

INTRODUCTION TO ADHOC WIRELESS NETWORKS

CELLULAR AND AD HOC WIRELESS NETWORKS

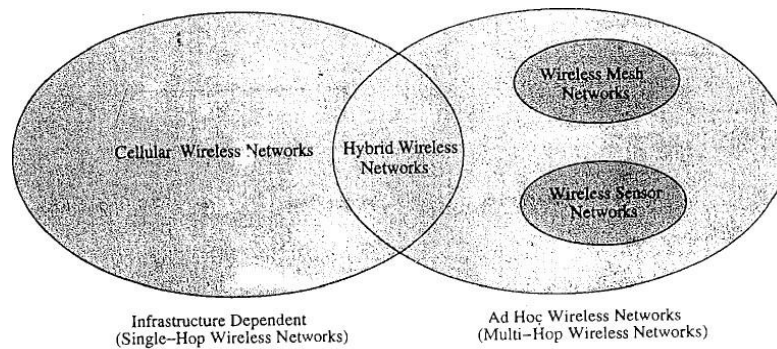


Figure 1: Cellular and ad hoc wireless networks.

The current cellular wireless networks are classified as the infrastructure dependent network. The path setup for a call between two nodes, say, node C to E, is completed through base station as illustrated in figure below.

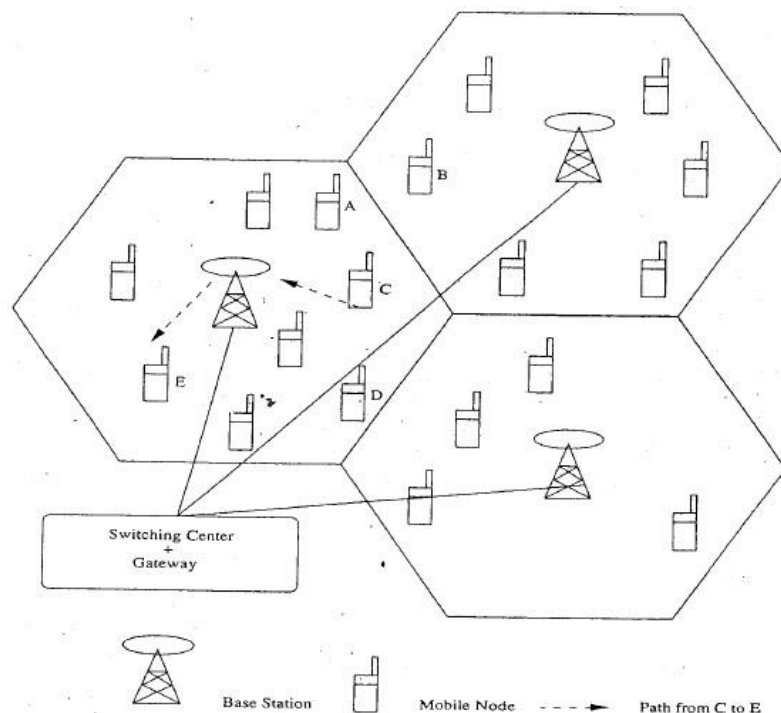


Figure 2 A cellular network

- Adhoc wireless networks are defined as a category of wireless network that utilize multi-hop radio replaying and are capable of operating without the support of any fixed infrastructure.
- Absence of any central co-ordinator or base station makes the routing complex.
- Adhoc wireless network topology for the cellular network shown in above figure is illustrated below.
- The path setup for a call between 2 nodes, say, node C to E , is completed through the intermediate mobile node F.
- Wireless mesh network and Wireless sensor networks are specific examples of adhoc wireless networks.

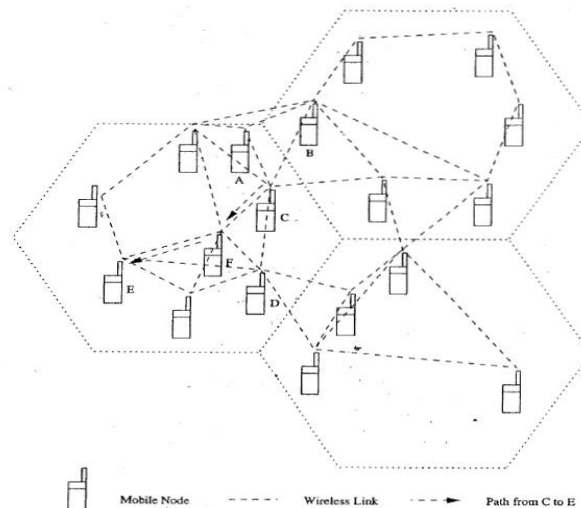


Figure 3: An ad hoc wireless network

- The presence of base station simplifies routing and resource management in a cellular network.
- But in adhoc networks, routing and resource management are done in a distributed manner in which all nodes co-ordinate to enable communication among them.

The following table shows the difference between cellular networks and adhoc wireless networks.

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)	Frequent path breaks 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 sectors	Application domains include battlefields, emergency search and rescue operations, 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 capability)
Major goals of routing and call admission are to maximize the call acceptance ratio and minimize the call drop ratio	Main 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 of evolution	Several issues are to be addressed for successful commercial deployment even though widespread use exists in defense

APPLICATIONS OF AD HOC WIRELESS NETWORKS

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.

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

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

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 extendability, high availability & low cost per bit.

Wireless Sensor Networks:

- Sensor networks are special category of Adhoc wireless network that are used to provide a wireless communication infrastructure among the sensors deployed in a specific application domain.
- Sensor nodes are tiny devices that have capability of sensing physical parameters processing the data gathered, & communication to the monitoring system.
- The issue that make sensor network a distinct category of adhoc wireless network are the following:

Mobility of nodes :

- ✓ Mobility of nodes is not a mandatory requirement in sensor networks.
- ✓ For example, the nodes used for periodic monitoring of soil properties are not required to be mobile & the nodes that are fitted on the bodies of patients in a post-surgery ward of a hospital are designed to support limited or partial mobility.
- ✓ In general, sensor networks need not in all cases be designed to support mobility of sensor nodes.

Size of the network :

- ✓ The number of nodes in sensor network can be much larger than that in a typical ad hoc wireless network.

Density of deployment :

- ✓ The density of nodes in a sensor network varies with the domain of application.
- ✓ For example, Military applications require high availability of the network, making redundancy a high priority.

Power constraints :

- ✓ The power constraints in sensor networks are much more stringent than those in ad hoc wireless networks. This is mainly because the sensor nodes are expected to operate in harsh environmental or geographical conditions, with minimum or no human supervision and maintenance.
- ✓ In certain case, the recharging of the energy source is impossible.
- ✓ Running such a network, with nodes powered by a battery source with limited energy, demands very efficient protocol at network, data link, and physical layer.
- ✓ The power sources used in sensor networks can be classified into the following 3 categories:
 - *Replenishable Power source*: The power source can be replaced when the existing source is fully drained.
 - *Non-replenishable Power source*: The power source cannot be replenished once the network has been deployed. The replacement of sensor node is the only solution.
 - *Regenerative Power source*: Here, Power source employed in sensor network have the capability of regenerating power from the physical parameter under measurement.

Data / Information fusion :

- ✓ Data fusion refers to the aggregation of multiple packets into one before relaying it.
- ✓ Data fusion mainly aims at reducing the bandwidth consumed by redundant headers of the packets and reducing the media access delay involved in transmitting multiple packets.
- ✓ Information fusion aims at processing the sensed data at the intermediate nodes and relaying the outcome to the monitor node.

Traffic Distribution :

- ✓ The communication traffic pattern varies with the domain of application in sensor networks.
- ✓ For example, the environmental sensing application generates short periodic packets indicating the status of the environmental parameter under observation to a central monitoring station.
- ✓ This kind of traffic requires low bandwidth.
- ✓ Ad hoc wireless networks generally carry user traffic such as digitized & packetized voice stream or data traffic, which demands higher bandwidth.

Hybrid Wireless Networks

- One of the major application area of ad hoc wireless network is in the hybrid wireless architecture such as Multi-hop Cellular Network [MCN] & Integrated Cellular Adhoc Relay [iCAR].
- The primary concept behind cellular networks is geographical channel reuse.
- Several techniques like cell sectoring, cell resizing and multi tier cells increase the capacity of cellular networks.
- MCNs combine the reliability & support of fixed base station of cellular network with flexibility & multi-hop relaying adhoc wireless networks.
- Major advantages are as follows:
 - Higher capacity than cellular networks due to the better channel reuse.
 - Increased flexibility & reliability in routing.
 - Better coverage & connectivity in holes of a cell can be provided by means of multiple hops through intermediate nodes in a cell.

ISSUES 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

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 *cogestion 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.

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.

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.

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.

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.

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 is basically depends on three components which are listed below

- **QoS parameters : depends upon applications**

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.

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 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.

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 machine is idle for a long time. In such a case, 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) *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.

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 :*
 - Demands a quick deployment of rescue personnel equipped with hand-held communication equipment.
 - The network should provide support for time-sensitive traffic such as voice & video.
 - Short data messaging can be used in case the resource constraints do not permit voice communication.
 - *Commercial wide-area deployment :*
 - Eg : wireless mesh networks.
 - 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 :*
 - Deployment needs to consider the limited range of the devices that are to be connected by the network.
 - 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.

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 :

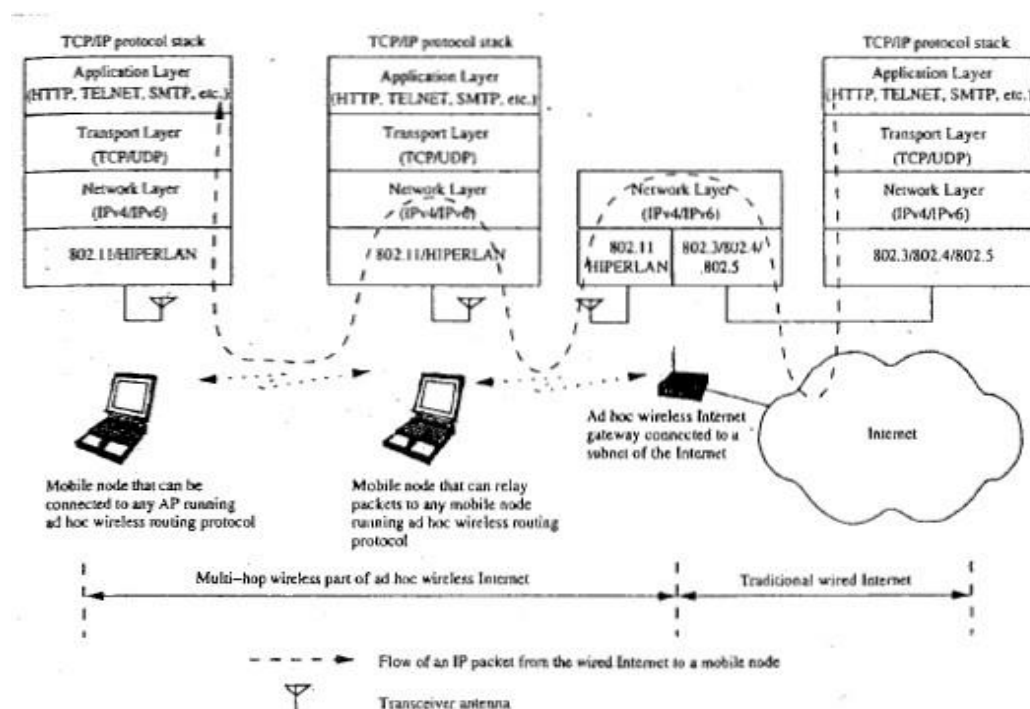


Figure 4. Schematic diagram of ad hoc wireless internet

❖ **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.
- 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.

MAC PROTOCOLS

ISSUES IN DESIGNING MAC PROTOCOL FOR AD HOC WIRELESS NETWORK

The main issues in designing MAC protocol for ad hoc wireless network are:

Bandwidth efficiency

- Bandwidth must be utilized in efficient manner
- Minimal Control overhead
- $BW = \text{ratio of BW used for actual data transmission to the total available BW}$

Quality of service support

- ★ Essential for supporting time-critical traffic sessions
- ★ They have resource reservation mechanism that takes into considerations the nature of wireless channel and the mobility of nodes

Synchronisation

- ★ MAC protocol must consider synchronisation between nodes in the network
- ★ Synchronisation is very important for BW (time slot) reservation by nodes
- ★ Exchange of control packets may be required for achieving time synchronisation among nodes

Hidden and exposed terminal problems

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

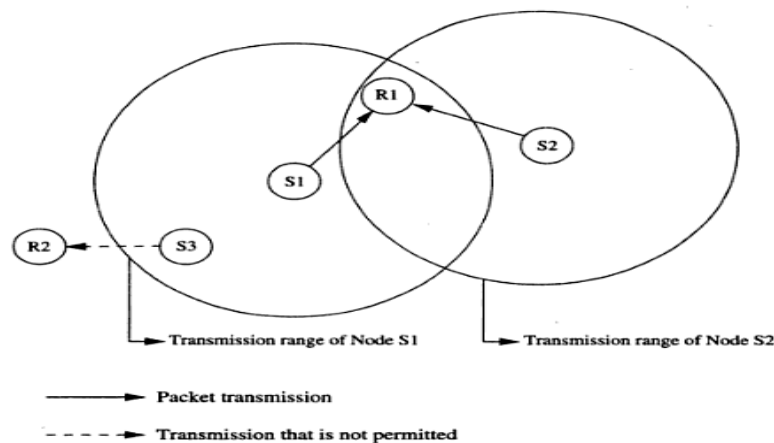


Figure 6.1. Hidden and exposed terminal problems.

- ★ S1 and S2 are hidden from each other & they transmit simultaneously to R1 which leads to collision
- ★ 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
- ★ If S1 is already transmitting to R1, then S3 cannot interfere with on-going transmission & it cannot transmit to R2.
- ★ The hidden & exposed terminal problems reduce the throughput of a network when traffic load is high

Error-prone shared broadcast channel

- ★ When a node is receiving data, no other node in its neighbourhood should transmit
- ★ A node should get access to the shared medium only when its transmission do not affect any ongoing session
- ★ MAC protocol should grant channel access to nodes in such a manner that collisions are minimized
- ★ Protocol should ensure fair BW allocation

Distributed nature/lack of central coordination

- ★ Do not have centralised coordinators
- ★ Nodes must be scheduled in a distributed fashion for gaining access to the channel
- ★ MAC protocol must make sure that additional overhead, in terms of BW consumption, incurred due to this control information is not very high

Mobility of nodes

- ★ Nodes are mobile most of the time
- ★ The protocol design must take this mobility factor into consideration so that the performance of the system is not affected due to node mobility

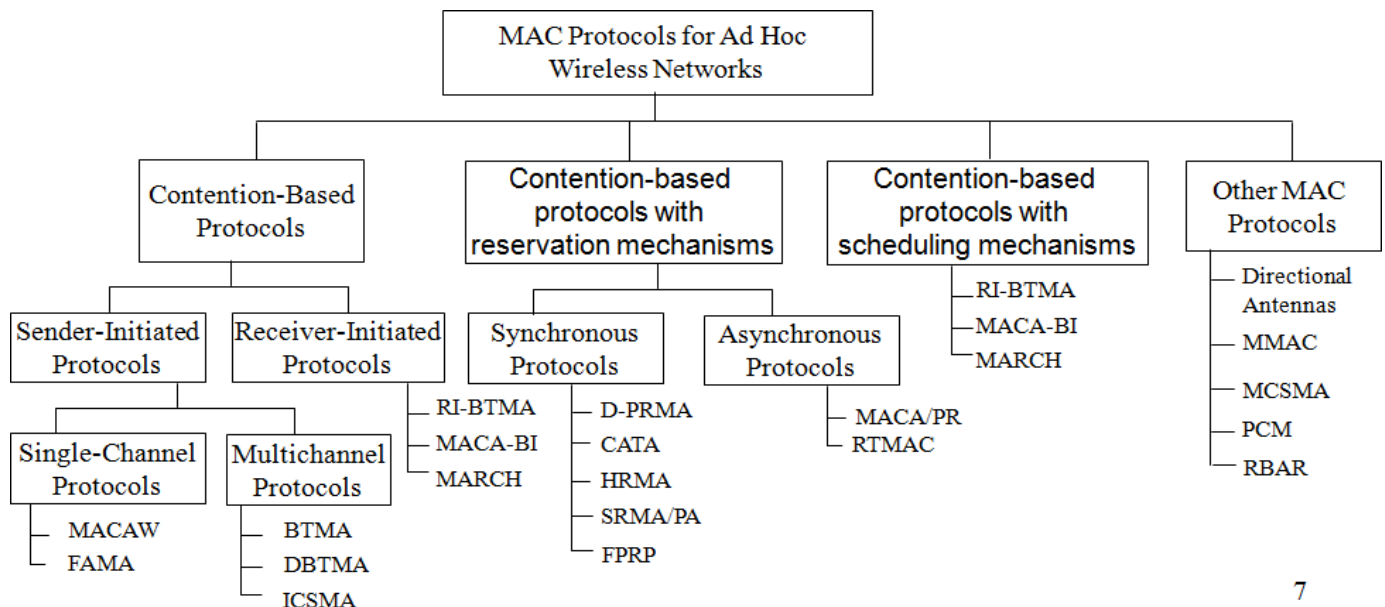
DESIGN GOALS OF A MAC PROTOCOL FOR AD HOC WIRELESS NETWORKS

- The operation of a protocol should be distributed
- The protocol should provide QoS support for real-time traffic
- The access delay, which refers to the average delay experienced by any packet to get transmitted, must be kept low
- The available bandwidth must be utilised efficiently
- The protocol should ensure fair allocation of bandwidth to nodes
- Control overhead must be kept as low as possible
- The protocol should minimise the effects of hidden and exposed terminal problems
- The protocol must be scalable to large networks
- It should have power control mechanisms in order to efficiently manage energy consumption of the nodes
- The protocol should have mechanisms for adaptive data rate control
- It should try to use directional antennas which can provide advantages such as reduced interference, increased spectrum reuse, and reduced power consumption
- The protocol should provide time synchronisation among nodes

CLASSIFICATION OF MAC PROTOCOLS

Ad hoc network MAC protocols can be classified into three basic types:

- Contention-based protocols
- Contention-based protocols with reservation mechanisms
- Contention-based protocols with scheduling mechanisms
- OTHER MAC protocols [protocols which do not fall under above 3 categories]



- **Contention-based protocols**
 - ***Sender-initiated protocols***: Packet transmissions are initiated by the sender node.
 - *Single-channel sender-initiated protocols*: A node that wins the contention to the channel can make use of the entire bandwidth.
 - *Multichannel sender-initiated protocols*: The available bandwidth is divided into multiple channels.
 - ***Receiver-initiated protocols***: The receiver node initiates the contention resolution protocol.
- **Contention-based protocols with reservation mechanisms**
 - ***Synchronous protocols***: All nodes need to be synchronized. Global time synchronization is difficult to achieve.
 - ***Asynchronous protocols***: These protocols use relative time information for effecting reservations.
- **Contention-based protocols with scheduling mechanisms**
 - Node scheduling is done in a manner so that all nodes are treated fairly and no node is starved of bandwidth.
 - Scheduling-based schemes are also used for enforcing priorities among flows whose packets are queued at nodes.
 - Some scheduling schemes also consider battery characteristics.
- **Other protocols** are those MAC protocols that do not strictly fall under the above categories.

CONTENTION BASED PROTOCOLS

SENDER INITIATED SINGLE CHANNEL PROTOCOL:

Multiple access collision avoidance for wireless LAN (MACAW) protocol

- MACAW is a revision of MACA protocol
- The sender senses the carrier to see and transmits a **RTS (Request To Send)** frame if no nearby station transmits a RTS.
- The receiver replies with a **CTS (Clear To Send)** frame.
- The MACAW protocol uses one more control packet called the **request-for-request-to-send (RRTS)**

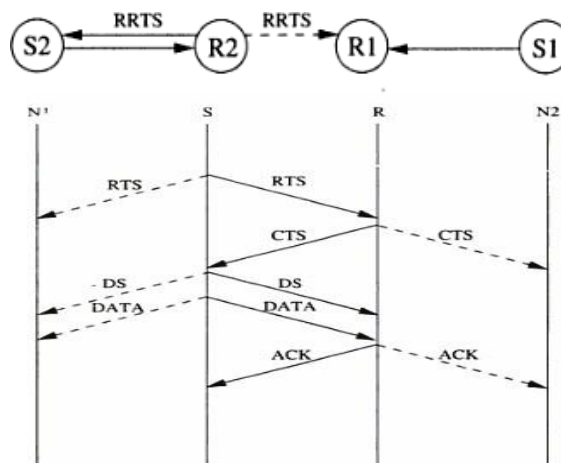


Figure 6.7. Packet exchange in MACAW.

- Neighbors
 - see CTS, then keep quiet.
 - see RTS but not CTS, then keep quiet until the CTS is back to the sender.
- The receiver sends an ACK when receiving a frame.
 - Neighbors keep silent until see ACK.
- Collisions
 - There is no collision detection.
 - The senders know collision when they don't receive CTS.
 - They each wait for the exponential back-off time.

SENDER INITIATED MULTICHANNEL PROTOCOL:

Busy Tone Multiple Access Protocol (BTMS)

- The busy tone multiple access (BTMA) protocol is one of the earliest protocols proposed for overcoming the hidden terminal problem faced in wireless environments.
- The transmission channel is split into two: a data channel and a control channel. The data channel is used for data packet transmissions, while the control channel is used to transmit the busy tone signal.
- When a node is ready for transmission, it senses the channel to check whether the busy tone is active. If not, it turns on the busy tone signal and starts data transmission;
- otherwise, it reschedules the packet for transmission after some random rescheduling delay. Any other node which senses the carrier on the incoming data channel also transmits the busy tone signal on the control channel. Thus, when a node is transmitting, no other node in the two-hop neighborhood of the transmitting node is permitted to simultaneously transmit.
- Though the probability of collisions is very low in BTMA, the bandwidth utilization is very poor.

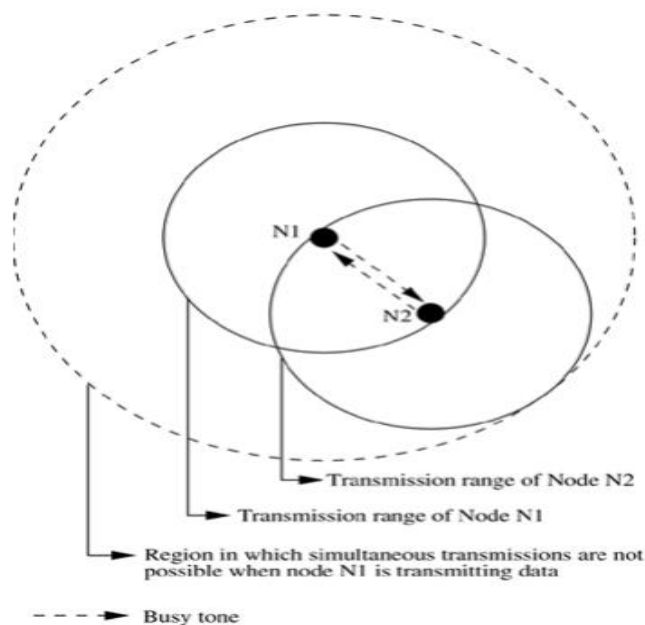


fig .Packet transmission in BTMS

- Figure above shows the worst-case scenario where the node density is very high; the dotted circle shows the region in which nodes are blocked from simultaneously transmitting when node N1 is transmitting packets.

RECIEVER INITIATED PROTOCOL:

Reciever Initiated Busy Tone Multiple Access Protocol (RI-BTMS)

- In the receiver-initiated busy tone multiple access protocol (RI-BTMA), similar to BTMA, the available bandwidth is divided into two channels: a data channel for transmitting data packets and a control channel.
- The control channel is used by a node to transmit the busy tone signal. A node can transmit on the data channel only if it finds the busy tone to be absent on the control channel.
- The busy tone serves two purposes. First, it acknowledges the sender about the successful reception of the preamble. Second, it informs the nearby hidden nodes about the impending transmission so that they do not transmit at the same time
- The data packet is divided into two portions: a preamble and the actual data packet. The preamble carries the identification of the intended destination node.
- Data transmission consists of two steps. First, the preamble needs to be transmitted by the sender.

- Once the receiver node acknowledges the reception of this preamble by transmitting the busy tone signal on the control channel, the actual data packet is transmitted.
- A sender node that needs to transmit a data packet first waits for a free slot, that is, a slot in which the busy tone signal is absent on the control channel. Once it finds such a slot, it transmits the preamble packet on the data channel.
- If the destination node receives this preamble packet correctly without any error, it transmits the busy tone on the control channel. It continues transmitting the busy tone signal as long as it is receiving data from the sender.
- If preamble transmission fails, the receiver does not acknowledge with the busy tone, and the sender node waits for the next free slot and tries again.
- The operation of the RI-BTMA protocol is shown in Figure below.

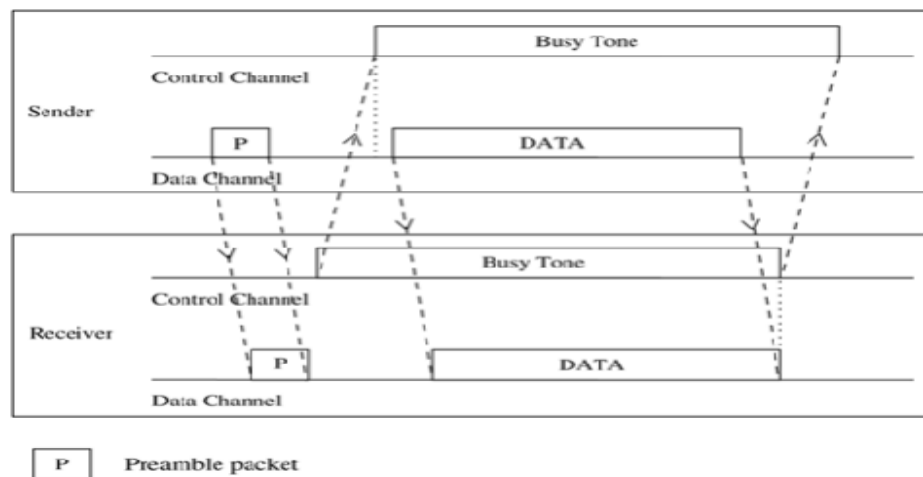


fig .Packet transmission in RI-BTMS

CONTENTION BASED PROTOCOLS WITH RESERVATION MECHANISMS

Synchronous protocols:

Collision Avoidance Time Allocation Protocol (CATA)

- It is based on dynamic topology-dependent transmission scheduling
- Nodes contend for and reserve time slots by means of a distributed reservation and handshake mechanism.
- Support broadcast, unicast, and multicast transmissions.
- The operation is based on two basic principles:
 - The receiver(s) of a flow must inform the potential source nodes about the reserved slot on which it is currently receiving packets. The source node must inform the potential destination node(s) about interferences in the slot.
 - Usage of negative acknowledgements for reservation requests, and control packet transmissions at the beginning of each slot, for distributing slot reservation information to senders of broadcast or multicast sessions.
- Time is divided into equal-sized frames, and each frame consists of S slots.
- Each slot is further divided into five minislots.
- The first 4 minislots are used for transmitting control packets and are called control minislots (CMS)

- The last minislot is called data minislot (DMS)

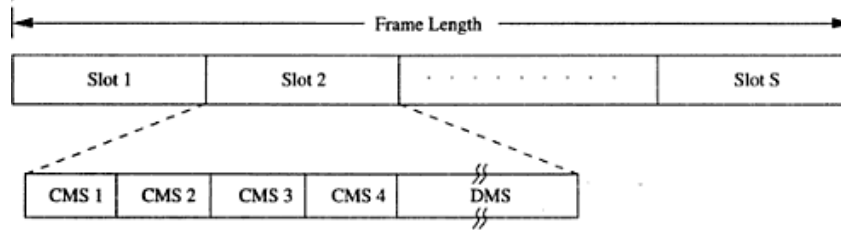


Figure 6.16. Frame format in CATA.

- Each node that receives data during the DMS of the current slot transmits a slot reservation (SR) packet during the CMS1 of the slot
- This serves to inform other neighbouring potential sender nodes about the currently active reservations
- The SR packet is either received without error at the neighbouring nodes or causes noise at those nodes, preventing them from attempting to reserve the current slot
- Every node that transmits data during the DMS of the current slot transmits a request-to-send packet
- The receiver node of a unicast session transmits a clear-to-send packet
- On receiving this packet, the source node clearly understands that the reservation was successful and transmits data during the DMS of that slot until unicast flow gets terminated
- Once the reservation has been made successfully in a slot, from the next slot onward, both the sender and receiver do not transmit anything during CMS3 and during CMS4 the sender node alone transmits a not-to-send (NTS) packet
- The not-to-send (NTS) packet serves as a negative acknowledgement
- A potential multicast or broadcast source node that receives the NTS packet or that detects noise, understands that its reservation request has failed & does not transmit during DMS of current slot
- The length of the frame is very important in CATA
- The worst case value of the frame-length = $\text{Min}(d^2+1, N)$, where d is the maximum degree of a node in the network and N is the total number of nodes in the network
- CATA works well with simple single-channel half-duplex radios
- It is simple and provides support for collision-free broadcast and multicast traffic

Asynchronous protocols:

MACA with Piggy-Backed Reservation

- Provide real-time traffic support in multi-hop wireless networks
- Based on the MACAW protocol with non-persistent CSMA
- The main components of MACA/PR are:
 - ✓ A MAC protocol
 - ✓ A reservation protocol
 - ✓ A QoS routing protocol
- Differentiates real-time packets from the best-effort packets
- Provide guaranteed BW support for real-time packets

- Provides reliable transmission of best efforts packets

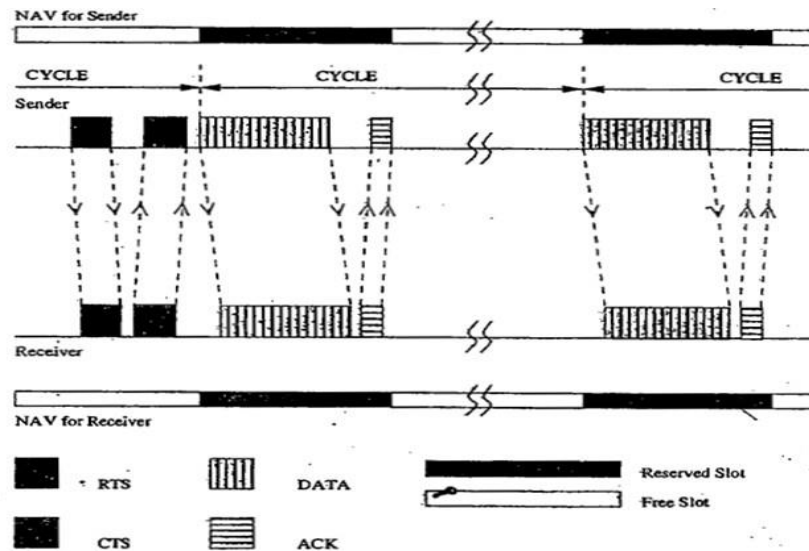


Figure 6.23. Packet transmission in MACA/PR.

- Time is divided into slots
- Slots are defined by the reservations made at nodes
- They are asynchronous in nature with varying lengths
- Each node in the network maintains a reservation table (RT) that records all the reserved transmit and receive slots/windows of all nodes within its transmission range
- The sender is assumed to transmit real-time packets at certain regular intervals, say, every CYCLE time period
- The first data packet of the session is transmitted in the usual manner
- The source node first sends an RTS packet, for which the receiver responds with a CTS packet
- Now the source node sends the first DATA packet of the real-time session
- Reservation information for the next DATA packet to be transmitted is piggy-backed on this current DATA packet.
- On receiving this DATA packet, the receiver node updates its reservation table with the piggy-backed reservation information
- It then sends ACK packet back to the source
- Receiver node piggy-backs the reservation confirmation information on the ACK packet
- Slot reservation information maintained in the reservation tables is refreshed every cycle
- Thus, MACA/PR is an efficient bandwidth reservation protocol that can support real-time traffic sessions
- Advantage → it does not require global synchronization among nodes
- Drawback → a free slot can be reserved only if it can fit the entire RTS-CTS-DATA-ACK exchange