Nodes within a certain distance from the node concerned, or within a particular geographical region, are said to be within the routing zone of the given node. For routing within this zone, a table-driven approach is used. For nodes that are located beyond this zone, an on-demand approach is used.

Based on the Routing Topology

Routing topology being used in the Internet is hierarchical in order to reduce the state information maintained at the core routers. Ad hoc wireless networks, due to their relatively smaller number of nodes, can make use of either a flat topology or a hierarchical topology for routing.

1. **Flat topology routing protocols:** Protocols that fall under this category make use of a flat addressing scheme similar to the one used in IEEE 802.3 LANs. It assumes the presence of a globally unique (or at least unique to the connected part of the network) addressing mechanism for nodes in an ad hoc wireless network.
2. **Hierarchical topology routing protocols:** Protocols belonging to this category make use of a logical hierarchy in the network and an associated addressing scheme. The hierarchy could be based on geographical information or it could be based on hop distance.

Based on the Utilization of Specific Resources

1. **Power-aware routing:** This category of routing protocols aims at minimizing the consumption of a very important resource in the ad hoc wireless networks: the battery power. The routing decisions are based on minimizing the power consumption either locally or globally in the network.
2. **Geographical information assisted routing:** Protocols belonging to this category improve the performance of routing and reduce the control overhead by effectively utilizing the geographical information available