BASIC ARCHITECTURAL FRAMEWORK

MAC LAYER (Medium Access Control)

OUTLINES

- Overview
- Wireless MAC protocols
  - Carrier Sense Multiple Access
  - Multiple Access with Collision Avoidance (MACA) and MACAW
  - MACA By Invitation
  - IEEE 802.11
  - IEEE 802.15.4 and ZigBee
- Characteristics of MAC Protocols in Sensor Networks
  - Energy Efficiency
  - Scalability
  - Adaptability
  - Low Latency and Predictability
  - Reliability
- Contention-Free MAC Protocols
- Contention-Based MAC Protocols
- Hybrid MAC Protocols

MAC LAYER

- In most networks, multiple nodes share a communication medium for transmitting their data packets
- The medium access control (MAC) protocol is primarily responsible for regulating access to the shared medium
- The choice of MAC protocol has a direct bearing on the reliability and efficiency of network transmissions
  - due to errors and interferences in wireless communications and to other challenges
- Energy efficiency also affects the design of the MAC protocol
  - trade energy efficiency for increased latency or a reduction in throughput or fairness

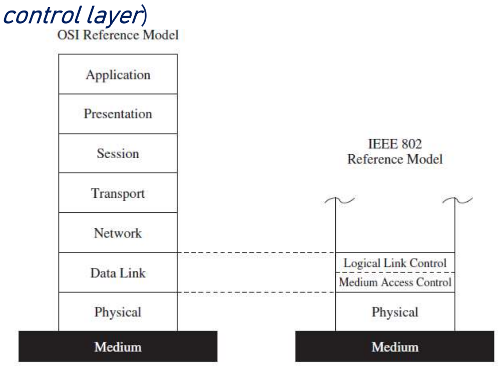
MAC LAYER

FUNCTIONS

- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- It also performs collision resolution and initiating retransmission in case of collisions.
- Framing: It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- Addressing: It resolves the addressing of source station as well as the destination station, or groups of destination stations.
- Flow Control: It generates the frame check sequences and thus contributes to protection against transmission errors.

MAC LAYER

- *Responsibilities* of MAC layer include:
  - ❑ Decide when a node accesses a shared medium
  - ❑ Resolve any potential conflicts between competing nodes like Collision Resolution and Retransmission of frames in case of collision
  - ❑ Correct communication errors occurring at the physical layer
  - ❑ Perform other activities such as framing, addressing, and flow control
- Second layer of the OSI reference model (data link layer) or the IEEE 802 reference model (which divides data link layer into *logical link control* and *medium access control layer*)



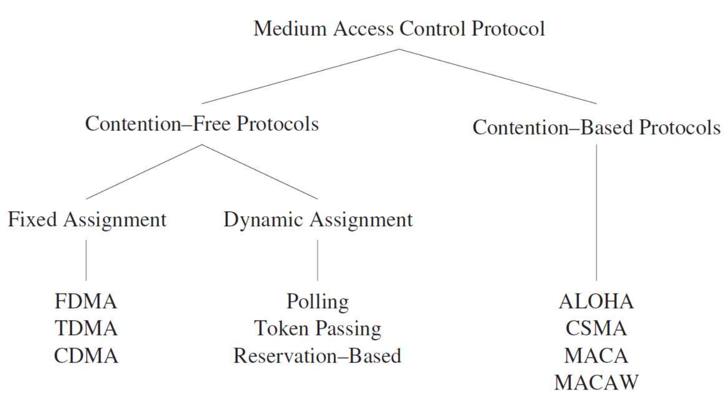
The MAC layer in the IEEE 802 reference model.

MAC LAYER

Most MAC protocols fall either into the categories of *contention-free* or *contention-based* protocols.

Contention-free Protocols:

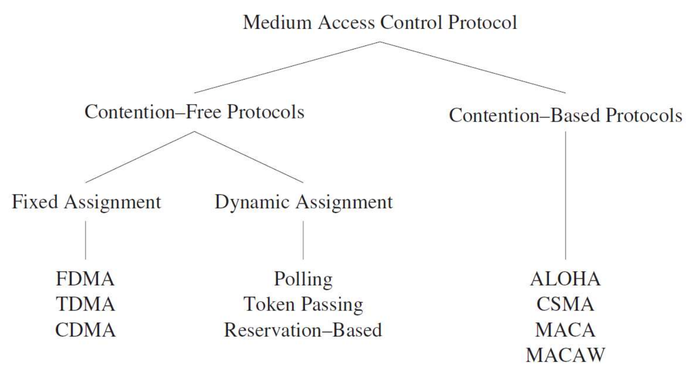
- In the first category, MAC protocols provide a medium sharing approach that ensures that only one device accesses the wireless medium at any given time.
- This category can further be divided into *fixed* and *dynamic* assignment classes, indicating whether the slot reservations are fixed or on demand.



MAC LAYER

Contention-based protocols allow nodes to access the medium simultaneously, but provide mechanisms to reduce the number of collisions and to recover from such collisions.

Finally, some MAC protocols do not easily fit into this classification since they share characteristics of both contention-free and contention-based techniques. These ***hybrid* approaches** often aim to inherit the advantages of these main categories, while minimizing their weaknesses.



MAC LAYER – CONTENTION-FREE MEDIUM ACCESS

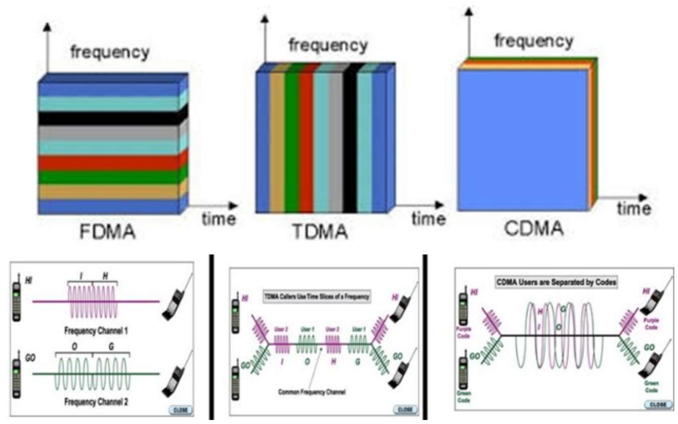
- Collisions can be avoided by ensuring that each node can use its allocated resources exclusively
- Examples of fixed assignment strategies:

❑ **FDMA:** Frequency Division Multiple Access
- the frequency band is divided into several smaller frequency bands
- the data transfer between a pair of nodes uses one frequency band
- all other nodes use a different frequency band

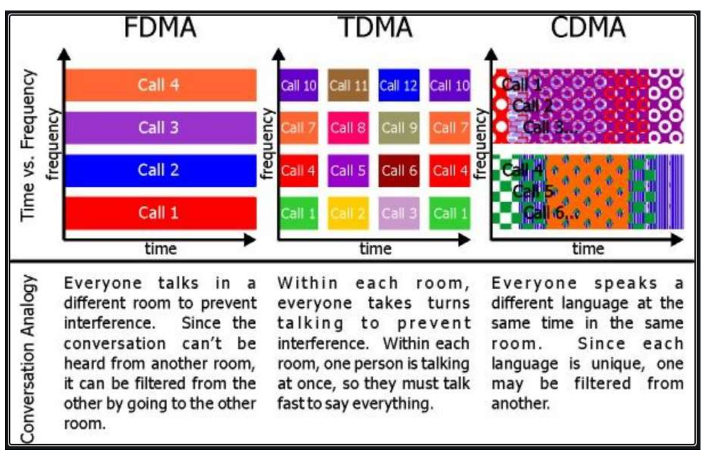
❑ **TDMA:** Time Division Multiple Access
- multiple devices to use the same frequency band
- relies on periodic time windows (frames)
  - frames consist of a fixed number of transmission slots to separate the medium accesses of different devices
  - a time schedule indicates which node may transmit data during a certain slot

MAC LAYER – CONTENTION-FREE MEDIUM ACCESS

- CDMA: Code Division Multiple Access
  - 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
  - forward error correction (FEC) at the receiver is used to recover from interferences among these simultaneous communications



MAC LAYER – CONTENTION-FREE MEDIUM ACCESS



- Fixed assignment strategies are *inefficient*
  - it is impossible to reallocate slots belonging to one device to other devices if not needed in every frame
  - generating schedules for an entire network can be a taunting task
  - these schedules may require modifications every time the network topology or traffic characteristics in the network change

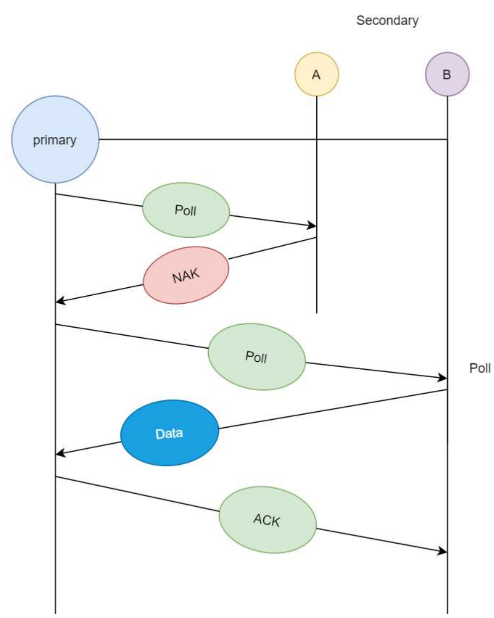
MAC LAYER – CONTENTION-FREE MEDIUM ACCESS

Dynamic assignment strategies: allow nodes to access the medium on demand:

- **Polling-based Protocols**
  - In a computer network there is a primary station or controller (teacher) and all other stations are secondary (students), the primary station sends a message to each station. The message which is sent by the primary station consists of the address of the station which is selected for granting access in a round-robin fashion.
  - The point to remember is that all the nodes receive the message but the addressed one responds and sends data in return, but if the station has no data to transmit then it sends a message called **Poll Reject or NAK** (negative acknowledgment).

MAC LAYER – CONTENTION-FREE MEDIUM ACCESS

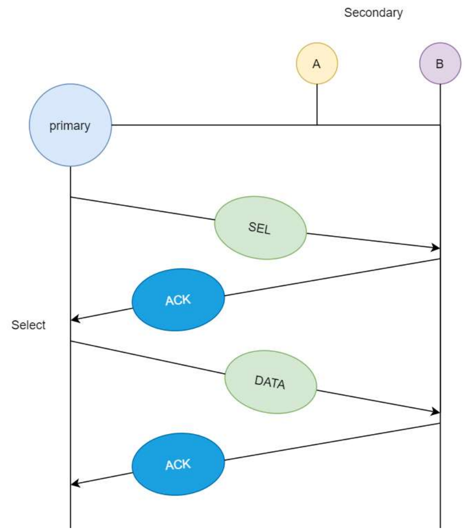
- **Polling-based Protocols**
- Whenever the primary station wants to receive the data, it asks the secondary stations present in its channel, this method is **polling**. In this diagram, we see that primary station asks station A if it has any data ready for transmission, since A does not have any data queued for transmission it sends NAK (negative acknowledgement), and then it asks station B, since B has data ready for transmission, so it transmits the data and in return receives acknowledgement from primary station.



MAC LAYER – CONTENTION-FREE MEDIUM ACCESS

❑ Polling-based Protocols

- In the next case, if primary station wants to send data to the secondary stations, it sends a select message, and if the secondary station accepts the request from the primary station, then it sends back an acknowledgement and then primary station transmits the data and in return receives an acknowledgement.

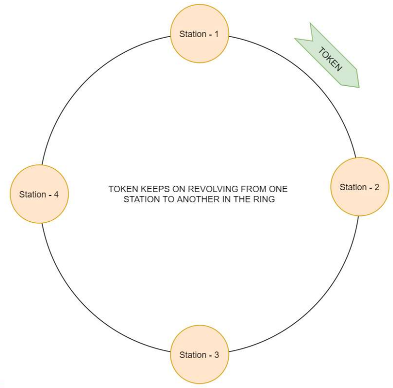


MAC LAYER – CONTENTION-FREE MEDIUM ACCESS

❑ Token Passing

- In computer networks a token is a special bit pattern that allows the token possessing system to send data or we can say that a token represents permission to transmit data.
- The token circulation around the table (or a network ring) is in a predefined order. A station can only pass the token to its adjacent station and not to any other station in the network.
- If a station has some data queued for transmission it can not transmit the data until it receives the token and makes sure it has transmitted all the data before passing on the received token.

In the diagram, when station-1 posses the token it starts transmitting all the data-frames which are in it's queue. now after transmission, station-1 passes the token to station-2 and so on. Station-1 can now transmit data again, only when all the stations in the network have transmitted their data and passed the token.



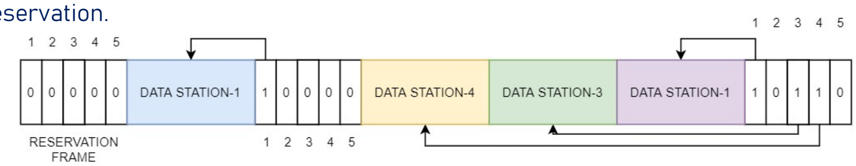
MAC LAYER – CONTENTION-FREE MEDIUM ACCESS

- 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

Consider there are 4 stations then the reservation intervals are divided into 4 slots so that each station has a slot. Means if n number of stations are there then n slot will be allotted.

Similarly, if station-1 transmits a 1-bit data-frame in slot-1 then at that time no other station can transmit its data-frames and they must wait for their time slot. After all the slots have transmitted and checked then each station knows which station now wishes for transmission.

The illustration below shows a scenario with five stations with a five-slot reservation frame. here, in the time interval station 1,3,4 are the only stations with reservations and in the second interval station-1 is the only station with a reservation.



MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Contention-based Medium Access Protocol

- Contention is a media access method that is used to share the broadcast medium.
- Nodes may initiate transmissions at the same time or any time. It requires mechanisms to reduce the number of collisions and to recover from collisions.
- Node does not make any resource reservation a priori.
- Whenever it receives a packet to be transmitted, it contends with its neighbor for access to the shared channel.
- Nodes are not guaranteed periodic access to the channel.
- Examples are: *Pure ALOHA, Slotted-ALOHA, CSMA, 802.11* etc.
- The listen before talk operating procedure in 802.11 is the well known contention based protocol.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

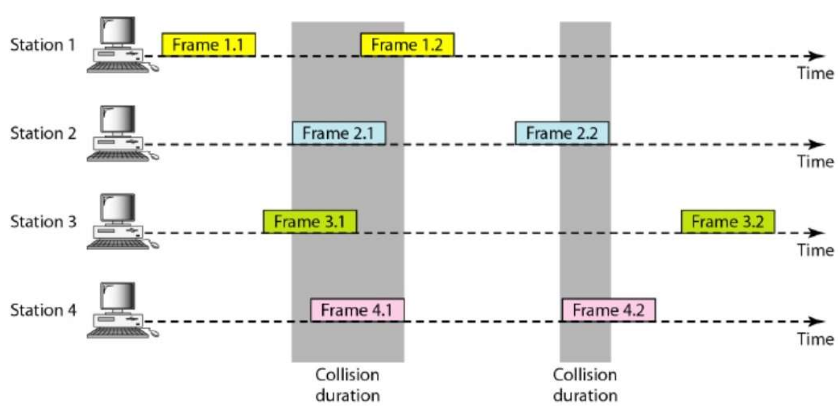
Pure ALOHA Protocol

- Packet Radio sends one packet per unit time.
- *Algorithm:* Node transmits packet whenever it requires. If Collision occurs, it waits for random time interval and retransmit the packet.
- *Topology*
  - All stations sends frame to central node, which broadcast packets to all stations.
  - Use of two distinct frequencies in a hub/star configuration.
  - The central station broadcast packets to everyone on the "Outbound" channel.
  - Various stations sends data packets to the central station on the "Inbound" channel.
- *Protocol:*
  - Whenever station has data, it transmits.
  - Sender finds out, whether the transmission was successful or not by listening to the broadcast from the central node.
  - If collision occurs, the sender retransmits frames/packets after some random time interval.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Pure ALOHA Protocol

- Very Simply to Apply
- Low utilization of channel
- Suitable for light loads only
- Chances of collisions are very high

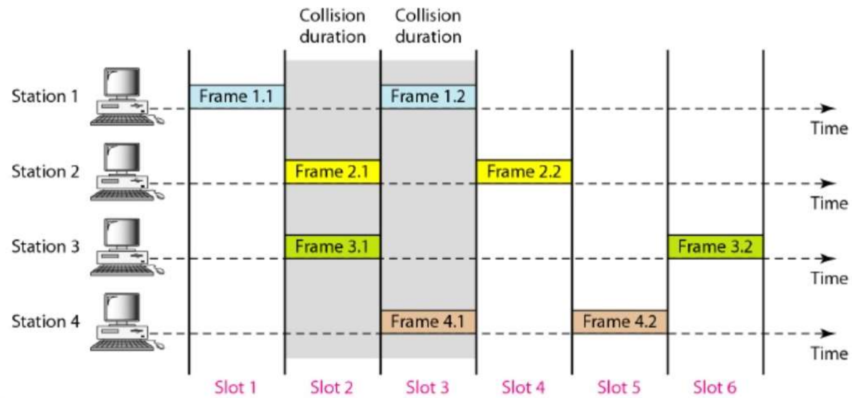


MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Slotted- LOHA Protocol

- Modified version of Pure ALOHA. It was invented to improve the efficiency of Pure ALOHA as chances of collisions in Pure ALOHA are very high.

- Slotted-ALOHA
  - It is a ALOHA with an additional constraint.
  - Time is divided into discrete time intervals (slots).
  - A station can only transmits at the beginning of the time frame.



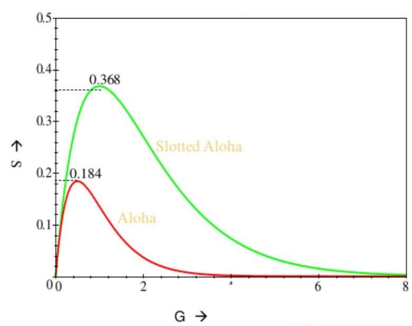
MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Slotted- LOHA Protocol

- Then, Slotted-ALOHA
  - Transmission synchronized to the start of the time frame.
  - Window of vulnerability is 1 time unit not 2.
  - It requires timing mechanism.
  - No partial collision.

- In Slotted ALOHA, there is still possibility of collision, if two stations try to sends at the beginning of the same time slot.

- Slotted-ALOHA is still has an edge over Pure ALOHA as chances of collisions are reduced to one-half.



MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access (CSMA) - Non-persistent CSMA

- When a node becomes ready to transmit a packet, it first senses the carrier to determine is another transmission in progress?
- To avoid collisions by listening to the carrier due to transmission from another user.
- If channel is idle or free, the node transmits its packet immediately and waits for the acknowledgement.
- In setting the acknowledgment timeout value, the node must take into account the round-trip propagation delay and the fact that the receiving node must also contend for the channel to transmit the acknowledgment.
- Estimating the average contention time required for a successful transmission is difficult, as it depends on the traffic load and the number of stations contending.
- In the absence of an acknowledgment, before a timeout occurs, the sending node assumes that the data packet is lost due to collision or noise interference.
- The station schedules the packet for retransmission.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

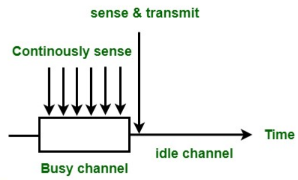
Carrier Sense Multiple Access (CSMA) - Non-persistent CSMA

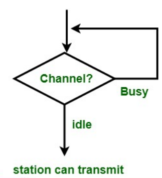
- If the channel is busy, the transmitting node "**backs off**" for a random period of time after which it senses the channel again.
- Non-Persistent CSMA protocol Depending on the status of the channel, the station transmits its packet if the channel is idle, or enters the back-off mode if the channel is busy.
- This process is repeated until the data packet is transmitted successfully.
- The non-persistent CSMA protocol minimizes the interference between packet transmissions, as it requires stations that find the channel busy to reschedule their transmissions randomly.
- *Drawback:*
  - Channel may become idle during the back-off time of a contending station.
  - The unnecessary waste of channel capacity can reduce significantly the overall network throughput.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access (CSMA) - Persistent CSMA

- The need to address the shortcomings of non-persistent CSMA led to the development of a class of p-persistent CSMA schemes.
- These schemes differ in the algorithm they use to acquire a free channel.
- The 1-persistent scheme never allows the channel to remain idle if a node is ready to transmit.
- Based on this scheme,
  - A node ready to transmit a data packet first senses the channel.
  - If the channel is free, the node transmits its message without any delay. It transmits the frame with probability 1. Due to probability 1, it is called 1-persistent CSMA.
  - If the channel is busy, however, the node persistently continues to listen until the channel becomes idle.





MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access (CSMA) - Persistent CSMA

The problem with this method is that there are a large number of chances for the collision it is because there is a chance when two or more stations found channel in idle state and the transmit frames at the same time. On the time when collision occurs the station has to wait for the random time for the channel to be idle and to start all again.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

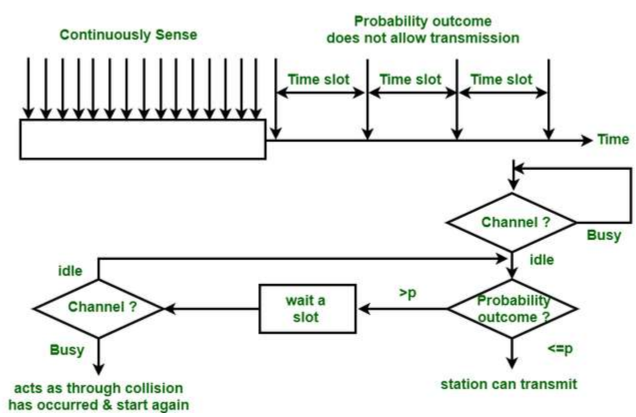
Carrier Sense Multiple Access (CSMA) - Persistent CSMA

- The p-persistent algorithm represents a compromise between the non-persistent & 1-persistent schemes.
- Based on this algorithm,
  - This is the method that is used when channel has time-slots and that time-slot duration is equal to or greater than the maximum propagation delay time.
  - When the station is ready to send the frames, it will sense the channel.
  - If the channel found to be busy, the channel will wait for the next slot.
  - If the channel found to be idle, it transmits the frame with probability p, thus for the left probability i.e. q which is equal to 1-p the station will wait for the beginning of the next time slot.
  - In case, when the next slot is also found idle it will transmit or wait again with the probabilities p and q.
  - This process is repeated until either the frame gets transmitted or another station has started transmitting.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access (CSMA) - Persistent CSMA

P-persistent algorithm



MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access /Collision Detection (CSMA/CD)

CSMA:

- In networks where the propagation delay is small relative to the packet transmission time, the CSMA scheme and its variants can result in smaller average delays and higher throughput than with the ALOHA protocols.
- This performance improvement is due to the fact that carrier sensing reduces the number of collisions and, more important, the length of the collision interval.

Drawback CSMA:

- Contending stations continue transmitting their data packets even when collision occurs.
- For long data packets, the amount of wasted bandwidth is significant compared with the propagation time.
- Nodes may suffer unnecessarily long delays waiting for the transmission of the entire packet to complete before attempting to transmit the packet again.

To overcome the shortcomings:

- Networks use CSMA/CD, to extend the capabilities of communicating node to listen while transmitting.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access /Collision Detection (CSMA/CD)

CSMA/CD

This allows the node:

- To monitor the signal on the channel and
- To detect a collision when it occurs.

OPERATION :

- More specifically, if a node has data to send, it first listens to determine if there is an ongoing transmission over the communication channel.
- In the absence of any activity on the channel, the node starts transmitting its data and continues to monitor the signal on the channel while transmitting.
- If an interfering signal is detected over the channel, the transmitting station immediately aborts its transmission.

ADVANTAGE:

- This reduces the amount of bandwidth wasted due to collision to the time it takes to detect a collision.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access /Collision Detection (CSMA/CD)

STRATEGY & ALGORITHM:

- When a collision occurs, each contending station involved in the collision waits for a time period of random length before attempting to retransmit the packet.
- The length of time that a colliding node waits before it schedules packet retransmission is determined by a probabilistic algorithm, referred to as the truncated binary exponential back-off algorithm.

DRAWBACK:

- The need to provision sensor nodes with collision detection capabilities.
- As the Sensor nodes have a very limited amount of storage, processing power and energy resources, these limitations impose severe constraints on the design of the MAC layer.
- Another important factor that works against using a CSMA/CD based strategy to regulate access to a shared medium in a wireless environment is the difficulty of detecting collision in a wireless environment.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access /Collision Avoidance (CSMA/CA)

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer.
- In contrast to CSMA/CD (Carrier Sense Multiple Access/Collision Detection) that deals with collisions after their occurrence, CSMA/CA prevents collisions prior to their occurrence.
- Nodes sense the medium, but do not immediately access the channel when it is found idle.
- Instead, a node waits for a time period called DCF interframe space (DIFS) plus a multiple of a slot size.
- In case there are multiple nodes attempting to access the medium, the one with the shorter back-off period will win.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access /Collision Avoidance (CSMA/CA)

Algorithm

The algorithm of CSMA/CA is:

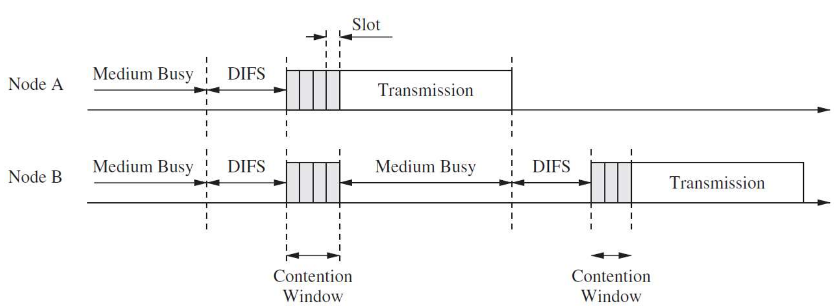
- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is busy, the station waits until the channel becomes idle.
- If the channel is idle, the station waits for an Inter-frame gap (IFG) amount of time and then sends the frame.
- After sending the frame, it sets a timer.
- The station then waits for acknowledgement from the receiver. If it receives the acknowledgement before expiry of timer, it marks a successful transmission.
- Otherwise, it waits for a back-off time period and restarts the algorithm.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access /Collision Avoidance (CSMA/CA)

Example:

- Node A waits for DIFS + 4 $*$ s (where s represents the slot size), while node B's back-off is DIFS + 7 $*$ s.
- Once node A begins with its transmission, node B freezes its own backoff timer and resumes the timer after node A completes its transmission plus another period of DIFS.
- Once node B's back-off timer expires, it can also begin its transmission.



Medium access using CSMA/CA

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access /Collision Avoidance (CSMA/CA)

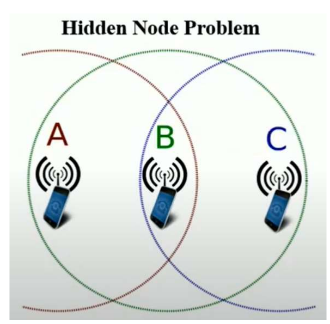
- Carrier sensing prior to transmission is an effective approach to increase the throughput efficiency in shared-medium access environments.
- In wireless environments, the scheme is susceptible to two problems, commonly referred to as the *hidden-node* and *exposed-node* problems.
- The hidden and exposed-node problems result indirectly from the time-varying properties of the wireless channel, which are caused by physical phenomena such as noise, fading, attenuation and path loss.
- These interferences, combined with the rapid decrease in the power received with the distance between the sender and receiver, limit the maximum transmission range that can be achieved by a sending node.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access /Collision Avoidance (CSMA/CA)

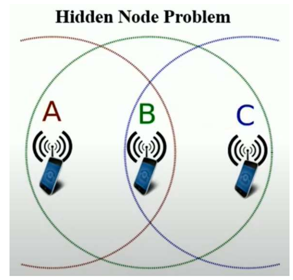
HIDDEN NODE PROBLEM

- A hidden node is defined as a node that is within the range of the destination node but out of range of the transmitting node.
- To illustrate this example, consider figure where node B is within the transmission range of nodes A and C.
- Furthermore, assume that nodes A and C are outside their mutual transmission ranges.
- Hidden node Consequently, any transmission from either of the two nodes will not reach the other node. { A $\leftrightarrow$ C}
- Given this network configuration, assume that node A needs to transmit a data packet to node B. {A $\rightarrow$ B}
- According to the CSMA protocol, node A senses the channel and determines that it is free.



MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access /Collision Avoidance (CSMA/CA)



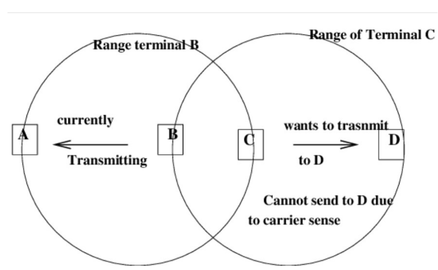
- Node A then proceeds to transmit its packet.
- Assume now that before node A completes its transmission to node B, node C decides to transmit a data packet to node B.
- Hidden node Using the CSMA protocol, node C senses the channel and also determines that the channel is free, since node C, which is outside the transmission range of node A, cannot hear the signal transmitted by node A.
- As a result, both transmissions collide at node B, thereby causing the loss of both data packets.
- Notice that neither node A nor node C is aware of the collision, since it happens at the receiver.
- This feature is intrinsic to wireless networks and constitutes a fundamental difference in the way that collisions are dealt with in wired and wireless environments.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access /Collision Avoidance (CSMA/CA)

EXPOSED NODE PROBLEM

- An exposed node is a node that is within the range of the sender but out of the range of the destination.
- To illustrate problem, the consider exposed-node the network depicted in Figure, where node B is within the transmission range of nodes A and C, nodes A and C are outside their mutual transmission ranges, and node D is within the transmission range of node C.
- Assume that node B wants to transmit a message to node A.
- Node B executes the CSMA protocol to sense the channel, determines that the channel is free, and proceeds to transmit the data packet to node A.

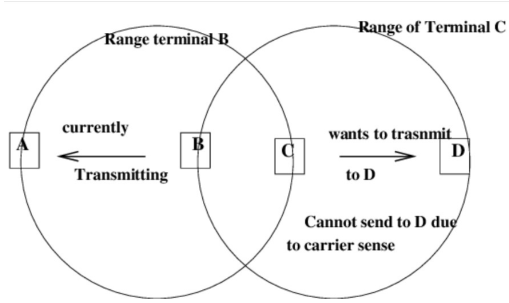


MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Carrier Sense Multiple Access /Collision Avoidance (CSMA/CA)

EXPOSED NODE PROBLEM

- Assume now that node C needs to send a packet to D.
- Node C follows the CSMA rule and first senses the channel.
- Due to the ongoing transmission between nodes B and A, node C determines that the channel is busy and delays the transmission of its packet to a later time.
- It is clear, however, that this delay is unnecessary, since the transmission from node C to node D would have been completed successfully, as node D is outside the range of node B.



MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

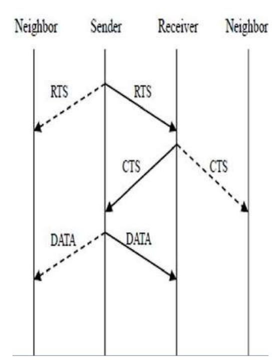
Multiple Access Collision Avoidance (MACA)

MACA

- It is a medium access control (MAC) layer protocol used in wireless networks, with a view to solve the hidden terminal problem and exposed terminal problem.
- The MAC layer protocol IEEE 802.11 RTS/CTS has been adopted from MACA.

Working Principle

- The MACA protocol works with the condition that the stations are synchronized and frame sizes and data speed are the same. It involves transmission of two frames called RTS and CTS prior to data transmission.
- RTS stands for Request to Send and CTS stands for Clear to Send.
- Once the sender receives the CTS packet without any error, it starts transmitting the data packet.
- If a packet transmitted by a node is lost, the node uses the binary exponential back-off (BEB) algorithm to back off a random interval of time before retrying. In this each time a collision occurs the node doubles its maximum back-off windows.



MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Multiple Access Collision Avoidance (MACA)

- The binary exponential back-off mechanism used in MACA might starves flows sometimes.
- The problem is solved by MACAW.

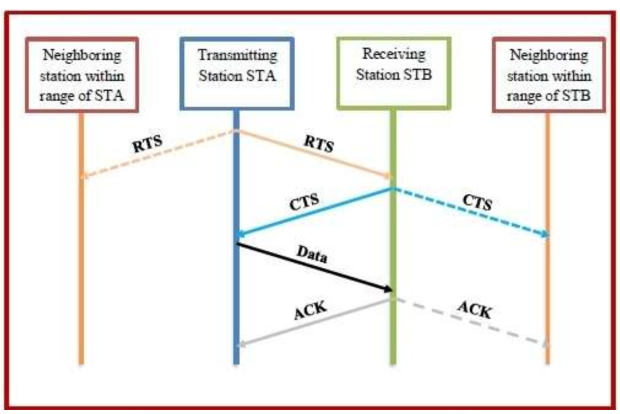
Let us consider that a transmitting station A has data frame to send to a receiving station B. The operation works as follows:

- Station A sends a RTS frame to the receiving station.
- On receiving the RTS, station B replies by sending a CTS frame.
- On receipt of CTS frame, station A begins transmitting its data frame.
- After successful receipt of the data frame, station B sends an ACK frame (acknowledgement frame).

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Multiple Access /Collision Avoidance (MACA)

- Any station than can hear RTS is close to the transmitting station and remains silent long enough for the CTS, or waits for a certain time period. If the RTS is not followed by a CTS, the maximum waiting time is the RTS propagation time.
- Any station that can hear the CTS is close to the receiving station and remains silent during the data transmission. It attempts for transmission after hearing the ACK.

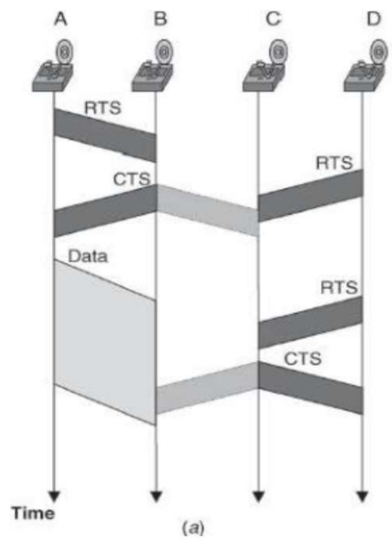


MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Multiple Access Collision Avoidance (MACA)

RTS & CTS handshake Approach: limitation Case-I

- Node A senses the channel to be free and sends an RTS packet to node B. In reply, node B sends a CTS packet.
- Node C, which is in the transmission range of node B, starts receiving the CTS packet.
- Before the reception of this packet is complete, however, node D, which is in the transmission range of node C, sends a RTS packet. The latter packet collides with the CTS packet sent by node B.
- Meanwhile, node A, which receives the CTS packet correctly, proceeds to transmit its data packet to node B

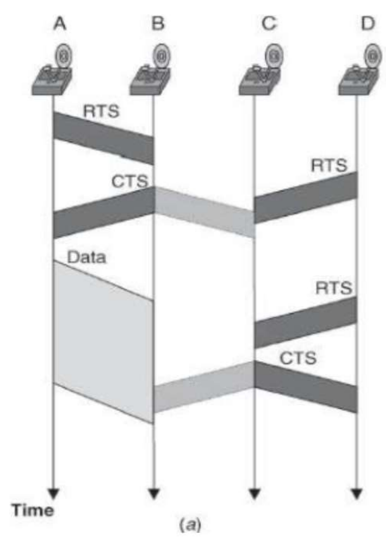


MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Multiple Access Collision Avoidance (MACA)

RTS & CTS handshake Approach: limitation Case-I

- Node D later times-out and retransmits its RTS packet.
- Since node C never received node B's CTS packet, it assumes that the channel is free and replies with a CTS packet to node D.
- Since node B is within the transmission range of node C, the latter packet collides with the data packet being transmitted by node A.

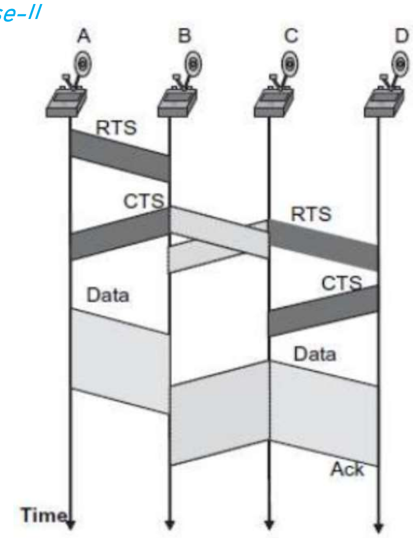


MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Multiple Access /Collision Avoidance (MACA)

RTS & CTS handshake Approach: limitation Case-II

- Node A senses the channel to be free and sends an RTS packet to node B. In reply, node B sends a CTS packet to node A.
- The CTS packet is received correctly by node A, which allows it to transmit its packet.
- The CTS packet is also received by node C, which is within the transmission range of node B.
- Since node C has started transmitting an RTS packet to node D, nearly at the same time that node B is transmitting its CTS packet; node C does not receive correctly the CTS packet sent by B.



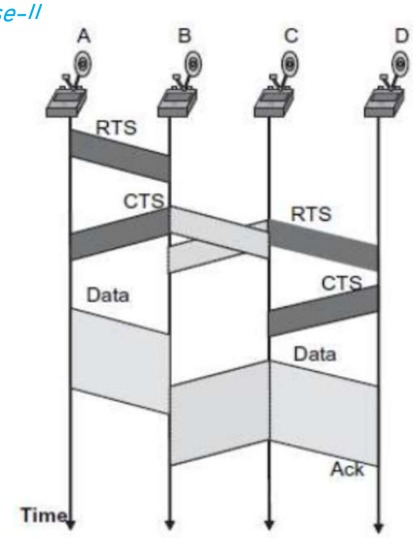
(b)

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Multiple Access Collision Avoidance (MACA)

RTS & CTS handshake Approach: limitation Case-II

- Node D, however, receives correctly the RTS packet sent by node C. In response, it sends a CTS packet to node C, thereby allowing it to start transmitting its data packet.
- Since node A did not complete transmission of its data packet to node B, node C's data transmission causes a collision at node B.



(b)

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Multiple Access Collision Avoidance (MACA)

- There is no carrier sensing in MACA so Collision occurs during the RTS-CTS phase
- Each mobile host adds a random amount of time to the minimum interval required to wait after overhearing an RTS or CTS control message.
- In MACA, the slot time is the duration of an RTS packet.
- If two or more stations transmit an RTS concurrently, resulting in a collision, these stations will wait for a randomly chosen interval and try again, doubling the average interval on every attempt.
- The station that wins the competition will receive a CTS from its responder, thereby blocking other stations to allow the data communication session to proceed.
- Compared to CSMA, MACA reduces the chances of data packet collisions. Since control messages (RTS and CTS) are much smaller in size compared to data packets, the chances of collision are also smaller

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Multiple Access Collision Avoidance With Wireless (MACAW)

MACAW (MACA with Wireless)

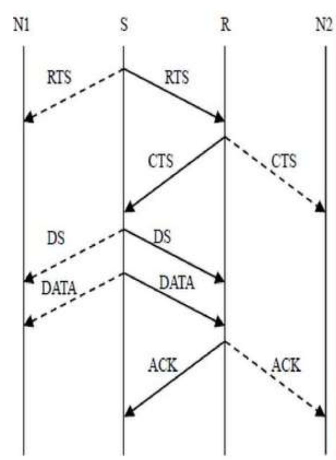
- The binary exponential back-off mechanism used in MACA might starves flows sometimes.
- The problem is solved by MACAW.
- The packet header has current back-off counter value of transmitting node.
- It implements per flow fairness as opposed to the per node fairness in MACA.
- MACAW is proposed as a series of improvements to the basic MACA algorithm.
  1. Suggest a less aggressive backoff algorithm:
     - a multiplicative increase and linear decrease(MILD) backoff mechanism is used.
     - Increasing BO by 1.5 after a timeout, and decreasing it by 1 after a successful RTS-CTS pair.
  2. proposes that receivers should send an ACK to the sender after successfully receiving a data message.
  3. Propose two related techniques for allowing transmitters to avoid contention more effectively:
     - Data sending (DS)
     - Request-for-request-to-send (RRTS)

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Multiple Access Collision Avoidance With Wireless (MACAW)

MACAW (MACA with Wireless)

- It is a revision of MACA. The sender transmits a RTS (Request To Send) frame if no nearby station transmits a RTS.
- The receiver replies with a CTS (Clear To Send) frame.
- 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.

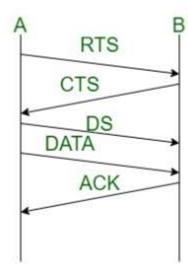


MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Multiple Access Collision Avoidance With Wireless (MACAW)

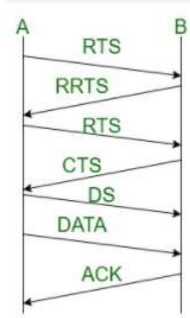
MACAW (MACA with Wireless)

- *DATA Sending (DS) Packets :*
  - A DS packet should be sent after a successful RTS-CTS exchange, just before the data message itself.
  - The idea is to explicitly announce that the RTS-CTS succeeded, so that if a node can hear an RTS but not the CTS response, it does not attempt to transmit a message during the subsequent data transfer period.



In MACA , an exposed node can received only the RTS and not the CTS packet

- *READY for RTS (RRTS):*
  - if a receiver hears an RTS while it is deferring any transmissions, at the end of the deferral period it replies with an RRTS ("ready for RTS") packet, prompting the sender to resend the RTS.

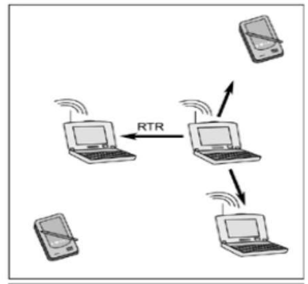


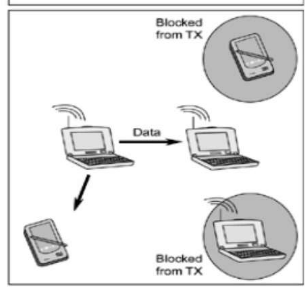
MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Multiple Access Collision Avoidance By Invitation(MACA-BI)

MACA-BI(MACA By Invitation)

- MACA-BI uses only a two-way handshake.
- No RTS. the CTS message is renamed as RTR (Ready To Receive).
- Type: Receiver initiated MAC Protocol
  - A node cannot transmit data unless it has received an invitation from the receiver.
- Receiver node does not necessarily know that the source has data to transmit.
  - receiver needs to predict if node has data to transmit to it.
- The timeliness of the invitation will affect communication performance.





MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Multiple Access Collision Avoidance By Invitation(MACA-BI)

MACA-BI(MACA By Invitation)

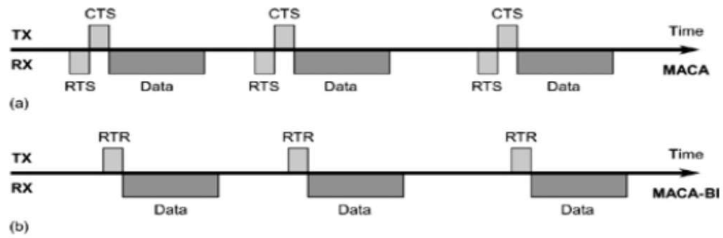
- Packet queue length and arrival rate information is piggyback into each data packet so that the receiver is aware of the transmitter's backlog.
- For constant bit rate (CBR) traffic, the efficiency of MACA-BI will be high since the prediction scheme will work fine. However, will not perform well in case of bursty traffic.
- To enhance the communication performance of MACA-BI under non-stationary traffic situations
  - a node may still transmit an RTS if the transmitter's queue length or packet delay exceeds a certain acceptable threshold before an RTR is issued.
  - MACA-BI now reverts back to MACA.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Multiple Access Collision Avoidance By Invitation(MACA-BI)

MACA Vs MACA-BI

- As MACA-BI only uses a single control message, this turn around limitation is reduced (i.e., up to 25 microseconds).
- MACA-BI is less likely to suffer from control packet collision since it uses half as many control packets as MACA



MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

IEEE 802.11

- Published in 1999 by the Institute of Electrical and Electronics Engineers (IEEE)
  - specifies the physical and data link layers of the OSI model for wireless connections
- Often referred to as *Wireless Fidelity (Wi-Fi)*
  - certification given by Wi-Fi Alliance, a group that ensures compatibility between hardware devices that use the 802.11 standard
- Wi-Fi combines concepts found in *CSMA/CA* and *MACAW*, but also offers features to preserve energy
- Two modes of operation
  - *Point Coordination Function (PCF)* mode
    - Communication among devices goes through a central entity called an access point (AP) or base station (BS): **managed mode**
  - *Distributed Coordination Function (DCF)* mode
    - Devices communicate directly with each other: **ad-hoc mode**

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

IEEE 802.11

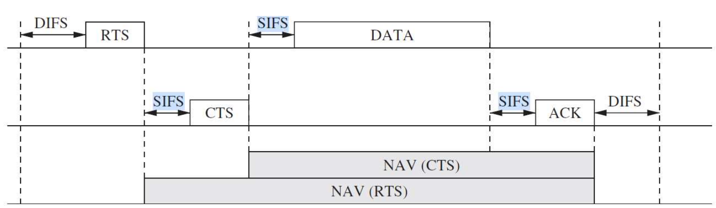
IEEE 802.11 is based on *CSMA/CA*

- before a node transmits, it first senses the medium for activity
- the node is allowed to transmit, if the medium is idle for at least a time period called the DCF interframe space (DIFS)
- otherwise the device executes a back-off algorithm to defer transmission to a later time
- this algorithm randomly selects a number of time slots to wait and stores this value in a back-off counter
- for every time slot that passes without activity on the network, the counter is decremented and the device can attempt transmission when this counter reaches zero
- if activity is detected before the counter reaches zero, the device waits until the channel has been idle for a period of DIFS before it continues to decrement the counter value

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

IEEE 802.11

- After a successful transmission
  - Receiver device responds with an acknowledgment after waiting for a time period called the *short interframe space* (SIFS)
  - The value of SIFS is smaller than the value of DIFS to ensure that no other device accesses the channel before the receiver can transmit its acknowledgment
- Once a node A makes a reservation using RTS and CTS control messages
  - Another neighboring node B, overhearing the RTS message, must refrain from accessing the medium until node A's transmission has been completed and acknowledged
  - However, this would mean that node B has to continuously sense the medium to detect when it becomes idle again



IEEE 802.11 medium access control

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

IEEE 802.11

- Instead, A's RTS message carries the size of the data it will transmit
  - Allowing node B to estimate how long the transmission will take and to decide whether to enter a low-power sleep mode
  - Some neighboring nodes may only overhear CTS (but not RTS), therefore, the data size is also carried in the CTS message
  - Using the data size information, neighboring nodes set a network allocation vector (NAV) that indicates how long the medium will be unavailable
    - reduces the need for continuously sensing the medium, allowing a node to save power

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

IEEE 802.11

PCF mode

- Access point (AP) coordinates channel access to ensure collision-free communication
  - periodically broadcasts a beacon to its client devices (includes list of devices with data pending at AP)
- During contention-free period, AP transmits these packets to its client devices
- AP can also poll client devices to allow them to initiate data transfers
- AP uses a wait period called the PCF interframe space (PIFS)
  - PIFS is shorter than DIFS, but longer than SIFS
  - Ensures that PCF traffic has priority over traffic generated by devices operating in the DCF mode, without interfering with control messages in the DCF mode such as CTS and ACK

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

IEEE 802.11

- Focus of IEEE 802.11 is on providing fair access to the medium with support for high throughput and mobility
  - Since devices spend a large amount of time listening to the medium and collisions occur frequently, this standard incurs large overheads, including significant energy costs

- *Energy consumption problem*
  - IEEE 802.11 offers a ***power saving mode (PSM)*** for devices operating in the PCF mode.
  - Devices can inform the AP that they wish to enter a low-power sleep mode using special control messages.
  - These devices wake up periodically to receive beacon messages from the AP to determine if they should stay awake to receive incoming messages.
  - Saves energy, but only works in the infrastructure mode and it is not specified when or how long devices should sleep.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

IEEE 802.15.4

- The Institute of Electrical and Electronics Engineers (IEEE) supports many working groups to develop and maintain wireless and wired communications standards.

- For example:
- 802.3 is Wired Ethernet and
- 802.11 is for Wireless LANs (WLANs), also known as Wi-Fi.
- The 802.15 group of standards specifies a variety of wireless personal area networks (WPANs) for different applications.
  - For instance, 802.15.1 is Bluetooth.
  - 802.15.3 is a high-data-rate category for ultra-wideband (UWB) technologies.
  - 802.15.6 is for body area networks (BAN). There are several others.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

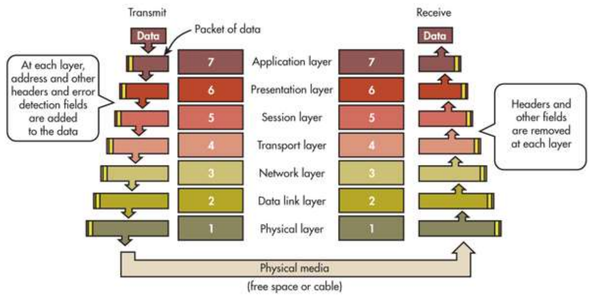
IEEE 802.15.4

- The 802.15.4 category is probably the largest standard for low-data-rate WPANs.
- It has many subcategories.
  - The 802.15.4 category was developed for low-data-rate monitor and control applications and extended-life low-power-consumption uses.
  - The basic standard with the most recent updates and enhancements is 802.15.4a/b, with 802.15.4c for China, 802.15.4d for Japan, 802.15.4e for industrial applications, 802.15.4f for active (battery powered) radio-frequency identification (RFID) uses, and 802.15.4g for smart utility networks (SUNs) for monitoring the Smart Grid.
  - All of these special versions use the same base radio technology and protocol as defined in 802.15.4a/b.

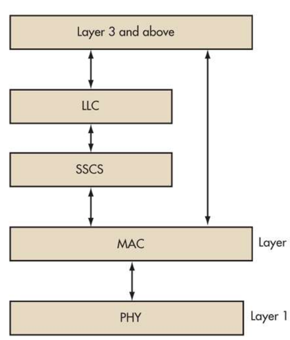
MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

IEEE 802.15.4

The 802.15.4 standard defines the physical layer (PHY) and media access control (MAC) layer of the Open Systems Interconnection (OSI) model of network operation.



- *Most networking systems, both wired and wireless, use the OSI communications model. Most systems also use at least the first four layers, but many do not use all seven layers.*
- *The 802.15.4 standard uses only the first two layers plus the logical link control (LLC) and service specific convergence sub-layer (SSCS) additions to communicate with all upper layers as defined by additional standards.*



MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

IEEE 802.15.4

- Created for low-power devices in the 868 MHz, 915 MHz, and 2.45 GHz frequency bands
- Supports two transmission modes:
  - UWB PHY
    – bit rates: 110 kbps, 851 kbps (nominal), 6.81 kbps, and 27.24 Mbps
  - CSS PHY
    – bit rates: 1 Mbps (nominal) and 250 kbps
- With regard to channel access, 802.15.4 uses carrier sense multiple access with collision avoidance (CSMA-CA). This multiplexing approach lets multiple users or nodes access the same channel at different times without interference.

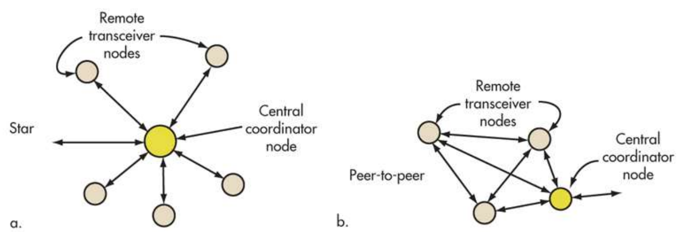
OPTIONS FOR FREQUENCY ASSIGNMENTS

Geographical regions	Europe	Americas	Worldwide
Frequency assignment	868 to 868.6 MHz	902 to 928 MHz	2.4 to 2.4835 GHz
Number of channels	1	10	16
Channel bandwidth	600 kHz	2 MHz	5 MHz
Symbol rate	20 ksymbols/s	40 ksymbols/s	62.5 ksymbols/s
Data rate	20 kbits/s	40 kbits/s	250 kbits/s
Modulation	BPSK	BPSK	Q-QPSK

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

IEEE 802.15.4

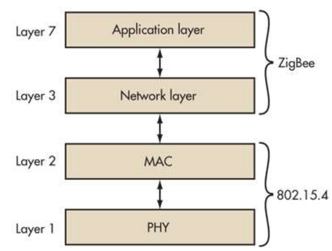
- Transmission range varies considerably depending on the nature of the path that must for the most part be line of sight (LOS). Under the best conditions the range can be as great as 1000 meters with a clear outdoor path. Most applications cover a shorter range of 10 to 75 meters.
- With regard to networking capability, *802.15.4 standard defines the star and peer-to-peer common network topologies.*
  - One of them is a basic **Star**. All communications between nodes must pass through the central coordinator node.
  - A basic **peer-to-peer (P2P)** topology is also defined. Any device may then talk to any other device. This basic topology may be expanded into other topologies in the upper network layers, such as the popular mesh topology.



MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Zigbee

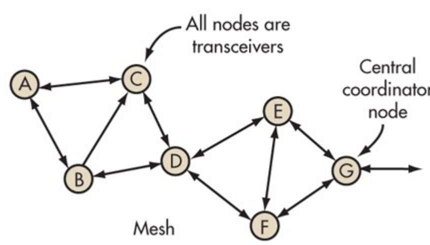
- The most widely deployed enhancement to the 802.15.4 standard is ZigBee, which is a standard of the ZigBee Alliance. The organization maintains, supports, and develops more sophisticated protocols for advanced applications.
- It uses layers 3 and 4 to define additional communications features *(Fig.)*.
- These enhancements include authentication with valid nodes, encryption for security, and a data routing and forwarding capability that enables mesh networking.
- The most popular use of ZigBee is wireless sensor networks using the mesh topology.
- The ZigBee protocol is defined by layer 3 and above. It works with the 802.15.4 layers 1 and 2.



MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Zigbee

- There are three kinds of nodes in a ZigBee network:
  1. **Coordinator**: is the "master" device, it governs all the network
  2. **Routers**: they route the information which sent by the end devices
  3. **End device**: (the motes): they are the sensor nodes, the ones which take the information from the environment
- Coordinator and routes can not be battery powered, motes can. ZigBee creates **star topologies**. There are some basic rules:
  - The end devices connect to a router or a coordinator.
  - The routers can connect among them and with the coordinator.
  - The routers and coordinators can not sleep. They have to save in their buffer the packets which go to the end devices.
  - The end devices can sleep.
- In a mesh network, each node communicates with its closest neighbor as conditions permit. Note that there are alternate paths between any two nodes.



MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Zigbee

- ZigBee offers basically four kinds of different services:
  - Extra Encryption services (application and network keys implement extra 128bit AES encryption)
  - Association and authentication (only valid nodes can join to the network).
  - Routing protocol: AODV, a reactive ad hoc protocol has been implemented to perform the data routing and forwarding process to any node in the network.
  - Application Services: An abstract concept called **"cluster"** is introduced. Each node belongs to a predefined cluster and can take a predefined number of actions.
- ZigBee is also available in a version that supports energy harvesting where no battery or ac mains power is available.
- One of the key benefits of ZigBee is the availability of pre-developed applications. These upper-layer software additions implement specialized uses for ZigBee.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

IEEE 802.15.4 Versus ZigBee

- 802.15.4 is thought to be a protocol to get point to point and energy efficient communications.
- ZigBee defines extra services (start topology routing, encryption, application services) over 802.15.4.
- ZigBee creates semi-centralized networks where just the end devices can sleep.
- Different completely distributed mesh algorithms are being used over 802.15.4 is the protocol used to create
- Both Waspmote and SquidBee benefit from all the 802.15.4, ZigBee and Digimesh protocols and support all the frequency bands 869MHz, 900MHz and 2.4GHz.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Characteristics of MAC Protocols in Sensor Networks

- Most MAC protocols are built for fairness
  - everybody should get an equal amount of resources
  - no one should receive special treatment
- In a WSN, all nodes cooperate to achieve a common purpose, therefore fairness is less of a concern.
- Instead, wireless nodes are mostly concerned with energy consumption.
- Sensing applications may value low latency or high reliability over fairness.
- The main characteristics and design goals for MAC protocols of WSNs:
  - *Energy Efficiency*
  - *Scalability*
  - *Adaptability*
  - *Low Latency and Predictability*
  - *Reliability*

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Characteristics of MAC Protocols in Sensor Networks

Energy Efficiency

- Sensor nodes must operate using finite energy sources, therefore MAC protocols must consider energy efficiency
- Common technique: *Dynamic Power Management (DPM)*
  - A resource can be moved between different operational modes such as active, idle, and asleep
  - For resources such as the network, the active mode can group together multiple different modes of activity, e.g., transmitting and receiving
- **Periodic Traffic Models** are very common in WSNs
  - Significant energy savings can be obtained by putting a device into a low-power sleep mode.
  - Fraction of time a sensor nodes spends in active mode is called the duty cycle.
  - Often very small due to the infrequent and brief data transmissions occurring in most sensor networks.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Characteristics of MAC Protocols in Sensor Networks

Energy Efficiency

- These are the main cause of energy consumption in WSN. It is required to use energy efficiently for the following operations.
  - idle listening (i.e., a device staying in idle mode unnecessarily)
  - inefficient protocol designs (e.g., large packet headers)
  - reliability features (collisions requiring retransmissions or other error control mechanisms)
  - control messages to address the hidden-terminal problem
  - choice of modulation scheme
  - choice of transmission rate
  - over emitting (that is, using larger transmit powers than necessary)

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Characteristics of MAC Protocols in Sensor Networks

Scalability

- Many wireless MAC protocols have been designed for use in infrastructure based networks.
  - Access points or controller nodes arbitrate access to the channel and perform some centralized coordination and management functions.
- Most wireless sensor networks rely on multi-hop and peer-to-peer communications without centralized coordinators.
- MAC protocols must be able to allow for efficient use of resources without incurring unacceptable overheads, particularly in very large networks.
- MAC protocols based on CDMA have to cache a large number of code (may be impractical for resource-constrained sensor devices).
- WSNs are not only constrained in their energy resources, but also in their processing and memory capacities.
- Therefore, MAC protocols should not impose excessive computational burden should not require too much memory to save state information

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Characteristics of MAC Protocols in Sensor Networks

Adaptability

- A key characteristic of a WSN is its ability to self-manage
  - adapt to changes in the network
  - including changes in topology, network size, density, and traffic characteristics
- A MAC protocol for a WSN should be able to gracefully adapt to such changes without significant overheads
- This requirement generally favors protocols that are dynamic in nature
  - Protocols that make medium access decisions based on current demand and network state
- Protocols with fixed assignments (e.g., TDMA with fixed-size frames and slots) may incur large overheads due to adaptations of such assignments that may affect many or all nodes in the network

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Characteristics of MAC Protocols in Sensor Networks

Low Latency & Predictability

- Many WSN applications have timeliness requirements
  - Sensor data must be collected, aggregated, and delivered within certain latency constraints or deadlines.
  - Example: wildfire detection (sensor data must be delivered to monitoring stations in a timely fashion to ensure timely responses).
- MAC protocol design
  - Choice of frame size and slot allocations in TDMA-based protocols may lead to large delays.
  - In contention-based protocols, nodes may be able to access the wireless medium sooner (than TDMA), but collisions and the resulting retransmissions incur delays.
  - Choice of MAC protocol can affect how predictable the experienced delay is (expressed as upper latency bounds).
  - Some contention-based MAC protocols allow the theoretical possibility of starvation.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Characteristics of MAC Protocols in Sensor Networks

Reliability

- Finally, reliability is a common requirement for most communication networks.
- The design of the MAC protocol can contribute to increased reliability by detecting and recovering from transmission errors and collisions (e.g., using acknowledgments and retransmissions).
- Particularly in wireless sensor networks, where node failures and channel errors are common, reliability is a key concern for many link-layer protocols.

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Contention-free Protocols

Concept:

- Allow only one sensor node to access the channel at any given time
- Thereby avoiding collisions and message retransmissions
- Assuming a perfect medium and environment
  - i.e., no other competing networks or misbehaving devices exist that could otherwise cause collisions or even jam a channel

- Contention-free protocols allocate resources to individual nodes to ensure exclusive resource access by only one node at any given time.
- Exposes a number of desirable characteristics
  - Node knows exactly when it has to turn on its radio
  - During all other times, radio can be turned off to preserve energy
  - Fixed slot allocations impose upper bounds on delay
  - Difficult to design schedules for large networks
  - Difficult to handle changes in topology, density, traffic load

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Contention-based Protocols

- These protocols do not rely on transmission schedules, instead they require other mechanisms to resolve contention when it occurs
- The main advantage of contention-based techniques is their simplicity compared to most schedule-based techniques
  - Schedule-based MAC protocols must save and maintain schedules or tables indicating the transmission order
  - Most contention-based protocols do not require to save, maintain, or share state information
  - This also allows contention-based protocols to adapt quickly to changes in network topologies or traffic characteristics
- However, they typically result in higher collision rates and overheads due to idle listening and overhearing (overheads usually refer to additional bits in a packet or additional packets such as control packets)
- They may also suffer from fairness issues (i.e., some nodes may be able to obtain more frequent channel accesses than others)

MAC LAYER – CONTENTION-BASED MEDIUM ACCESS

Various MAC Layer Protocols Developed for WSN

MAC Protocols

- Contention-free Protocols
  1. Traffic-Adaptive Medium Access (TRAMA) protocol
  2. *Y-MAC*
  3. *DESYNC-TDMA*
  4. Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol
  5. Lightweight Medium Access Control (LMAC) protocol
- Contention-based Protocols
  1. Power Aware Multi-Access with Signaling (PAMAS) protocol
  2. Sensor MAC (S-MAC) protocol
  3. Timeout MAC (T-MAC) protocol
  4. Pattern MAC (PMAC) protocol
  5. Routing-Enhanced MAC (RMAC) protocol
  6. Data-Gathering MAC (DMAC)
  7. *Preamble Sampling and Wise MAC*
  8. Receiver-Initiated MAC (RI-MAC) protocol
- Hybrid MAC Protocols
  1. Zebra MAC
  2. *Mobility Adaptive Hybrid MAC*

Questions asked in University Examination

Long Questions (5 Marks)

1. Discuss the energy efficiency in MAC protocol.
2. Discuss the distributed assignment of network wide unique MAC address for WSN.
3. Write short notes on MAC sublayer management.
4. Why CSMA protocol fails to avoid collisions and inefficient in WSN?
5. What is early sleep problem in T-MAC protocol? Explain the solution to avoid the problem?
6. Write Short Note on:
   a. S-MAC
   b. T-MAC
   c. D-MAC
7. Explain in brief about Directional MAC Protocols for Ad hoc wireless network?
8. Briefly explain the Classifications of MAC Protocols?
9. Explain in brief about Interleaved CSMA Protocol?
10. How low power listening mode is used to conserve energy in B-MAC protocol?
11. Explain why the relay diversity scheme may not work well with some sleep-oriented MAC protocols proposed for sensor networks.
12. Explain different characteristics of Contention-Free MAC Protocols.
13. How future-request-to-send (FRTS) is used to avoid the Early sleeping problem in case of T-MAC protocol.

Questions asked in University Examination

Short Questions (2 Marks)

1. What are the advantages of Contention-based MAC protocols over Contention-free MAC protocols?
2. Explain exposed node problem with suitable example.
3. Explain the different components of B-MAC protocol.
4. Explain different characteristics of Contention-Free MAC Protocols.
5. Explain different goals of MCA protocol in wireless sensor network.
6. Differentiate between S-Mac and T-MAC.
7. List the different disadvantages of ALOHA protocol.
8. What do you mean by slotted ALOHA?
9. what are the classification of MAC protocol?
10. What are the MAC services of IEEE 802.11 that are not provided in traditional LAN 802.3?
11. List the advantages of ALOHA protocol.