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.

Applications
- Multimedia application
- Military application
- Defense application
- Emergency search and rescue operations
- Hybrid wireless network
- Communication among the nodes in a sensor network

Corresponding QoS parameter
- Bandwidth & Delay.
- Security & Reliability.
- Finding trustworthy intermediate hosts & routing.
- Availability.
- Maximum available link life, delay, bandwidth & channel utilization.
- Minimum energy consumption, battery life & energy conservation

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.
  - Path loss.

QoS framework:
- A framework for QoS is a complete system that attempts to provide the promised services to each user or application.
- The key component of QoS framework is a QoS service model which defines the way user requirements are served.

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)

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.

Addressing and service discovery

- Addressing & service discovery assume significance in ad hoc wireless network due to the absence of any centralized 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.

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
     ➢ Reachability 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 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.

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.

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) Re-configurability:**
- 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.

The following are the major issues to be considered in deploying an ad hoc wireless network:

**a) Scenario of deployment:**
- The scenario of deployment has significance because the capability required for a mobile node varies with the environment in which it is used.
- The following are some of the different scenarios in which the deployment issues vary widely:
  
  **- Military deployment:**
  It can be either,
  ✓ Data-centric network: Handle a different pattern of data traffic & can be partially comprised of static nodes.
  Eg: a wireless sensor network.
  ✓ User-centric network: Consists of highly mobile nodes with or without any support from any infrastructure.
  Eg: soldiers or armored vehicles carrying soldiers equipped with wireless communication devices.

  **- Emergency operations deployment:**
  o Demands a quick deployment of rescue personnel equipped with hand-held communication equipment.
  o The network should provide support for time-sensitive traffic such as voice & video.
  o Short data messaging can be used in case the resource constraints do not permit voice communication.

  **- Commercial wide-area deployment:**
  o Eg : wireless mesh networks.
  o The aim of the deployment is to provide an alternate communication infrastructure for wireless communication in urban areas & areas where a traditional cellular base station cannot handle the traffic volume.

  **- Home network deployment:**
  o Deployment needs to consider the limited range of the devices that are to be connected by the network.
  o Eg : short transmission range avoid network partitions.
b) **Required longevity of network:**
- If the network is required for a short while, battery-powered mobile nodes can be used.
- If the connectivity is required for a longer duration of time, fixed radio relaying equipment with regenerative power sources can be deployed.

c) **Area of coverage:**
- Determined by the nature of application for which the network is set up.
- Eg: the home area network is limited to the surroundings of a home.
- The mobile nodes’ capabilities such as the transmission range & associated hardware, software, & power source should match the area of coverage required.

d) **Service availability:**
- Defined as the ability of an ad hoc wireless network to provide service even with the failure of certain nodes.
- Has significance in a fully mobile ad hoc wireless network used for tactical communication & in partially fixed ad hoc wireless network used in commercial communication infrastructure such as wireless mesh networks.

e) **Operational integration with other infrastructure:**
- Considered for improving the performance or gathering additional information, or for providing better QoS.
- In military environment, integration of ad hoc wireless networks with satellite networks or unmanned aerial vehicles (UAVs) improves the capability of the ad hoc wireless networks.

f) **Choice of protocol:**
- The choice of protocols at different layers of the protocol stack is to be done taking into consideration the deployment scenario.
- A TDMA-based & insecure MAC protocol may not be the best suited compared to a CDMA-based MAC protocol for a military application.