1.5 Ad hoc wireless Internet

Ad hoc wireless internet extends the services of the internet to the end users over an ad hoc wireless network. It shows in figure 1.6.

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.

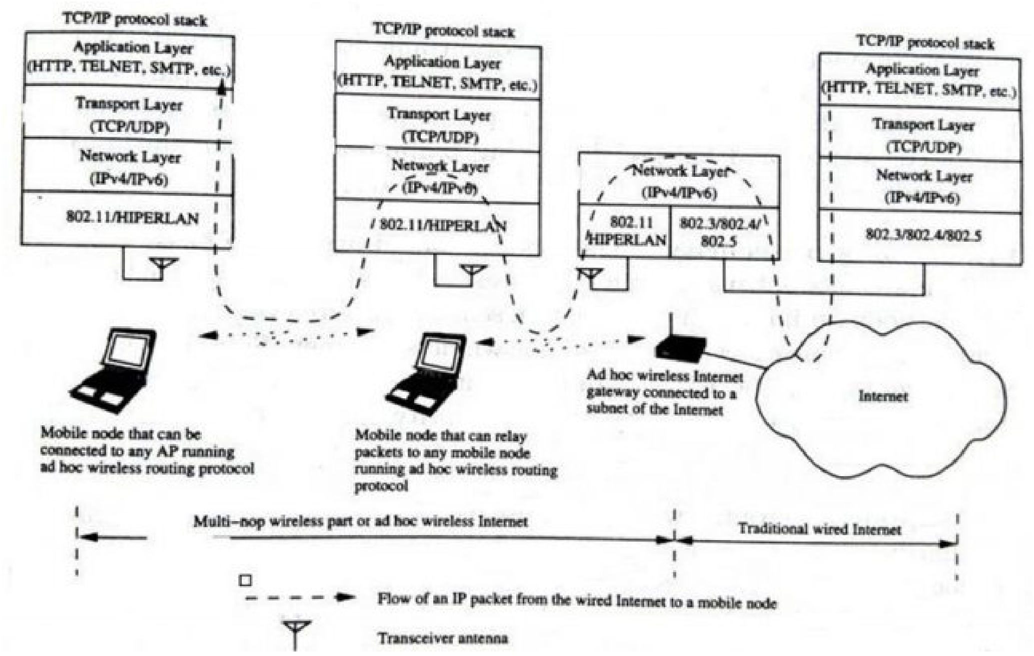


Figure (a) Ad Hoc Wireless Internet

Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

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.

1.6 Routing Protocols for Ad Hoc Wireless Networks

Routing is the exchange of information from one station of networks to other and Protocol is the set of standard or rules to exchange data between two devices.

An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network.

An ad hoc wireless network consists of a set of mobile nodes (hosts) that are connected by wireless links. The network topology (the physical connectivity of the communication network) in such a network may keep changing randomly.

Routing protocols that find a path to be followed by data packets from a source node to a destination node used in traditional wired networks cannot be directly applied in ad hoc wireless networks due to their highly dynamic topology absence of established infrastructure for centralized administration (e.g., base stations or access points), bandwidth-constrained wireless links, and resource (energy)-constrained nodes.

1.7 Issues in Designing a Routing Protocol for Ad Hoc Wireless Networks

The major challenges that a routing protocol designed for ad hoc wireless networks faces are:

- Mobility of nodes
- Bandwidth Constraints
- Error-Prone channel state
- Hidden Terminal Problem
- Exposed Terminal Problems
- Resource Constraints

1.7.1 Mobility

Network topology is highly dynamic due to movement of nodes. Hence, an ongoing session suffers frequent path breaks.

Disruption occurs due to the movement of either intermediate nodes in the path or end nodes.

Wired network routing protocols cannot be used in adhoc wireless networks because the nodes are here are not stationary and the convergence is very slow in wired networks.

Mobility of nodes results in frequently changing network topologies

Routing protocols for ad hoc wireless networks must be able to perform efficient and effective mobility management.

1.7.2 Bandwidth Constraint

Abundant bandwidth is available in wired networks due to the advent of fiber optics and due to the exploitation of wavelength division multiplexing (WDM) technologies.

In a wireless network, the radio band is limited, and hence the data rates it can offer are much less than what a wired network can offer.

This requires that the routing protocols use the bandwidth optimally by keeping the overhead as low as possible.

The limited bandwidth availability also imposes a constraint on routing protocols in maintaining the topological information.

1.7.3 Error-prone shared broadcast radio channel

The broadcast nature of the radio channel poses a unique challenge in ad hoc wireless networks.

The wireless links have time-varying characteristics in terms of link capacity and link- error probability.

This requires that the adhoc wireless network routing protocol interact with the MAC layer to find alternate routes through better-quality links.

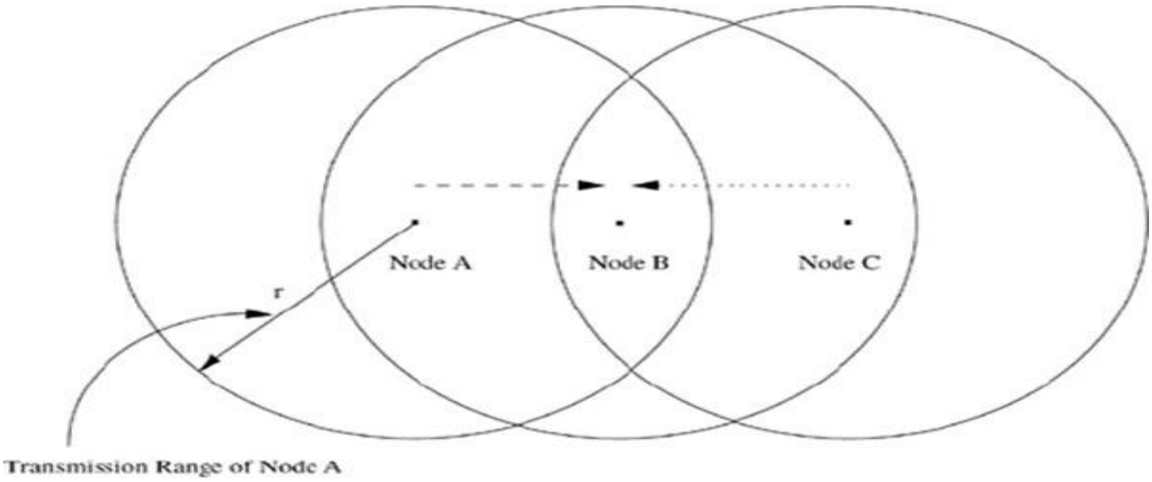
Transmissions in ad hoc wireless networks result in collisions of data and control packets.

Therefore, it is required that ad hoc wireless network routing protocols find paths with less congestion.

1.7.4 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 receiver, but are within the transmission range of the receiver.

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



Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

For example, consider figure (a). Here, if both node A and node C transmit to node B at the same time, their packets collide at node B. This is due to the fact that both node A and C are hidden from each other, as they are not within the direct transmission range of each other and hence do not know about the presence of each other.

Solution for this problem (figure 1.8), include medium access collision avoidance (MACA)

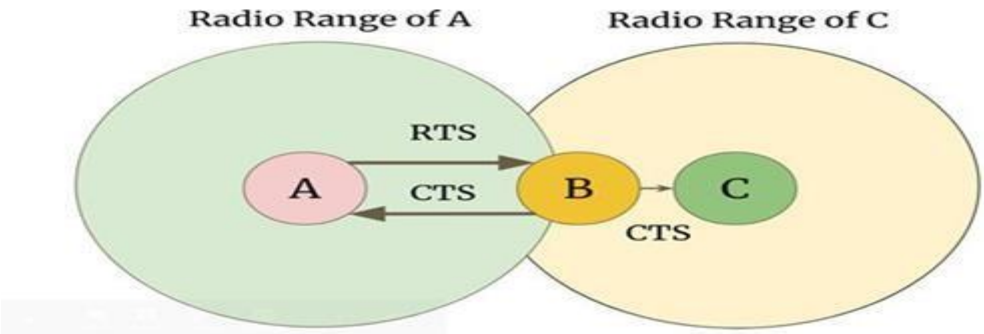


Figure 1.8 Solution for Hidden Terminal Problem

Transmitting node first explicitly notifies all potential hidden nodes about the forthcoming transmission by means of a two way handshake control protocol called RTS-CTS protocol exchange. This may not solve the problem completely but it reduces the probability of collisions.

1.7.5 Exposed Terminal Problem

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

For example, consider the figure 1.9, Here, if a transmission from node B to another node A is already in progress, node C cannot transmit to node D, as it concludes that its neighbor node B, is in transmitting mode and hence should not interfere with the on-going transmission. Thus, reusability of the radio spectrum is affected.

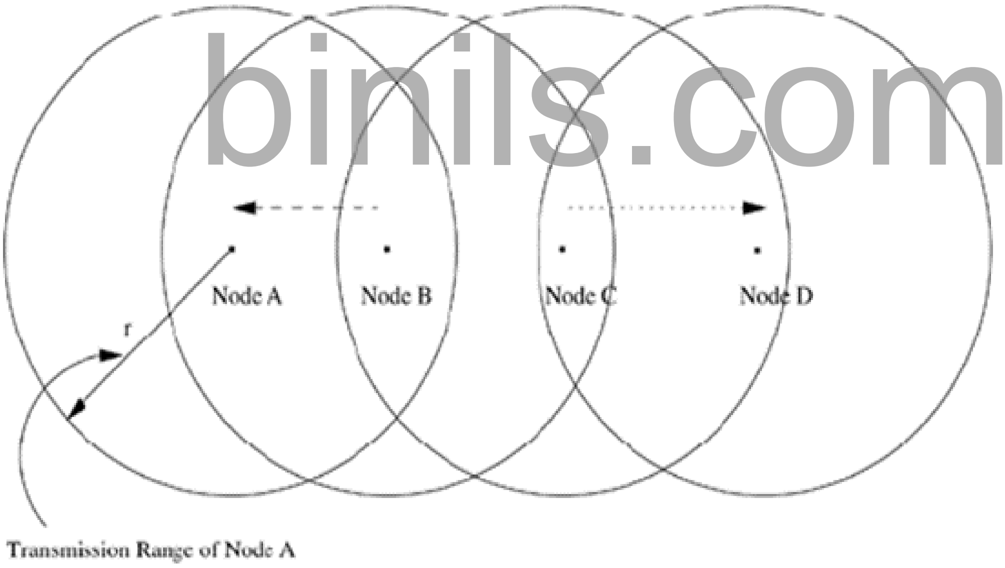


Figure 1. 9 Exposed Terminal Problem

Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

Solution for this problem, illustrated in figure 1.10. In this case, node A did not successfully receive the CTS originated by node R and hence assumes that there is no on-going transmission in the neighborhood. Since node A is hidden from node T, any attempt to originate its own RTS would result in collision of the on-going transmission between nodes T and R.

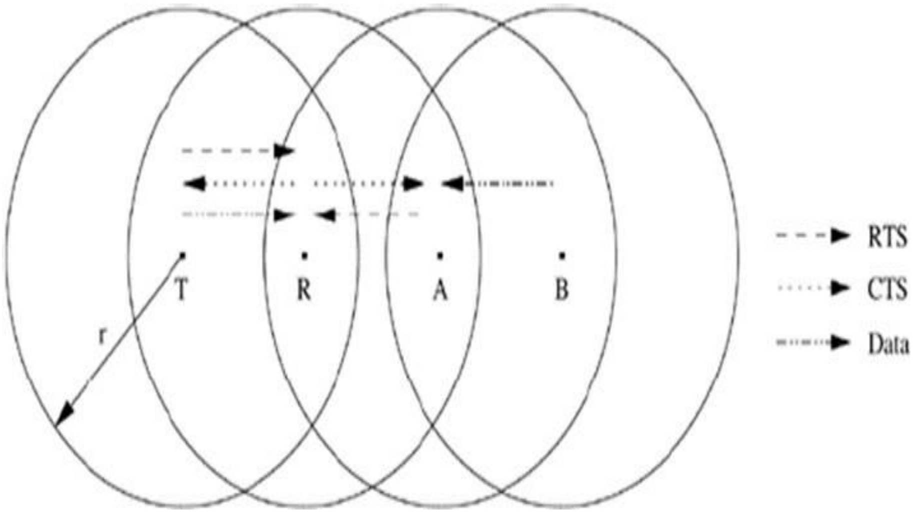


Figure 1. 10 Solution for Exposed Terminal Problem

Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

1.7.6 Resource Constraints

Two essential and limited resources are battery life and processing power.

Devices used in adhoc wireless networks require portability, and hence they also have size and weight constraints along with the restrictions on the power source.

Increasing the battery power and processing ability makes the nodes bulky and less portable.

1.8 Characteristics of an Ideal Routing Protocol for Ad Hoc Wireless Networks

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

- It must be fully distributed as centralized routing involves high control overhead and hence is not scalable.
- It must be adaptive to frequent topology changes caused by the mobility of nodes.

- Route computation and maintenance must involve a minimum number of nodes. Each node in the network must have quick access to routes, that is, minimum connection setup time is desired.
- It must be localized, as global state maintenance involves a huge state propagation control overhead.
- It must be loop-free and free from state routes.

- The number of packet collisions must be kept to a minimum by limiting the number of broadcasts made by each node. The transmissions should be reliable to reduce message loss and to prevent the occurrence of state routes.
- It must converge to optimal routes once the network topology becomes stable. The convergence must be quick.
- It must optimally use scarce resources such as bandwidth, computing power, memory, and battery power.
- Every node in the network should try to store information regarding the stable local topology only. Changes in remote parts of the network must not cause updates in the topology information maintained by the node.
- It should be able to provide a certain level of quality of service (QoS) as demanded by the applications, and should also offer support for time-sensitive traffic.

1.3 Issues in Ad hoc wireless networks

The major issues that affect the design, deployment, and performance of an ad hoc wireless system are as follows:

- Medium Access Control (MAC)
- Routing
- Multicasting
- Transport layer protocol
- Quality of Service (QOS)
- Self-organization
- Security
- Energy management
- Addressing and service discovery
- Scalability
- Deployment considerations

1.3.1 Medium Access Control

The purpose of this protocol is to achieve a distributed FIFO schedule among multiple nodes in an ad hoc network. When a node transmits a packet, it adds the information about the arrival time of queued packets. It provide fair access to shared broadcast radio channel. The major issues in MAC protocol are as follows:

- Distributed Operation: The MAC protocol design should be fully distributed involving minimum control overhead, because it need to operate in environment without centralized device.
- Synchronization: The synchronization is mandatory for TDMA-based systems for management of transmission and reception slots.
- Hidden Terminals Problem: 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. (Figure 1.2)

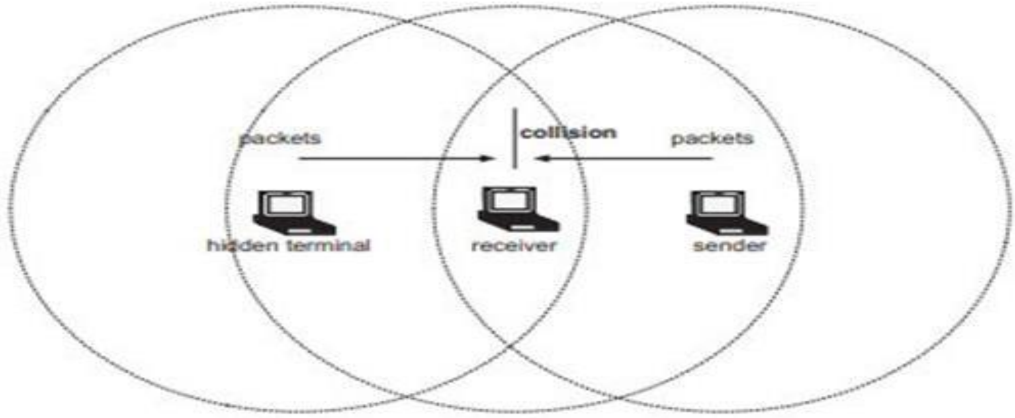


Figure 1.2 Hidden Terminal Problem

Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

Collisions at receiver node -> inefficient bandwidth utilization, reduce throughput.

- Exposed Terminals Problem: The nodes that are in the transmission range of the sender of an on-going session, are prevented from making a transmission. The exposed nodes should be allowed to transmit in a controlled fashion without causing collision to the on-going data transfer. (Figure 1.3)

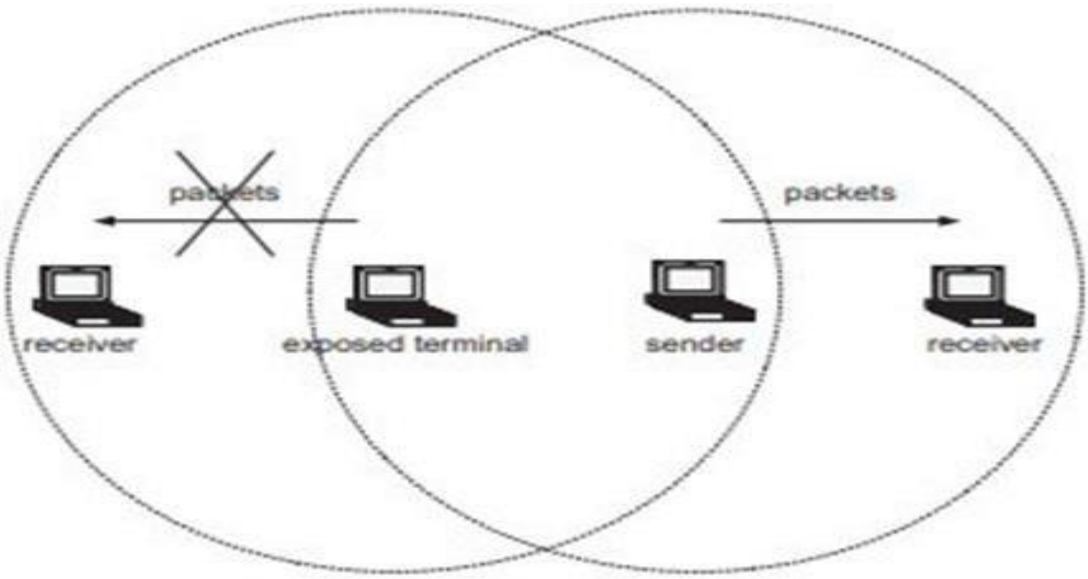


Figure 1.3 Exposed Terminal Problem

Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- Throughput: The MAC protocol employed in ad hoc 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
  - Minimizing control overhead.
- Access delay: The average delay that any packet experiences to get transmitted. The MAC protocol should attempt to minimize the delay.
- 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.
- 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.
- 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.
- 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.
- 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.

• 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.

1.3.2 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:

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

• 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.

• 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].

• 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.

• 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 ad hoc wireless networks are the following.

• Minimum route acquisition delay

- Quick route reconfiguration
- Loop-free routing
- Distributed routing approach
- Minimum control overhead
- Scalability
- Provisioning of QoS
- Support for time-sensitive traffic
- Security and privacy

1.3.3 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:

- 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.
- Efficiency: A multicast protocol should make a minimum number of transmissions to deliver a data packet to all the group members.
- Control overhead: The scarce bandwidth availability in ad hoc wireless networks demands minimal control overhead for the multicast session.
- Quality of Service: QoS support is essential in multicast routing because, in most cases, the data transferred in a multicast session is time-sensitive.

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

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

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

1.3.4 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.

1.3.5 Quality of Service (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

QoS-aware routing

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

1.3.6 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)

1.3.7 Security

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

Attacks against network are two types

- Passive attack → Made by malicious node to obtain information transacted in the network without disrupting the operation.
- Active attack → They disrupt the operation of network.

❒ Further active attacks are two 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.

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.

1.3.8 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.

1.3.9 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:

- 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.

- 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.

- 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.

- 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.

1.3.10 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.

1.3.11 Deployment Considerations

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

- 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.

- 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.

- Short deployment time

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

- 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.