MAC Layer Protocols for MANET
OSI MODEL
OSI Layers

1. Delivers letters & packages
   - Mail Carrier
2. Pack letter for individual
   - Intake & Sorting
3. Takes letter and puts in right compartment
   - Intake & Sorting
4. Drives letter to post office
   - Driver
5. Provides address. Puts in envelope
   - Secretary
6. Proofreads, corrects and prepares the message
   - Assistant
7. Dictates or writes a message
   - Manager

- Reads message
- Alerts manager of incoming message
- Opens message. Reads it
- Picks up message from post office
- Sorts messages
- Unpacks packages from various sources
- Picks up letters & packages
VARIOUS FUNCTION OF OSI MODEL

7. Application → Network Processes to Applications
6. Presentation → Data Representation
5. Session → Interhost Communication
4. Transport → End-to-end Connections
3. Network → Address and Best Path
2. Data Link → Access to Media
1. Physical → Binary Transmission
Layer - 7: Application
Layer - 6: Presentation
Layer - 5: Session
Layer - 4: Transport
Layer - 3: Network
Layer - 2: Data Link
Layer - 1: Physical

Upper Layer or Software Layer
Heart of OSI
Lower Layer or Hardware Layer
Data Link Layer:

- The main function of data link layer is to take data in the form of 0 & 1 from physical layer, check transmission error and pack it into frames and give it to network layer.
- To decrease complexity of data link layer, it is divided into two sub layers.

  1- Logical Link Control (LLC)
  2- Multiple Access Control (MAC)
DATA LINK LAYER

Network layer

Gives services to

Data link layer

Packetizing
Flow control
Media access control
Addressing
Error control

Receives services from

Physical layer

LANs

WANs
Logical Link Control (LLC)

- It provides services to network layer or upper layer.
- It establishes and controls link between local devices.
- It hides data link layer details from network layer.
- All different technologies to work seamlessly with the upper layers.
Medium Access Control (MAC) ?

- MAC protocols play an important role in the performance of MANETs.
- The MAC protocol is primarily responsible for regulating access to the shared medium.
- It decides how devices will access the medium.
- These protocols are responsible for per-link connection establishment (i.e., acquiring the medium) and per-link connection cancellation (i.e., releasing the medium).
Many people gather in a large room
- “Give everyone a chance to speak”
- “Don’t speak until you are spoken to”
- “Don’t monopolize the conversation”
- “Raise your hand if you have a question”
- “Don’t interrupt when someone is speaking”
- “Don’t fall asleep when someone else is talking”
SAME RULE FOR MULTIPLE ACCESS

- Broadcast medium – air

- The problem of controlling the access to the medium is similar to the rules of speaking

- If more than 2 users transmit at the same time - collision

- All collided packets are lost -> waste of bandwidth
CHALLENGES IN MOBILE ENVIRONMENTS (NEED OF MAC)

- Limitations of the Wireless Network
  - packet loss due to transmission errors
  - variable capacity links
  - frequent disconnections/partitions
  - limited communication bandwidth
  - Broadcast nature of the communications

- Limitations Imposed by Mobility
  - dynamically changing topologies/routes
  - lack of mobility awareness by system/applications

- Limitations of the Mobile Computer
  - short battery lifetime
  - limited capacities
DESIGN GOALS OF A MAC PROTOCOL-I

- The operation of the 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 utilized efficiently.
- The protocol should ensure fair allocation of bandwidth to nodes.
- Control overhead must be kept as low as possible.
Design Goals of a MAC Protocol-II

- The protocol should minimize the effects of hidden and exposed terminal problems.
- The protocol must be scalable to large networks.
- The protocol must have power control mechanisms.
- The protocol should have mechanisms for adaptive data rate control.
- The protocol should provide synchronization among nodes.
There are hundreds of MAC protocols proposed for wireless networks.

We need performance metrics so that we can compare one protocol from the other.

The key metrics are:

- Throughput
- Delay
- Fairness
- Stability
- Robustness against channel fading
- Power Consumption
- Support for multimedia
MAC PERFORMANCE METRICS

- **Throughput**:  
  - Average rate of successful message delivery over a communication channel from source to destination.  
  - MAC need to maximize throughput while keeping the access delay to minimum

- **Delay**:  
  - Defined as the average time spent by a packet in the MAC queue,  
  - Sensitive to traffic characteristics,  
  - So two MAC protocols should be compared under identical traffic conditions
○ **Fairness:**
  - **It is** measure of how fair the channel allocation is among the nodes.
  - When all nodes are treated equally, and no node is given preference
  - Leads to fair sharing of bandwidth
  - Traffic with different priorities can bias this definition
  - For multimedia traffic, usually the MAC is considered fair when (voice, data, video) get their allocated bandwidth

○ **Stability:**
  - System need to be stable if instantaneously high load is seen by the MAC
- **Robustness against channel fading**:
  - Wireless channel is time varying and error prone
  - Fading may make channel unusable for short durations
  - MAC needs to work reliably while channel in fade

- **Power Consumption**:
  - Wireless nodes have limited battery power -> MAC should conserve energy

- **Support for multimedia**:
  - MAC should support multimedia applications (voice, video, data)
  - Multimedia data implies data with real-time constraints
  - By using priorities and scheduling – delay can be controlled and/or guaranteed
MAC CLASSIFICATION
Medium Access Control

Contestion Free (Polling, Token-Based, TDMA, CDMA, FDMA)

Contestion Based

Random Access

Noncarrier Sensing (ALOHA, Slotted ALOHA)

Carrier Sensing (CSMA)

Reservation/Collision Resolution

Use of Control Packet (MACA, MACAW)

Use of Control Packets and Carrier Sensing (FAMA, CSMA/CA, IEEE802.11)
Contention-Free Medium Access (Fixed Assignment)

- The aim of MAC is to provide an orderly and efficient use of the common spectrum to avoid any collision.
- Collisions can be avoided by ensuring that each node can use its allocated resources exclusively.
TYPES OF CONTENTION FREE MAC

- **FDMA:**
  - The frequency band is divided into several smaller frequency bands, the data transfer between a pair of nodes uses one frequency band
TDMA: Multiple devices to use the same frequency band but at different slot
frames consist of a fixed number of transmission slots to separate the medium accesses of different devices
a time schedule indicates which node may transmit data during a certain slot

CDMA: Simultaneous accesses of the wireless medium are supported using different codes
if these codes are orthogonal, it is possible for multiple communications to share the same frequency band
Polling based protocols:
- A controller device issues small polling frames in a round-robin fashion,
- Asking each station if it has data to send
- If no data to be sent, the controller polls the next station

Token passing:
- Stations pass a polling request to each other (round-robin fashion) using a special frame called a token
- A station is allowed to transmit data only when it holds the token
Reservation-based protocols:

- static time slots used to reserve future access to the medium e.g., a node can indicate its desire to transmit data by toggling a reservation bit in a fixed location.

- these often very complex protocols then ensure that other potentially conflicting nodes take note of such a reservation to avoid collisions.
CONTENTION-BASED MEDIUM ACCESS

- no station is superior and none is assigned the control over another.
- A station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.
- This decision depends on the state of the medium (idle or busy).
CONTENTION-BASED MEDIUM ACCESS

Random Access
- Noncarrier Sensing (ALOHA, Slotted ALOHA)
  - Carrier Sensing (CSMA)

Reservation/Collision Resolution
- Use of Control Packet (MACA, MACAW)
  - Use of Control Packets and Carrier Sensing (FAMA, CSMA/CA, IEEE802.11)
RANDOM ACCESS

- In this method, each station has the right to the medium without being controlled by any other station.

- However, if more than one station tries to send, there is an access conflict-collision-and the frames will be either destroyed or modified.
Why is this called Contention and Random access protocol?
1- No rules specify which station should send next i.e. stations compete with one another to access the medium.

2- There is no scheduled time for a station to transmit i.e. transmission is random among the stations.
HOW TO AVOID ACCESS CONFLICT?
To avoid access conflict or to resolve it, each station follows a procedure that answers the following questions:

- When the station can access the medium?
- What the station can do if the medium is busy?
- How the station can determine the success or failure of the transmission?
- What the station can do if there is an access conflict?
NON CARRIER SENSING PROTOCOL-ALOHA

- Developed by Norm Abramson at the Univ. of Hawaii
- Designed for a radio (wireless) LAN, but it can be used on any shared medium.
- **Aloha** in the Hawaiian language means affection, peace, compassion and mercy.
The original ALOHA protocol is called pure ALOHA.
This is a simple and elegant protocol.
The idea is that each station sends a frame whenever it has a frame to send.
Since there is only one channel to share, there is the possibility of collision between frames from different stations.
PURE ALOHA

Station 1
Frame 1.1
Frame 1.2
Collision duration

Station 2
Frame 2.1
Frame 2.2
Collision duration

Station 3
Frame 3.1
Frame 3.2
Collision duration

Station 4
Frame 4.1
Frame 4.2
Collision duration
The pure ALOHA is based on ACK from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgment. If the ACK does not arrive after a time-out period, the station assumes that the frame (or the ACK) has been destroyed and there is need to resend the frame.
A collision involves two or more stations.

If all these stations try to resend their frames after the time-out, the frames may be collide again.

Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame called back-off time ($T_B$)
WHAT IS BACK OFF TIME ($T_B$) ?

- It is a random value that normally depends on $K$ (the number of attempted unsuccessful transmissions).

- The time-out period is equal to the maximum possible round-trip propagation delay, which is twice the amount of time required to send a frame between the two most widely separated stations ($2 \times T_p$)
In this method, for each retransmission, a multiplier in the range 0 to $2^K - 1$ is randomly chosen and multiplied by $T_p$ (maximum propagation time) or $T_{rr}$ (the average time required to send out a frame) to find $T_B$.

In this procedure, the range of the random numbers increases after each collision.

The value of $K_{max}$ is usually chosen as 15.

Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames.

After a maximum number of retransmission attempts $K_{max}$' a station must give up and try later.
VULNERABLE TIME

- The time, in which there is a possibility of collision.
- We assume that the stations send fixed-length frames with each frame taking $T_{fr}$ sec to send.
**THROUGHPUT**

- The throughput for pure ALOHA is \( S = G \times e^{-2G} \).
  
  where

G the average number of frames generated by the system during one frame transmission time.

if \( G = 1/2 \) (one frame during two frame transmission times)

The maximum throughput \( S_{\text{max}} = 0.184 \) i.e 18.4%
DRAW BACK OF PURE ALOHA

- Pure ALOHA has a vulnerable time of $2 \times T_{fr}$.

- There is no rule that defines when the station can send.

- A station may send soon after another station has started or soon before another station has finished.
SLOTTED ALOHA (NON CARRIER SENSING)

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA.
- In slotted ALOHA, the time is divided into slots of Tfr sec and force the station to send only at the beginning of the time slot.
Assumptions

- All frames have the same size length
- Time is divided into equal size slots (time to transmit 1 frame)
- Nodes start to transmit frames only at the beginning of slots
- All nodes are synchronized
- If 2 or more nodes transmit in a slot, all nodes detect collision
Frames in a Slotted ALOHA Network
• A station is allowed to send only at the beginning of the synchronized time slot
• if a station misses this moment, it must wait until the beginning of the next time slot.
• Of course, there is still the possibility of collision if two stations try to send at the beginning of the same time slot.
• But, the vulnerable time is now reduced equal to $T_{fr}$

• e.i vulnerable time = $T_{fr}$
A collides with C

Begin

B

End

Begin

C

End

\[ t + T_{fr} \]

Vulnerable time = \( T_{fr} \)

Time
THROUGHPUT OF SLOTTED ALOHA

- The throughput for slotted ALOHA is $S = G \times e^{-G}$.

- The maximum throughput $S_{max} = 0.368$ when $G=1$. 
CARRIER SENSE MULTIPLE ACCESS (CSMA)
Invented to minimize collisions and increase the performance
A station “follows” the activity of other stations
Simple rules for a polite human conversation
  - Listen before talking
  - If someone else begins talking at the same time as you, stop talking
CSMA:
  - A node should not send if another node is already sending
    - carrier sensing
CD (collision detection):
  - A node should stop transmission if there is interference
    - collision detection
CSMA

- A node should not send if another node is already sending
  - carrier sensing
CSMA OR PERSISTENCE METHODS

- What should a station do if the channel is busy?
- What should a station do if the channel is idle?
  Three methods have been devised to answer these questions:
  - The 1-persistent method,
  - The non-persistent method,
  - The p-persistent method.
1-Persistent CSMA

• In this method, station that wants to transmit data continuously sense the Channel to check whether the channel is idle or busy.
• If the channel is busy, the station waits until it becomes idle.
• When the station detects an idle channel, it immediately transmits the frame with probability 1.
• Hence it is called 1-persistent CSMA.
DRAW BACK OF I-PERSISTENT

- This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and can transmit their frames.
- When the collision occurs, the stations wait a random amount of time and start all over again.
DRAWBACK OF 1-PERSISTENT

- The propagation delay time greatly affects this protocol.
- Suppose, just after the station 1 begins its transmission, station 2 also become ready to send its data and sense the channel.
- If the station 1 signal has not yet reached station 2, station 2 will sense the channel to be idle and will begin its transmission. This will result in collision.
- Even if propagation delay time is zero, collision will still occur. If two stations become ready in the middle of third station’s transmission both stations will wait until the transmission of first station ends and both will begin their transmission exactly simultaneously. This will also result in collision.
Non-persistent CSMA

- A station that has a frame to send senses the channel.
- If the channel is idle, it senses immediately.
- If the channel is busy, it waits a random amount of time and then senses the channel again.
- In non-persistent CSMA, the station does not continuously sense the channel for the purpose of capturing it.
channel

Wait randomly

idle

Busy

Sense & transmit

Station can transmit

Sense

Sense

Wait (Random time)

wait

Busy channel

time
ADVANTAGES OF NON-PERSISTENT

- It reduces the chances of collision because the stations wait a random amount of time.
- It is unlikely that two or more stations will wait for the same amount of time and will retransmit at the same time.
DISADVANTAGES OF NON-PERSISTENT

- It reduces the efficiency of network because the channel remains idle when there may be stations with frames to send.
- This is due to the fact that the stations wait a random amount of time after the collision.
P-persistent CSMA

- This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.
- Whenever a station becomes ready to send the channel.
- If channel is busy, station waits until next slot.
- If the channel is idle, it transmits with a probability $p$.
- With the probability $q=1-p$, the station then waits for the beginning of the next time slot.
• If the next slot is also idle, it either transmits or wait again with probabilities p and q.

• This process is repeated till either frame has been transmitted or another station has begun transmitting.

• In case of the transmission by another station, the station act as though a collision has occurred and it waits a random amount of time and starts again.
COUNTINUOUSLY SENSES

PROBABILITY OUTCOME DOES NOT ALLOW TRANSMISSION

Time slot

Time slot

Time slot

TRANSMIT

TIME

CHANNEL?

IDLE

BUSY

CHANNEL?

> P

WAIT A SLOT

<= P

PROBABILITY OUTCOME?

STATION CAN START

Acts as though collision has occurred & start again
ADVANTAGES OF P-PERSISTENT

- It reduces the chances of collision and improves the efficiency of the network.
CSMA WITH COLLISION DETECTION (CSMA-CD)

- **Procedure**
  - Listen to medium and wait until it is free
  - Then start talking, but listen if someone else starts talking too
  - If a collision occurs, stop and then start talking after a random back off time

- **Advantages**
  - More efficient than basic CSMA

- **Disadvantages**
  - Requires ability to detect collisions
COLLISION DETECTION PROBLEM

- Transmit signal is MUCH stronger than received signal
- Due to high path loss in the wireless environment (up to 100dB)
- Impossible to “listen” while transmitting because you will drown out anything you hear
NEED FOR SPECIAL MAC PROTOCOLS

- The popular CSMA/CA and its variation such as CSMA/CD, developed for wired networks, cannot be used directly in the wireless networks because of Hidden and Exposed terminals.
So it is interesting to know...

What is Hidden and Exposed terminal problem?
HOW TO SOLVE HIDDEN & EXPOSED TERMINAL PROBLEMS?
The answer lies under the protocol reservation/collision resolution.
RESERVATION/COLLISION RESOLUTION

Random Access

Noncarrier Sensing (ALOHA, Slotted ALOHA)

Carrier Sensing (CSMA)

Reservation/Collision Resolution

Use of Control Packet (MACA, MACAW)

Use of Control Packets and Carrier Sensing (FAMA, CSMA/CA, IEEE802.11)
RESERVATION/COLLISION RESOLUTION PROTOCOL

- To solve the hidden and exposed-terminal problems
- Some schemes are contention-based and involve some forms of dynamic reservation and collision resolution
- Some schemes use the RTS/CTS control packets to prevent collisions e.g. Multiple Access Collision Avoidance (MACA) and MACA for wireless LANs (MACAW).
**Hidden Terminal Problem**

- Node B is in the range of node A and C both
- A and C are not in the range of each other
- When A transmits to B, C cannot detect the transmission using the *carrier sense* mechanism
- If C is also transmits to B, collision will occur at B
EXPOSED TERMINAL PROBLEM

- Node C is the range of B and D both
- Node B can communicate with A and C
- Node A cannot hear C
- Node D can not hear B
- When C transmits to D, B detect the transmission using the *carrier sense* mechanism and postpone to transmit to A, even though such transmission will not cause collision
A and D transmit simultaneously to B, the signal strength received by B from D is much higher than that from A, and D’s transmission can be decoded without errors. This will result unfair sharing of bandwidth.
MACA: Multiple Access Collision Avoidance (MACA) - A New Channel Access Method for Packet Radio
MACA

- Proposed as an alternative to the traditional CSMA
- CSMA senses the state of the channel only at the transmitter
  - Leads to hidden node problem
- Does not use carrier sensing
  - Nodes start transmitting after a random backoff
- MACA uses RTS and CTS to overcome hidden node problem and exposed node problem
  - Node which only hears CTS (but no RTS), stops from transmitting (hidden node)
  - Node which only hears RTS (but no CTS), is free to transmit (exposed node)
  - RTS and CTS carry the expected duration of data transmission
- When there is a collision, it uses binary exponential backoff (BEB) before retrying
Goals, New Ideas, and Main Contributions

- **Goals:**
  - Try to overcome hidden & exposed terminal problems

- **New idea:**
  - Reserve the channel before sending data packet
  - Minimize the cost of collision (control packet is much smaller than data packet)

- **Main Contribution:**
  - A three-way handshake MAC protocol: MACA
**FUNDAMENTAL ASSUMPTIONS**

- **Symmetry**
  - $A$ can hear from $B \Leftrightarrow B$ can hear from $A$

- No capture

- No channel fading

- Packet error only due to collision

- Data packets and control packets are transmitted in the same channel
**THREE-WAY HANDSHAKE**

- **A** sends Ready-to-Send (RTS)
- **B** responds with Clear-to-Send (CTS)
- **A** sends DATA PACKET
- RTS and CTS announce the duration of the data transfer
- Nodes overhearing RTS keep quiet for some time to allow **A** to receive CTS
- Nodes overhearing CTS keep quiet for some time to allow **B** to receive data packet
THREE-WAY HANDSHAKE

Diagram showing a network with nodes A, B, C, D, and E, with packets RTS (10) and CTS (10) exchanged.
DETAILS OF MACA

- **A** sends out RTS and set a timer and waits for CTS
  - If **A** receives CTS before timer go to zero, OK! sends data packet
  - Otherwise, **A** assumes there is a collision at **B**
    - Double the backoff counter interval
      - Randomly pick up a timer from backoff counter]
    - Send next RTS after timer go to zero

- **B** sends out CTS, then set a timer and waits for data packet
  - If data packet arrives before timer go to zero, OK!
  - Otherwise, **B** can do other things
**DETAILS OF MACA**

- C overhears A’s RTS, set a timer which is long enough to allow A to receive CTS. After the timer goes to zero, C can do other things.
- D overhears B’s CTS, set a timer which is long enough to allow B to receive data packet.
- E overhears A’s RTS and B’s CTS, set a timer which is long enough to allow B to receive data packet.
- RTS and CTS can also contain info to allow sender A to adjust power to reduce interference.

*Note: no carrier sense*
Hidden Terminal Problem Still Exists

- Data packet still might suffer collision
Exposed Terminal Problem Still Exists

- Node C cannot receive CTS
Note: In fact, when hidden terminals are present and the network traffic is high, the performance of MACA degenerates to that of ALOHA.
### Drawbacks of MACA

- MACA did not solve hidden & exposed terminal problems
- MACA did not provide any information about parameters e.g.
  - Size of RTS, CTS packet?
  - How to decide timers?
  - Initial back off window size?
MACAW: A Media Access Protocol for Wireless Lan
GOALS, NEW IDEAS, AND MAIN CONTRIBUTIONS

Goals:

- To extend MACA
  - Concept: Information sharing to achieve fairness
    - Modified control messages
      - Four-way handshake (reliable, recover at MAC layer)
      - Five-way handshake (relieve exposed terminal problem)
      - RRTS (unfairness)
    - Modified back-off algorithms
REVISIT HIDDEN TERMINAL PROBLEM

- Data packet still may suffer collision
- Recovery of packet loss at transport layer is too slow
- So it is better to recover that packet at MAC layer which is more fast
- For this, there is a need of ACK from destination
FOUR-WAY HANDSHAKE

- Sender sends Ready-to-Send (RTS)
- Receiver responds with Clear-to-Send (CTS)
- Sender sends DATA PACKET
- Receiver acknowledge with ACK
- RTS and CTS announce the duration of the transfer
- Nodes overhearing RTS/CTS keep quiet for that duration
- Sender will retransmit RTS if no ACK is received
- If ACK is sent out, but not received by sender, after receiving new RTS, receiver returns ACK instead of CTS for new RTS
FOUR-WAY HANDSHAKE

source -> RTS(T) -> destination

destination -> CTS(T) -> source
**Revisit Exposed Terminal Problem**

- RTS/CTS/DATA/ACK can not solve exposed terminal problem
- When overhearing RTS, the node needs to wait longer enough to allow the data packet being completely transmitted even it does not overhear CTS.
- To relieve exposed terminal problem,
  - Let exposed terminal know the DATA packet does be transmitted
  - Extra message DS (data send)
- Five Handshaking to let exposed terminal know how long it should wait
FIVE-WAY HANDSHAKE

- Sender sends Ready-to-Send (RTS)
- Receiver responds with Clear-to-Send (CTS)
- Sender sends DATA SENDING (DS)
- Sender sends DATA PACKET
- Receiver acknowledge with ACK
- RTS and CTS announce the duration of the transfer
- Nodes overhearing RTS/CTS keep quiet for that duration
FIVE-WAY HANDSHAKE
UNFAIRNESS

- Using *RTS/CTS/DATA/ACK* or *RTS/CTS/DS/DATA/ACK* might cause unfairness
- A sends data to B; D sends data to C
- A and D have enough data to send
- C can hears from B and D, but not A
- B can hear from A and C, but not D
  - A is in luck and gets the channel
  - D sends RTS and times out
  - Back off window for D repeatedly doubles
- For the next transmission, A picks a random number from a smaller window
  - Unequal probability of channel access
  - Throughput for flow A ➔ B > 90%
  - Throughput for flow D ➔ C ~ 0%
Unfairness
REQUEST FOR RTS (RRTS)

- Try to solve unfairness by having C do the contending for D
WHY USES RRTS INSTEAD OF CTS?

- CTS or RTS packet size << data packet size

- When nodes overhear CTS, they need to defer a time period to allow the expected data packet transmission.

- When nodes overhear RRTS, they only need to defer a time period to overhear the expected CTS.

- Uses CTS will cost long waiting.
Information Sharing in Backoff Algorithms

- When a node sends a packet, it embeds its current back-off counter in the packet header.
- Other nodes which overhears the packet copy the value as itself back off counter.
- Key idea: all nodes have the same backoff counter to achieve fairness.
Floor acquisition Multiple Access (FAMA) Protocols
- FAMA is another MACA based scheme
- It requires every transmitting station to acquire control of the floor (i.e., the wireless channel) before it actually sends any data packet.
- FAMA has two phases
  - Acquiring channel
  - Actual transmission of data
- Unlike MACA or MACAW, FAMA requires that collision avoidance should be performed both at the sender as well as the receiver.
In order to acquire the floor, the sending node sends out an RTS.

The receiver responds with a CTS packet, which contains the address of the sending node.

Any station overhearing this CTS packet knows about the station that has acquired the floor.

The CTS packets are repeated long enough for the benefit of any hidden sender that did not register another sending node's RTS.
RESERVATION/COLLISION RESOLUTION

Random Access

Noncarrier Sensing (ALOHA, Slotted ALOHA)

Carrier Sensing (CSMA)

Reservation/Collision Resolution

Use of Control Packet (MACA, MACAW)

Use of Control Packets and Carrier Sensing (FAMA, CSMA/CA, IEEE802.11)
The IEEE 802.11 MAC
The IEEE 802.11 standard specifies for the MAC layer and the Physical Layer.

Physical layers offers

- FHSS
- DSSS
- Infrared (IF)

The MAC layer offers two modes of protocols:

- A contention-free service implemented by the PCF
- A contention-free service implemented by the DCF
DISTRIBUTED COORDINATION FUNCTION (DCF)

- The IEEE 802.11 WLAN standard adopts a dynamic channel allocation scheme based on carrier sensing technique, called DCF.
- It supports best effort delivery of packets at the data link layer.
- It is based on CSMA/CA protocol, which can be seen as a combination of the CSMA and MACA schemes.
IEEE 802.11 defines physical and virtual carrier sensing mechanisms to avoid interference for the kind of interference originating from within the receiving range of a receiver.

However, in wireless ad hoc networks most interference comes from outside of this range.
- Carrier sensing range (Rc) is the range within which stations can sense transmitted power.

- **Physical carrier sensing**: Detects presence of other stations by analyzing all detected packets
  - Detects activity in the channel via relative signal strength from other sources

- **Virtual carrier sensing** is done by sending MPDU duration information in the header of RTS/CTS and data frames

- Channel is busy if **either** mechanisms exist
Collisions from the nodes hidden in the vulnerable region can be effectively avoided by four-way handshake based on RTS and CTS packets.
Node $N_R$ may be initiate its transmission because it is hidden for $S$. 

$N_R$ would collide with $S$’s Tx at $R$. 

**VULNERABLE REGION IN CSMA**
**Busy Tone Multiple Access Protocols (BTMA)**

- BTMA is used to avoid the hidden terminal problem.
- Whenever any node detects a packet being transmitted, it starts to send a signal, called a busy tone, in a separate frequency channel.
- For example, when node S starts to send a packet to node R, node R as well as node $N_S$ will start to send a busy tone.
- All the nodes that can hear the busy tone will not initiate their own transmission and thus node R will experience no collision.
IS BUSY TONE SCHEME EFFECTIVE?

- BTMA has a critical problem.
- Use of busy tones prohibit many nodes (all 2-hop neighbors of node S) to transmit.
- The number of nodes affected may be about four times the number of nodes within the transmission range of the receiver.
- This approach almost completely eliminates collisions but it is not a very promising approach from a throughput standpoint.
Dual Busy Tone Multiple Access Protocol (DBTMAP)
It is extension of BTMAP.

In the DBTMA protocol, two narrow-bandwidth tones are implemented on shared channel.
- The transmit busy tone
- The receive busy tone

Indicate whether the node is transmitting RTS packets or receiving data packets, respectively.

All nodes sensing any busy tone are not allowed to send RTS requests.

Any node sending the RTS packet is required to abort such transmission immediately.

Indeed, the RTS packets and the receive busy tone solve the hidden- and the exposed-terminal problems.
The transmit busy tone provides protection for the RTS packets to increase the probability of successful RTS reception at the intended receiver.

The receive busy tone provides acknowledge the RTS packet and provide continuous protection for the transmitted data packets.
IS DBTMA EFFECTIVE?

- BTMA and DBTMA are proposed to be used in a network with a base station and the scheme uses the busy tone in a centralized manner.
- Although the protocol could be used in ad hoc networks with distributed control.
- Moreover, the performance of the scheme has not been investigated in such networks.
DISTRIBUTED COORDINATION FUNCTION (DCF)

- DCF is the fundamental MAC technique of the IEEE 802.11 based WLAN standard to share the medium between multiple stations.
- DCF employs a CSMA/CA with binary exponential backoff algorithm.
- This is based on four way handshake scheme i.e. RTS/CTS WITH NAV, DATA, ACK,
ACK, RTS/CTS WITH NAV, IFS AND BACK OFF ALGORITHM WITH CW

?
ACK (Acknowledgement)

- ACK is used for collision detection.
- Let the node know whether its transmission was successful.
- If no ACK packet is received or an ACK is received in error, the sender will contend again for the medium to retransmit the data packet.
- If all fails, the sender drops the packet consequently leaving it to a higher level reliability protocol.
**RTS/CTS with NAV Between Sender and Receiver**

- It is used for solving hidden terminal problem.
- All neighboring nodes recognize the transmission and back off during the transmission time advertised along with the RTS and CTS packets, and set their NAV.
**What is NAV(Network Allocation Vector)?**

- The NAV contains a time value that represents the duration up to which the medium is expected to be busy because of transmissions.
- Every node overhearing a packet continuously updates its own NAV.
RTS/CTS AND NAV
DC FRAME SPACING

- A node must sense the status of the wireless medium before transmitting.
- If it finds that the medium is continuously idle for **DCF Inter frame Space** (DIFS) duration, it is then permitted to transmit a frame.
- If the channel is found busy during the DIFS interval, the station should defer its transmission.
- RTS packet can be transmitted after waiting for DIFS duration of time.
- DIFS duration can be calculated by the following method.

\[ \text{DIFS} = \text{SIFS} + (2 \times \text{Slot time}) \]
INTER FRAME SPACING (IFS)

- The time interval during which each node has to wait before transmitting any packet.
- IFS is used to provide a priority to access the channel.
- **Short IFS (SIFS)**: Frames (CTS, DATA, and ACK) use SIFS before attempting to transmit.
BACK OFF ALGORITHM
BACK OFF ALGORITHM WITH CW

- Provide fair access with congestion control
- The main purpose of the back-off algorithm is to reduce the probability of collisions when contention is severe.
**HOW IT AVOID COLLISION?**

- After waiting for the DIFS duration, each competing node waits for a back off time, which is randomly chosen in the interval (0, CW)
- During the first transmission of a packet, CW is set to its minimum preset value, CWmin.
- If the channel continues to be idle during the back-off time, it transmits (winner).
- Other waiting nodes become aware of the transmission,
- Freeze their back off time, contend again in the next competition cycle after the current transmission completes
The frozen back-off time plays an important role in ensuring fairness.
HOW IT SUPPORT TO FAIRNESS?

- All nodes entering the competition for the first time should have an equal chance of transmitting.
- But nodes that have lost in the previous competition should have higher priority than newly arrived nodes.
- So the losers are given a higher priority by using the remaining frozen back off time.
- Thereby preserving the first-come, first-serve policy.
FLOW DIAGRAM OF BACK-OFF ALGORITHM USED IN DCF

Data Ready

 CW = CW_{min}

 Medium idle

 Wait for IFS duration

 CW = CW \times 2 \text{ if } CW \text{ is not } CW_{max}

 Maximum retransmissions reached

 Transmit frame

 Wait for ACK or ACK timeout

 ACK timeout

 ACK received

 Drop packet

 Wait until current transmission ends

 Wait for IFS duration

 Still idle

 Still idle

 Choose backoff time between (0, CW-1) and wait. (Use frozen backoff time if it exists)

 Backoff time expired

 Medium busy (Freeze backoff time)

 Done
**DRAWBACK OF BACK OFF ALGORITHM WITH CW?**

- DCF has problems under heavy or light loads.
- If CW is too small compared to the number of competing nodes, it causes many collisions.
- On the other hand, if CW is too large, it causes unnecessary delay.
- Generally size of CW vary 0-31.
SOLUTION IS BINARY EXPONENTIAL ALGORITHM ....?
DCF adopts the binary exponential back-off scheme to allow an adaptive solution to this problem.
EXTENDED INTERFRAME SPACING (EIFS)
When a node fails to receive an ACK in response to transmission of a DATA packet, it needs to contend in the next competition cycle.

However, CW is doubled after the collision and this continues until CW reaches a preset limit, CW max.
IS FOUR-WAY HANDSHAKE EFFECTIVELY ELIMINATES THE VULNERABLE REGION/ COLLISION?
Yes, the RTS/CTS mechanism together with NAV effectively eliminates the vulnerable region.
But …

some packets are still vulnerable to collisions
Which packets...?
- Coverage area of a transmitter depends on the power of the transmitted signal and the path loss.

- Each receiver has particular power sensitivity; e.g., it can only detect and decode signals with strength larger than this sensitivity.

- There are two threshold values when receiving radio signals
  - Receive threshold (RX Thresh)
  - Carrier sense threshold (CS Thresh).
If the power of the received signal is higher than RX thresh, it is regarded as a valid packet and passed up to the MAC layer.

The distance for two nodes to communicate successfully is called the transmission range.

If the received signal power is lower than CS Thresh, it is discarded as noise and thus the node can start its own transmission or reception.

If the signal power is in between RX Thresh and CS thresh, the node cannot receive the packet intelligibly but acknowledges that some active transmission is going on.

The corresponding distance is referred to as interference range.
Vulnerable region with considering the interference range

Interference range (node S)  Interference range (node R)

Transmission range (node S)  Transmission range (node R)

Group III  Group II  Group IV

ACK from R is vulnerable to collisions at S. (It is removed by using EIFS.)

Data (as well as RTS) from S is vulnerable to collisions at R.
- **Group I**: A node is within the transmission range of S or R. It can receive RTS or CTS and sets its NAV accordingly.
- **Group II**: A node is outside of transmission range of S and R but is within the interference range of S and R. It cannot receive packets intelligently but recognizes the ongoing communication.
- **Group III**: A node is outside of interference range of R but is within the interference range of S. It cannot sense CTS and ACK transmission from R.
- **Group IV**: A node is outside of interference range of S but is within the interference range of R. It cannot sense data packet transmission from S.
Nodes in Group I correctly set their NAVs when receiving RTS/CTS, and defer their transmission until the S-R communication is finished.

Nodes in Group II cannot decode the packets and do not know the duration of the packet transmission, but they do sense on-going communications and thus do not cause collisions.

However, in Group III and IV, respectively, ACKs (from R to S) and DATA (from S to R) are vulnerable to collisions.
BOTTLENECK OF FOUR-WAY HANDSHAKE

- Collisions may be critical for any type of packets
- But **ACK** collisions is a more serious problem.
Why
ACK COLLISION IS SO SERIOUS?
An ACK packet is a vital piece of information as the last step of the four-way handshake.

A loss of ACK results in retransmission of long DATA packet

Thus significantly degrades the performance of N/W.
ANY SOLUTION TO THIS SERIOUS PROBLEM?
YES ...! ITS EXTENDED IFS (EIFS)
EIFS is used in DCF to prevent collisions with ACK receptions at the sender.
How...?
When nodes detect a transmission but cannot decode it, they set their NAVs for the EIFS duration.

In Figure, when S completes its data transmission at $T_C$, nodes in Group II and III would set their NAV to $T_C + EIFS$.

At $T_C + SIFS + t$, R replies back to S with an ACK and the transmission is completed at $TC + SIFS + 2t + ACKt$,
- where $t$ is the propagation delay of the channel and $ACKt$ is the transmission time for the ACK packet.

If EIFS is larger than $SIFS + 2t + ACKt$, nodes in Group II and III would not corrupt the ACK packet from R to S.

These nodes have to wait an additional DIFS to start the competition, thus EIFS is set to $SIFS + ACKt + DIFS$ in the IEEE 802.11 MAC standard.
when node S transmits a data packet to node R, four different groups of nodes in the network came into existence as shown in Figure.
## Radio Transceiver Characteristics and Key Elements of DCF

<table>
<thead>
<tr>
<th>Key elements</th>
<th>Parameters</th>
<th>Typical values</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Radio transceiver</strong></td>
<td>Transmission power</td>
<td>0.2818 W</td>
<td>Transmission range 250m (with two-ray ground model)</td>
</tr>
<tr>
<td></td>
<td>RxThresh</td>
<td>$3.652 \times 10^{-10}$ W</td>
<td>Interference range 550m (with two-ray ground model)</td>
</tr>
<tr>
<td></td>
<td>CSThresh</td>
<td>$1.559 \times 10^{-11}$ W</td>
<td></td>
</tr>
<tr>
<td><strong>ACK</strong></td>
<td>ACK frame size</td>
<td>376 μsec</td>
<td>184-bit ACK packet with 144 and 48 bits of physical layer preamble and header over 1Mbps link</td>
</tr>
<tr>
<td></td>
<td>RTS frame size</td>
<td>424 μsec</td>
<td>232-bit RTS packet with 144 and 48 bits of physical layer preamble and header over 1Mbps link</td>
</tr>
<tr>
<td></td>
<td>CTS frame size</td>
<td>376 μsec</td>
<td>184-bit CTS packet with 144 and 48 bits of physical layer preamble and header over 1Mbps link</td>
</tr>
<tr>
<td></td>
<td>RTSThreshold</td>
<td>Not specified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Retry limit for a long packet</td>
<td>4</td>
<td>For DATA packet longer than RTSThreshold</td>
</tr>
<tr>
<td></td>
<td>Retry limit for a short packet</td>
<td>7</td>
<td>For RTS and shorter DATA packet</td>
</tr>
<tr>
<td><strong>IFS</strong></td>
<td>SIFS (Short IFS)</td>
<td>10 μsec</td>
<td>For CTS, DATA and ACK packet</td>
</tr>
<tr>
<td></td>
<td>DIFS (DCF IFS)</td>
<td>50 μsec</td>
<td>For RTS and short DATA packet</td>
</tr>
<tr>
<td></td>
<td>EIFS (Extended IFS)</td>
<td>436 μsec</td>
<td>SIFS (10) + ACKt (376) + DIFS (50)</td>
</tr>
<tr>
<td><strong>Backoff algorithm</strong></td>
<td>Slot time</td>
<td>20 μsec</td>
<td>Equivalent to 640 μsec</td>
</tr>
<tr>
<td></td>
<td>CWmin</td>
<td>32</td>
<td>Equivalent to 20.48 msec</td>
</tr>
<tr>
<td></td>
<td>CWmax</td>
<td>1024</td>
<td></td>
</tr>
</tbody>
</table>
Good Morning...
PERFORMANCE LIMIT OF DCF ?
There has been active research on estimating the performance of IEEE 802.11 MAC, analytically as well as via simulation. According to the results, the theoretical throughput is around 80% when the typical DCF parameters are used. In reality, DCF operates far from the theoretical limits due to collisions and control overhead associated with RTS/CTS and the backoff algorithm. In MANET, the situation becomes worse due to the many reasons which have been discussed.
Li et al. showed that the end-to-end throughput is at most 1/4 of the channel bandwidth even without any other interfering nodes.

In other words, when IEEE 802.11-based 2 Mbps wireless network interface is used, a source-destination pair in a MANET cannot support more than 500 kbps.

This is mainly due to collisions among intermediate nodes of the same data stream.

In addition, the control overhead of DCF aggravates the situation and the maximum throughput is reduced to about 1/7 of the channel bandwidth.

When other data traffic exists, the throughput is reduced even further.
ENHANCING PERFORMANCE OF DCF
ENHANCING TEMPORAL CHANNEL UTILIZATION

- The performance limitation is mainly due to the limited capability of MAC protocols in a multi hop environment.
- A key idea for improving DCF for MANET is adaptivity, i.e., each node should be able to behave adaptively according to traffic intensity in its vicinity.
- To enhance the effective channel utilization by reconsidering the DCF parameters such as
  - RTS Threshold
  - The backoff algorithm
The parameter RTS Threshold is used to determine whether RTS/CTS is used or not.

However, this parameter is not fixed in the DCF standard as discussed previously.

Khurana et al. studied the throughput of an IEEE 802.11-based ad hoc network to obtain the optimal parameters for DCF including the RTS Threshold.

Assuming that the physical layer uses DSSS and DCF uses typical parameters, they recommend a value of 250 bytes for the RTS Threshold.

In other words, the RTS/CTS exchange is beneficial only when data packet size is larger than 250 bytes.
Weinmiller et al. performed a similar study and concluded via simulation that the best throughput is obtained when 200-500 bytes is used for the RTS Threshold.

A better idea is to adjust the parameter depending on the traffic and the collision probability.

Even if data packet size is large, the RTS/CTS exchange is a waste of bandwidth if the number of hidden terminals is small and collisions are unlikely.

Therefore, the optimal value for RTS Threshold depends on the traffic intensity, which can be estimated indirectly by noting the number of collisions experienced.
EXPONENTIAL BACKOFF ALGORITHM

- The contention window is reduced to CW min for every new packet whether the last packet was successfully delivered or not.
- If the network area is congested with many competing data streams, each packet transmission starts with the CW min and thus experiences a large number of collisions before its window size becomes appropriate.
- In addition, restoration of CW to CW min makes the backoff algorithm unfair since it favors the mobile node that has most recently transmitted.
Unfairness problem in DCF due to backoff algorithm

(a) The first competition cycle
(Node A, having chosen a smaller backoff time, wins.)

(b) The second competition cycle
(Node A, having CWmin, wins again.)
- In figure node A wins in the first competition cycle because it chooses the smaller backoff time than node B and C.
- While node A restores its CW to CWmin in the next competition cycle, nodes B and C, being losers, keep the same CW.
- Nodes B and C reduce their backoff time by using the frozen values (BOFFB-BOFFA and BOFFC-BOFFA, respectively).
- Even Though node A has a better chance of winning in the next competition cycle again due to the reduced CW size.
SOLUTION OF THE PROBLEM

- In order to solve the collision and fairness problem, Bharghavan et al. proposed a Multiplicative Increase and Linear Decrease (MILD) algorithm
MULTIPlicative INCREASE AND LINEAR DECREASE (MILD) ALGORITHM

- In MILD Algorithm the contention window size increases multiplicatively on collisions but decreases linearly on successful transmission.

- MILD algorithm works well when the network traffic is high, but under light traffic condition, it incurs additional delay to return the CW to CWmin, which is not required in the original backoff algorithm.
Cali et al. observed that the collision probability increases as the number of active nodes increases.

Due to the static backoff algorithm of DCF, it cannot be dynamically controlled.
The optimal setting of CW, and thus the optimal backoff time, can be achieved by estimating the number of active nodes in its vicinity at run time.

Since each node can estimate the number of empty slots in a virtual transmission time by observing the channel status, the number of active nodes can be computed and exploited to select the appropriate CW without paying the collision costs.
ENHANCING SPATIAL CHANNEL UTILIZATION

- MAC protocols that better utilize the channel along the spatial dimension
- we have many types of scheme for this.
ASSIGNMENT

- What is MAC protocol?
- What is the need of MAC Protocol?
- Various challenges of MAC Protocol?
- What are various goals of MAC protocol design?
- Explain classification of MAC protocol?
IEEE802.11 MAC FRAME FORMAT

The MAC frame format comprises a set of fields that occur in a fixed order in all frames.
The first three fields (Frame Control, Duration/ID, and Address 1) and the last field (FCS) in above Figure constitute the minimal frame format and are present in all frames, including reserved types and subtypes.

The fields Address 2, Address 3, Sequence Control, Address 4, QoS Control, HT Control, and Frame Body are present only in certain frame types and subtypes.
The Frame Control field consists of the following subfields:
**TYPE AND SUBTYPE FIELDS**

The Type field is 2 bits in length, and the Subtype field is 4 bits in length. The Type and Subtype fields together identify the function of the frame. There are three frame types:

- control,
- data,
- management.

Each of the frame types have several defined subtypes.
To DS field
- The To DS field is 1 bit in length and is set to 1 in data type frames destined for the DS.
- This includes all data type frames sent by STAs associated with an AP.
- The To DS field is set to 0 in all other frames.

From DS field
- The From DS field is 1 bit in length and is set to 1 in data type frames exiting the DS.
- It is set to 0 in all other frames.
MORE FRAGMENTS FIELD

- The More Fragments field is 1 bit in length and is set to 1 in all data or management type frames that have another fragment of the current MSDU or current MMPDU to follow.
- It is set to 0 in all other frames.
**Retry Field**

- The Retry field is 1 bit in length and is set to 1 in any data or management type frame that is a retransmission of an earlier frame.
- It is set to 0 in all other frames.
- A receiving station uses this indication to aid in the process of eliminating duplicate frames.
**POWER MANAGEMENT FIELD**

- The Power Management field is 1 bit in length and is used to indicate the power management mode of a STA.
- The value of this field remains constant in each frame from a particular STA within a frame exchange sequence.
- The value indicates the mode in which the station will be after the successful completion of the frame exchange sequence.
- A value of 1 indicates that the STA will be in power-save mode.
- A value of 0 indicates that the STA will be in active mode.
- This field is always set to 0 in frames transmitted by an AP.
MORE DATA FIELD

- The More Data field is 1 bit in length and is used to indicate to a STA in power-save mode that more MSDUs, or MMPDUs are buffered for that STA at the AP.
- The More Data field is valid in directed data or management type frames transmitted by an AP to an STA in power-save mode.
- A value of 1 indicates that at least one additional buffered MSDU, or MMPDU, is present for the same STA.
- The More Data field may be set to 1 in directed data type frames transmitted by a contention-free (CF)-Pollable STA to the point coordinator (PC) in response to a CF-Poll to indicate that the STA has at least one additional buffered MSDU available for transmission in response to a subsequent CF-Poll.
- The More Data field is set to 0 in all other directed frames.
The WEP field is 1 bit in length.

It is set to 1 if the Frame Body field contains information that has been processed by the WEP algorithm.

The WEP field is only set to 1 within frames of type Data and frames of type Management, subtype Authentication.

The WEP field is set to 0 in all other frames.

When the WEP bit is set to 1,
Reservation Time Division Multiple Access

- every frame consists of $N$ mini-slots and $x$ data-slots
- every station has its own mini-slot and can reserve up to $k$ data-slots using this mini-slot (i.e. $x = N \times k$).
- other stations can send data in unused data-slots according to a round-robin sending scheme (best-effort traffic)

![Diagram showing TDMA reservations and data slots](image)
DISTRIBUTED PACKET RESERVATION MULTIPLE ACCESS PROTOCOL (D-PRMA)

- Implicit reservation (PRMA - Packet Reservation Multiple Access):
  - a certain number of slots form a frame, frames are repeated
  - stations compete for empty slots according to the slotted aloha principle
  - once a station reserves a slot successfully, this slot is automatically assigned to this station in all following frames as long as the station has data to send
  - competition for this slots starts again as soon as the slot was empty in the last frame
CONTENTION-BASED PROTOCOLS WITH RESERVATION MECHANISMS

Collision avoidance time allocation protocol (CATA)

- 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.
Hop reservation multiple access protocol (HRMA)
- a multichannel MAC protocol which is based on half-duplex, very slow frequency-hopping spread spectrum (FHSS) radios
- uses a reservation and handshake mechanism to enable a pair of communicating nodes to reserve a frequency hop, thereby guaranteeing collision-free data transmission.
- can be viewed as a time slot reservation protocol where each time slot is assigned a separate frequency channel.

Soft reservation multiple access with priority assignment (SRMA/PA)
- Developed with the main objective of supporting integrated services of real-time and non-real-time application in ad hoc networks, at the same time maximizing the statistical multiplexing gain.
- Nodes use a collision-avoidance handshake mechanism and a soft reservation mechanism.
Five-Phase Reservation Protocol (FPRP)
- a single-channel time division multiple access (TDMA)-based broadcast scheduling protocol.
- Nodes uses a contention mechanism in order to acquire time slots.
- The protocol assumes the availability of global time at all nodes.
- The reservation takes five phases: reservation, collision report, reservation confirmation, reservation acknowledgement, and packing and elimination phase.

MACA with Piggy-Backed Reservation (MACA/PR)
- 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
Real-Time Medium Access Control Protocol (RTMAC)

- Provides a bandwidth reservation mechanism for supporting real-time traffic in ad hoc wireless networks
- RTMAC has two components
  - A MAC layer protocol is a real-time extension of the IEEE 802.11 DCF.
    - A medium-access protocol for best-effort traffic
    - A reservation protocol for real-time traffic
  - A QoS routing protocol is responsible for end-to-end reservation and release of bandwidth resources.
Protocols in this category focus on packet scheduling at the nodes and transmission scheduling of the nodes.

The factors that affects scheduling decisions
- Delay targets of packets
- Traffic load at nodes
- Battery power

Distributed priority scheduling and medium access in Ad Hoc Networks present two mechanisms for providing quality of service (QoS)
- Distributed priority scheduling (DPS) – piggy-backs the priority tag of a node’s current and head-of-line packets o the control and data packets
- Multi-hop coordination – extends the DPS scheme to carry out scheduling over multi-hop paths.
Distributed Wireless Ordering Protocol (DWOP)
- A media access scheme along with a scheduling mechanism
- Based on the distributed priority scheduling scheme

Distributed Laxity-based Priority Scheduling (DLPS) Scheme
- Scheduling decisions are made based on
- The states of neighboring nodes and feedback from destination nodes regarding packet losses
- Packets are recorded based on their uniform laxity budgets (ULBs) and the packet delivery ratios of the flows. The laxity of a packet is the time remaining before its deadline.
MAC protocols that use directional antennas have several advantages:
  - Reduce signal interference
  - Increase in the system throughput
  - Improved channel reuse

MAC protocol using directional antennas
  - Make use of an RTS/CTS exchange mechanism
  - Use directional antennas for transmitting and receiving data packets

Directional Busy Tone-based MAC Protocol (DBTMA)
  - It uses directional antennas for transmitting the RTS, CTS, data frames, and the busy tones.

Directional MAC Protocols for Ad Hoc Wireless Networks
  - DMAC-1, a directional antenna is used for transmitting RTS packets and omni-directional antenna for CTS packets.
  - DMAC-1, both directional RTS and omni-directional RTS transmission are used.