SRI MUTHUKUMARAN INSTITUTE OF TECHNOLOGY

(Approved by AICTE, Accredited by NBA and Affiliated to Anna University, Chennai)
Chikkarayapuram (Near Mangadu), Chennai- 600 069.

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

CEC365 – WIRELESS SENSOR NETWORK DESIGN
(REGULATION – 2021)

YEAR: III **SEM: V**

UNIT II: - MAC AND ROUTING PROTOCOLS

PART- A

1. What do you mean by Medium Access Control?

The Medium Access Control (MAC) is a sub layer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

2. List down the important classes of MAC protocol.

They can be roughly classified into the following classes:

- Fixed assignment protocols
- Demand assignment protocols
- Random access protocols

3. What do you mean by overhearing in wireless senor network?

Unicast frames have one source and one destination node. However, the wireless medium is a broadcast medium and all the source's neighbours that are in receive state hear a packet and drop it when it is not destined to them; these nodes overhear the packet.

4. What is Idle Listening.

A node being in idle state is ready to receive a packet but is not currently receiving anything. This state is called Idle Listening. This readiness is costly and useless in case of low network loads; for many radio modems, the idle state still consumes significant energy.

5. What is Cycled Receiver Approach?

In this approach, nodes spend most of their time in the sleep mode and wake up periodically to receive packets from other nodes. Specifically, a node A listens onto the channel during its listen period and goes back into sleep mode when no other node takes the opportunity to direct a packet to A.

6. Give the three phases of S-MAC protocol.

- SYNCH phase
- RTS phase
- CTS phase

7. List the advantages of Mediation Device Protocol.

- It does not require any time synchronization between the nodes.
- The protocol is asymmetric in the sense that most of the energy burden is shifted to the mediation device.

- The other nodes can be in the sleep state most of the time and have to spend energy only for the periodic beacons.

8. Write briefly about the Wake up radio Concept?

In this concept, several parallel data channels separated either in frequency (FDMA) or by choosing different codes in a CDMA schemes are available. A node wishing to transmit a data packet randomly picks one of the channels and performs a carrier – sensing operation. If the channel is busy, the node makes another random channel choice and repeats the carrier – sensing operation. After a certain number of unsuccessful trails, the node backs off for a random time and starts again. If the channel is idle, the node sends a wakeup signal to the intended receiver, indication both the receiver identification and the channel to use. The receiver wakes up its data transceiver, tune to the indicated channel, and the data packet transmission can proceed. Afterward, the receiver can switch its data transceiver back into sleep mode.

9. Give the features of PAMAS.

- Power Aware Multi-access with Signalling
- Overhearing avoidance mechanism
- Combines the busy-tone solution and RTS/CTS handshake
- Uses two channels: a data channel and a control channel

10. What are the disadvantages of Schedule base protocols?

- The setup and maintenance of schedules involves signalling traffic
- If a TDMA variant is employed, maintaining time synchronization involves some extra signalling traffic not easily adapted to different load situations on small time scales.
- The schedule of a node any require a significant amount of memory.

11. Give the phases of a LEACH round.

Each round in LEACH protocol is subdivided into

1. a setup phase and
2. a steady-state phase

12. What are the reasons of Hidden Terminal Problem?

The hidden-terminal problem occurs specifically for the class of Carrier Sense Multiple Access (CSMA) protocols, where a node senses the medium before starting to transmit a packet.

13. How CSMA based MAC work on Wireless Sensor Network?

In CSMA based MAC protocols, each sensor node uses constant period to contend channels; but back-off wait time can be random in order to eliminate repetitive collisions. An Adaptive Transmission Rate Control (ARC) is used to balance the traffic between sensor nodes using linear increase and multiplicative decrease method for initiative traffic in a node.

14. What are the goals of MAC protocols?

- Minimize Energy Consumption
- Overhearing
- Idle Listening
- Minimize the active time
- Eliminate packet collisions
- Minimize control packet overhead
- Prevent buffer overflow

15. What is PEGASIS?

PEGASIS is a hierarchical based routing algorithm used to address the overhead caused by the cluster formation in LEACH by constructing chains of nodes instead of clusters. The chain construction is performed according to a greedy algorithm, where nodes select their closest neighbours as next hops in the chain.

16. What is the purpose of Low duty cycle protocols?

It tries to avoid spending time in the idle state and to reduce the communication activities of a sensor node to a minimum.

17. What is duty cycle?

The ratio of the listen period length to the wakeup period length is also called the node's **duty cycle**.

18. What is exposed terminal problem?

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

19. Mention the design considerations for MAC protocols in wireless sensor networks.

- Balance of requirements
- Energy problems on the MAC layer
- Collisions
- Overhearing
- Protocol overhead
- Idle listening

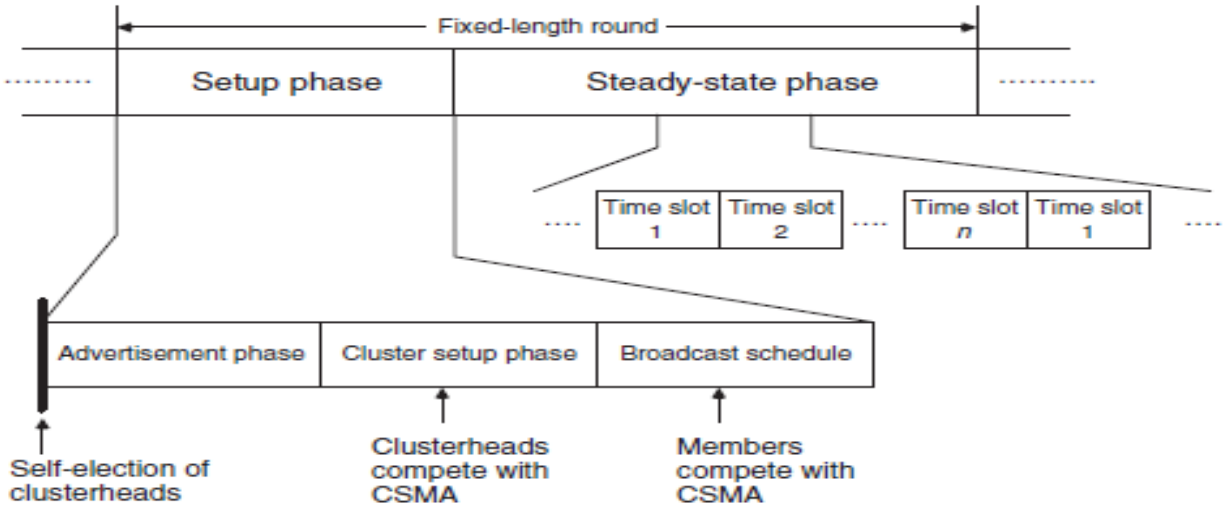
20. What are the mechanisms used in MAC layer?

The MAC protocol provides a channel of access and an addressing mechanism, so that each available node on the network may communicate with other nodes which are available – either on the same network, or on others.

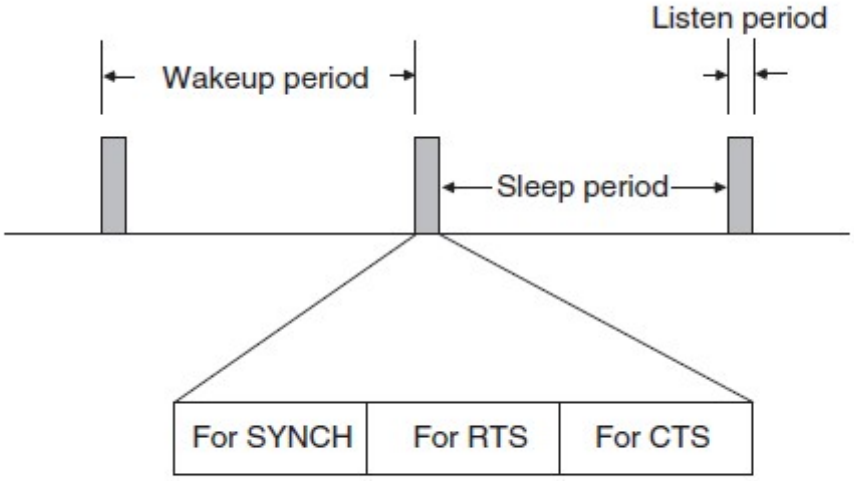
21. List the challenges of MAC Protocols for Sensor Networks.

- No single controlling authority, so global synchronization is difficult
- Power efficiency issue
- Frequent topology changes due to mobility and failure

22. Draw the frame structure of LEACH.



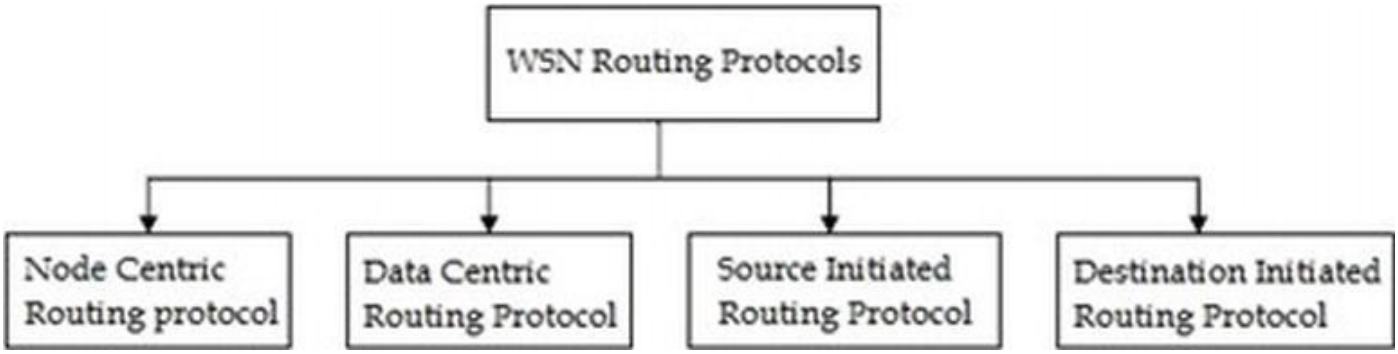
23. Draw the frame structure of SMAC.



24. What do you mean by LEACH protocol in wireless sensor network?

- The LEACH protocol (Low-energy Adaptive Clustering Hierarchy) assumes a dense sensor network of homogeneous, energy-constrained nodes, which shall report their data to a sink node.
- In LEACH, a TDMA based MAC protocol is integrated with clustering and a simple "routing" protocol.

25. How Routing Protocols are classified in WSN?



PART- B

1. Explain the design considerations for MAC protocols in wireless sensor networks.

Balance of requirements

- The importance of energy efficiency for the design of MAC protocols is relatively new and many of the "classical" protocols like ALOHA and CSMA contain no provisions toward this goal.
- Other typical performance figures like fairness, throughput, or delay tend to play a minor role in sensor networks.
- Further important requirements for MAC protocols are scalability and robustness against frequent topology changes.
- It is caused by nodes powering down temporarily to replenish their batteries by energy scavenging, mobility, deployment of new nodes, or death of existing nodes.

Energy problems on the MAC layer

- A nodes transceiver consumes a significant share of energy.
- The transceiver has four main states: transmitting, receiving, idling, or sleeping.
- Transmitting is costly, receive costs often have the same order of magnitude as transmit costs, idling can be significantly cheaper but also about as expensive as receiving, and sleeping costs almost nothing but results in a "deaf" node.
- Some **energy problems** and design goals are mentioned below:

Collisions

- Collisions incur useless receive costs at the destination node, useless transmit costs at the source node, and the prospect to expend further energy upon packet retransmission.
- Hence, collisions should be avoided, either by design (fixed assignment/TDMA or demand assignment protocols) or by appropriate collision avoidance/hidden-terminal procedures in CSMA protocols.

Overhearing

- Unicast frames have one source and one destination node.
- However, the wireless medium is a broadcast medium and all the source's neighbors that are in receive state hear a packet and drop it when it is not destined to them; these nodes overhear the packet.

Protocol overhead

- Protocol overhead is induced by MAC-related control frames like, RTS and CTS packets or request packets in demand assignment protocols.

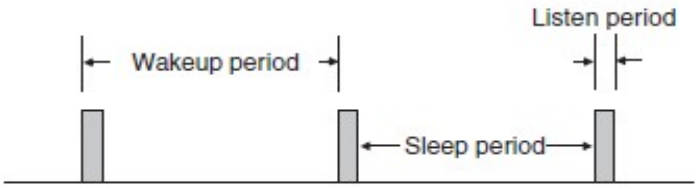
Idle listening

- A node being in idle state is ready to receive a packet but is not currently receiving anything.
- This readiness is costly and useless in case of low network loads; the idle state still consumes significant energy.
- Switching off the transceiver is a solution
- A design constraint somewhat related to energy concerns is the requirement for **low complexity operation**.
- Sensor nodes shall be simple and cheap and cannot offer plentiful resources in terms of processing power, memory, or energy.

- Therefore, computationally expensive operations like complex scheduling algorithms should be avoided.

2. Explain about Low duty protocols in WSN with neat diagram.

- **Low duty cycle protocols** try to avoid spending time in the idle state and to reduce the communication activities of a sensor node to a minimum.
- In an ideal case, the sleep state is left only when a node is about to transmit or receive packets.
- A concept for achieving this is called wakeup radio.
- In several protocols, a **periodic wakeup** scheme is used. Such schemes exist in different flavors. One is the **cycled receiver** approach is illustrated in below Figure.



- In this approach, nodes spend most of their time in the sleep mode and wake up periodically to *receive* packets from other nodes.
- Specifically, a node *A* listens onto the channel during its **listen period** and goes back into sleep mode when no other node takes the opportunity to direct a packet to *A*.
- A potential transmitter *B* must acquire knowledge about *A*'s listen periods to send its packet at the right time – this task corresponds to a *rendezvous*.
- This rendezvous can be accomplished by letting node *A* transmit a short beacon at the beginning of its listen period to indicate its willingness to receive packets.
- Another method is to let node *B* send frequent request packets until one of them hits *A*'s listen period and is really answered by *A*.
- However, in either case, node *A* only *receives* packets during its listen period.
- If node *A* itself wants to transmit packets, it must acquire the target's listen period.
- A whole cycle consisting of sleep period and listen period is also called a **wakeup period**.
- The ratio of the listen period length to the wakeup period length is also called the node's **duty cycle**.
- By choosing a small duty cycle, the transceiver is in sleep mode most of the time, avoiding idle listening and conserving energy.
- By choosing a small duty cycle, the traffic directed from neighboring nodes to a given node concentrates on a small time window (the listen period) and in heavy load situations significant competition can occur.
- Choosing a long sleep period induces significant **per-hop latency.** In the multihop case, the per-hop latencies add up and create significant end-to-end latencies.
- Sleep phases should not be too short lest the start-up costs outweigh the benefits.
- In other protocols like S-MAC, there is also a periodic wakeup but nodes can both *transmit and receive* during their wakeup phases.
- When nodes have their wakeup phases at the same time, there is no necessity for a node wanting to transmit a packet to be awake *outside* these phases to rendezvous its receiver.

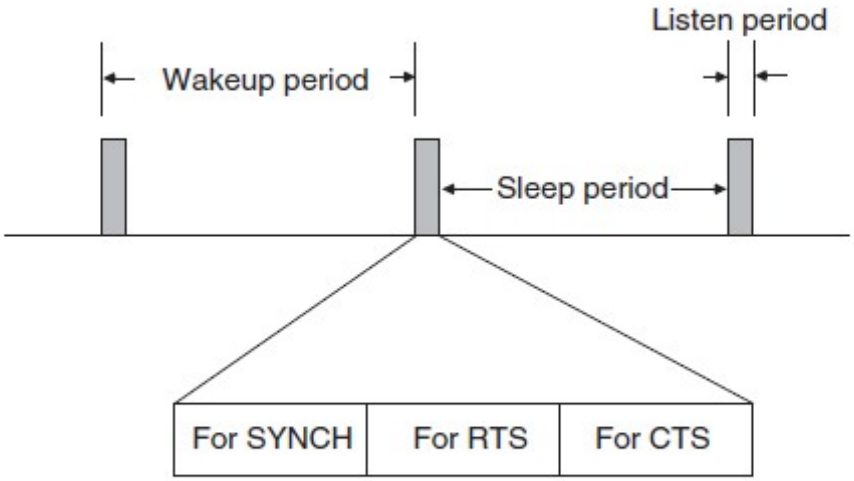
3. Explain about S-MAC protocol in WSN with neat diagram.

- The S-MAC (Sensor-MAC) protocol provides mechanisms to circumvent idle listening, collisions, and overhearing.

- S-MAC adopts a periodic wakeup scheme, that is, each node alternates between a fixed-length listen period and a fixed-length sleep period according to its **schedule.**
- The listen period of S-MAC can be used to receive *and transmit* packets.
- S-MAC attempts to coordinate the schedules of neighboring nodes such that their listen periods start at the same time.

Phases in listen period:

- A node *x*'s listen period is subdivided into three different phases:



1. First phase

- In the first phase (**SYNCH phase**), node *x* accepts SYNCH packets from its neighbors.
- In these packets, the neighbors describe their own schedule and *x* stores their schedule in a table (the **schedule table**).
- Node *x*'s SYNCH phase is subdivided into time slots and *x*'s neighbors contend according to a CSMA scheme with additional backoff.
- Each neighbor *y* wishing to transmit a SYNCH packet picks one of the time slots randomly and starts to transmit if no signal was received in any of the previous slots.
- In the other case, *y* goes back into sleep mode and waits for *x*'s next wakeup.
- In the other direction, since *x* knows a neighbor *y*'s schedule, *x* can wake at appropriate times and send its own SYNCH packet to *y* (in broadcast mode).
- It is not required that *x* broadcasts its schedule in every of *y*'s wakeup periods.
- However, for reasons of time synchronization and to allow new nodes to learn their local network topology, *x* should send SYNCH packets periodically. The according period is called **synchronization period**.

2. Second phase

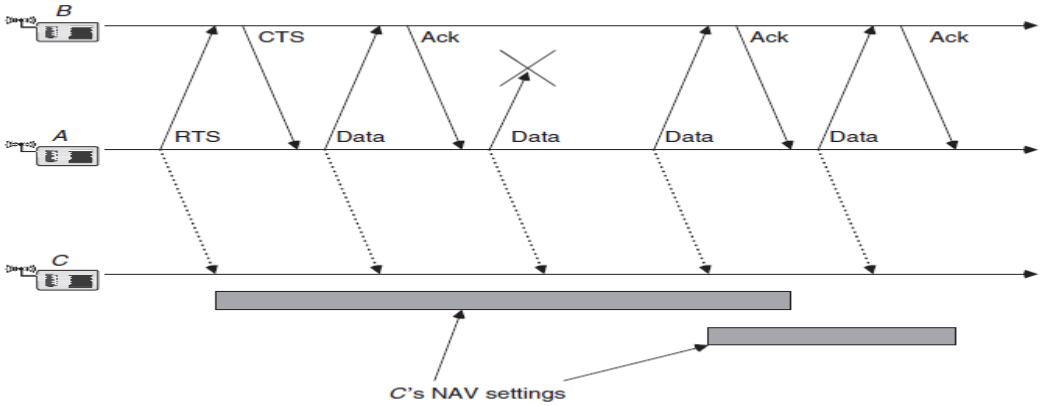
- In the second phase (**RTS phase**), *x* listens for RTS packets from neighboring nodes.
- In S-MAC, the RTS/CTS handshake is used to reduce collisions of data packets due to hidden-terminal situations.
- Again, interested neighbors contend in this phase according to a CSMA scheme with additional backoff.

3. Third Phase

- In the third phase (**CTS phase**), node *x* transmits a CTS packet if an RTS packet was received in the previous phase. After this, the packet exchange continues, extending into *x*'s nominal sleep time.

Working of S-MAC Protocol

- When competing for the medium, the nodes use the RTS/CTS handshake, including the virtual carrier-sense mechanism.
- When transmitting in a broadcast mode (for example SYNCH packets), the RTS and CTS packets are dropped and the nodes use CSMA with backoff.
- If we can arrange that the schedules of node *x* and its neighbors are synchronized, node *x* and all its neighbors wake up at the same time and *x* can reach all of them with a single SYNCH packet.
- The S-MAC protocol allows neighboring nodes to agree on the same schedule and to create **virtual clusters**.
- The clustering structure refers solely to the exchange of schedules; the transfer of data packets is not influenced by virtual clustering.
- The S-MAC protocol proceeds as follows to form the virtual clusters:
  - ✓ A node *x*, newly switched on, listens for a time of at least the synchronization period.
  - ✓ If *x* receives any SYNCH packet from a neighbor, it adopts the announced schedule and broadcasts it in one of the neighbors' next listen periods.
  - ✓ In the other case, node *x* picks a schedule and broadcasts it.
  - ✓ If *x* receives another node's schedule during the broadcast packet's contention period, it drops its own schedule and follows the other one.
  - ✓ It might also happen that a node *x* receives a different schedule after it already has chosen one, for example, because bit errors destroyed previous SYNCH packets.
  - ✓ If node *x* already knows about the existence of neighbors who adopted its own schedule, it keeps its schedule and in the future has to transmit its SYNCH and data packets according to both schedules.
  - ✓ On the other hand, if *x* has no neighbor sharing its schedule, it drops its own and adopts the other one.
  - ✓ Since there is always a chance to receive SYNCH packets in error, node *x* periodically listens for a whole synchronization period.



S-MAC includes a fragmentation scheme

- A series of fragments is transmitted with only one RTS/CTS exchange between the transmitting node *A* and receiving node *B*.
- After each fragment, *B* has to answer with an acknowledgment packet.
- All the packets (data, ack, RTS, CTS) have a duration field and a neighboring node *C* is required to set its NAV field accordingly.
- In S-MAC, the duration field of all packets carries the remaining length of the whole transaction, including all fragments and their acknowledgments. Therefore, the whole message shall be passed at once.
- If one fragment needs to be retransmitted, the remaining duration is incremented by the length of a data plus ack packet, and the medium is reserved for this prolonged time.

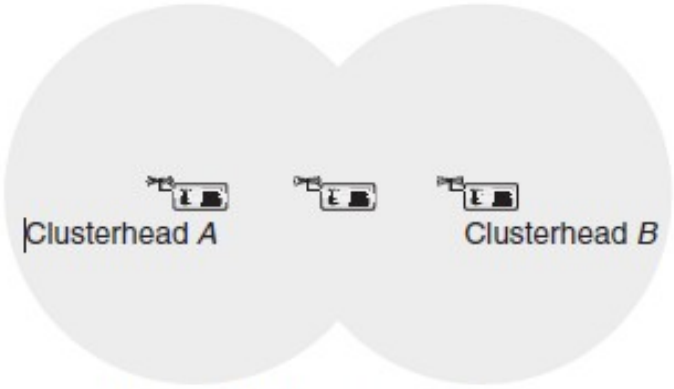
- However, there is the problem of how a nonparticipation node shall learn about the elongation of the transaction when he has only heard the initial RTS or CTS packets.

Drawbacks:

- It is hard to adapt the length of the wakeup period to changing load situations, since this length is essentially fixed, as is the length of the listen period.

4. Explain the operation of LEACH protocol.

- The LEACH protocol (Low-energy Adaptive Clustering Hierarchy) assumes a dense sensor network of homogeneous, energy-constrained nodes, which shall report their data to a sink node.
- In LEACH, a TDMA based MAC protocol is integrated with clustering and a simple "routing" protocol.
- LEACH partitions the nodes into **clusters** and in each cluster a dedicated node, the **cluster head**, is responsible for creating and maintaining a TDMA schedule; all the other nodes of a cluster are **member nodes**.
- To all member nodes, TDMA slots are assigned, which can be used to exchange data between the member and the cluster head; there is no peer-to-peer communication.
- With the exception of their time slots, the members can spend their time in sleep state.
- The cluster head aggregates the data of its members and transmits it to the sink node or to other nodes for further relaying.
- Since the sink is often far away, the cluster head must spend significant energy for this transmission.
- For a member, it is typically much cheaper to reach the cluster head than to transmit directly to the sink.
- The cluster heads role is energy consuming since it is always switched on and is responsible for the long-range transmissions.
- If a fixed node has this role, it would burn its energy quickly, and after it died, all its members would be "headless" and therefore useless.
- Therefore, this burden is rotated among the nodes. Specifically, each node decides independent of other nodes whether it becomes a cluster head, and therefore there is no signalling traffic related to cluster head election.
- This decision takes into account when the node served as cluster head the last time, such that a node that has not been a cluster head for a long time is more likely to elect itself than a node serving just recently.
- The protocol is round based, that is, all nodes make their decisions whether to become a cluster head at the same time and the nonclusterhead nodes have to associate to a cluster head subsequently.
- The non-cluster heads choose their cluster head based on received signal strengths.
- The network partitioning into clusters is time variable and the protocol assumes global time synchronization.
- After the clusters have been formed, each cluster head picks a random CDMA code for its cluster, which it broadcasts and which its member nodes have to use subsequently.
- This avoids a situation where a border node belonging to cluster head *A* distorts transmissions directed to cluster head *B*.

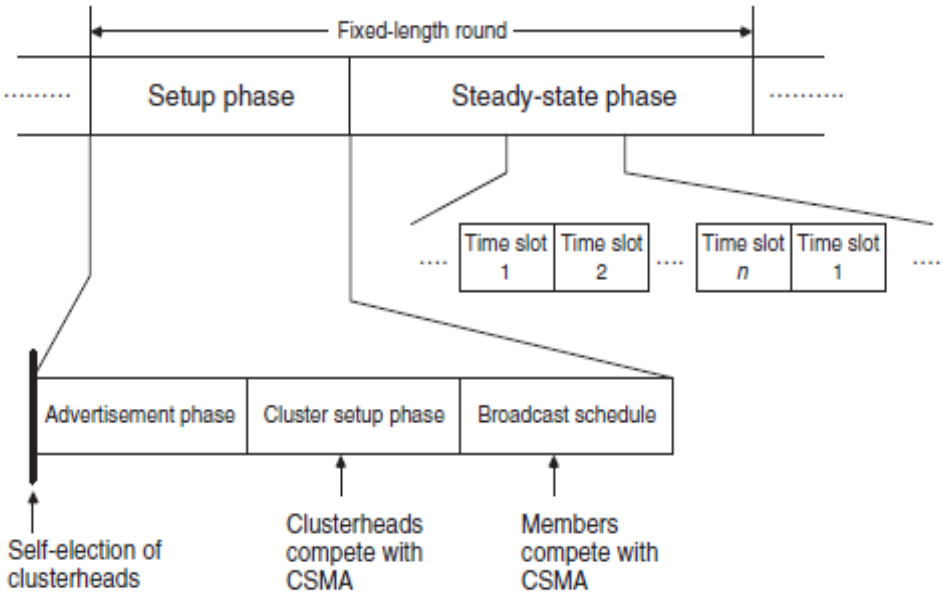


Stages of LEACH protocol:

- The protocol is organized in **rounds** and each round is subdivided into a setup phase and a steady-state phase.

Setup Phase:

- The **setup phase** starts with the self-election of nodes to clusterheads.
- In the following **advertisement phase**, the clusterheads inform their neighborhood with an advertisement packet.
- The clusterheads contend for the medium using a CSMA protocol with no further provision against the hidden-terminal problem.
- The nonclusterhead nodes pick the advertisement packet with the strongest received signal strength.
- In the following cluster-setup phase, the members inform their clusterhead ("join"), again using a CSMA protocol.
- After the cluster setup-phase, the clusterhead knows the number of members and their identifiers.
- It constructs a TDMA schedule, picks a CDMA code randomly, and broadcasts this information in the broadcast schedule subphase.



Steady state phase:

- After this, the TDMA steady-state phase begins. Because of collisions of advertisement or join packets, the protocol cannot guarantee that each non clusterhead node belongs to a cluster.
- However, it can guarantee that nodes belong to at most one cluster.

- The clusterhead is switched on during the whole round and the member nodes have to be switched on during the setup phase and occasionally in the steady-state phase, according to their position in the cluster's TDMA schedule.

Drawback:

- unable to cover large geographical areas because a clusterhead two miles away from the sink likely does not have enough energy to reach the sink at all, not to mention achieving a low BER.

Solution:

- If it can be arranged that a clusterhead can use other clusterheads for forwarding, this limitation can be mitigated.

5. Write short notes on advantages and disadvantages of scheduled based protocols.

Advantages:

- Schedule-based protocols that do not explicitly address idle listening avoidance but do so implicitly, for example, by employing TDMA schemes, which explicitly assign transmission and reception opportunities to nodes and let them sleep at all other times.
- In schedule-based protocols is that transmission schedules can be computed such that no collisions occur at receivers and hence no special mechanisms are needed to avoid hidden-terminal situations.

Disadvantages:

- First, the setup and maintenance of schedules involves signalling traffic, especially when faced to variable topologies.
- Second, if a TDMA variant is employed, time is divided into comparably small slots, and both transmitter and receiver have to agree to slot boundaries to actually meet each other and to avoid overlaps with other slots, which would lead to collisions.
- However, maintaining time synchronization involves some extra signaling traffic.
- Third drawback is that such schedules are not easily adapted to different load situations on small timescales. Specifically, in TDMA, it is difficult for a node to give up unused time slots to its neighbors.
- Fourth drawback is that the schedule of a node may require a significant amount of memory, which is a scarce resource in several sensor node designs.
- Finally, distributed assignment of conflict-free TDMA schedules is a difficult problem in itself.

6. Describe about the SPIN and PEGASIS routing with the help of neat diagram. Give its advantages and disadvantages.

- SPIN is abbreviation of sensor protocol for information via negotiation.
- This protocol is defined to use to remove the deficiency like flooding and gossiping that occurs in other protocols.
- The main idea is that the sharing of data, which is sensed by the node, might take more resources as compare to the meta-data, which is just a descriptor about the data sensed, by the node.
- The resource manager in each node monitors its resources and adapts their functionality accordingly.

- Three messages namely ADV, REQ and DATA are used in SPIN.
- The node broadcast an ADV packet to all the other nodes that it has some data.
- This advertising node ADV message includes attributes of the data it has.
- The nodes having interests in data, which the advertising node has requested by sending REQ message, to the advertising node.
- On receiving the REQ message the advertising node send data to that node.
- This process continues when the node on reception of data generate an ADV message and send it.

SPIN Protocol Example

- A sends an ADV message to B

- B sends a REQ listing all of the data it would like to acquire.

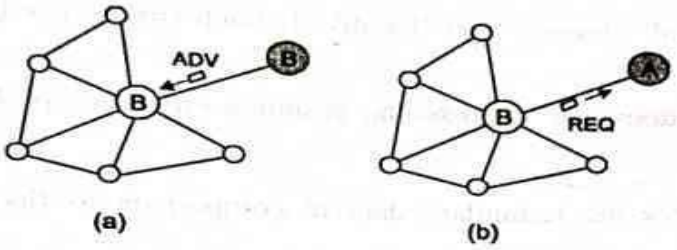


Fig. 2.22 Node A advertise

- If node B had its own data, it could aggregate this with the data of node A and advertise.

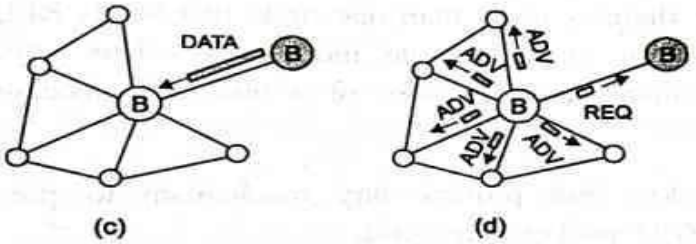


Fig. 2.23 Data Request

- Nodes need not respond to every message

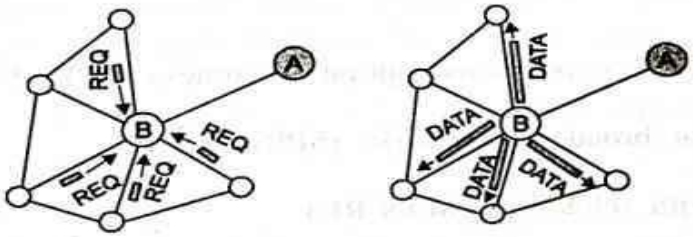


Fig. 2.24 Data flooding

- The basic operation explained in above Example is referred to as the point-to-point SPIN protocol (SPIN-PP).

Advantages

- Topological changes are localized Each node needs to know only its neighbors.
- SPIN-PP does not address the resource-blindness problem of conventional flooding
- SPIN halves the redundant data in comparison to flooding

Disadvantages

- It cannot guarantee data delivery
- SPIN NOT good for applications that need reliable data delivery.
- Whenever there is more than one node that sends REQ packets, the DATA packet is sent to each node individually. This approach is a waste of resources since each neighbor of a node can receive the packet in each unicast.
- SPIN-PP does not provide any mechanism to prevent collisions when multiple REQ packets are send.
- In addition to SPIN-PP, several variations have been proposed to address some of the disadvantages of SPIN-PP.
- They are
  - SPIN with energy consumption awareness (SPIN-EC)
  - SPIN for broadcast networks (SPIN-BC)
  - SPIN with reliability (SPIN-RL).
- Although the DATA packet transmission is limited to nodes that provide interest, energy consumption is still a concern in SPIN -PP.
- SPIN-EC addresses this through a simple energy conservation heuristic such that whenever the residual energy of a node is lower than a threshold, the node does not participate in the protocol operation, i.e., it does not send a REQ packet if it does not have enough energy to transmit the REQ packet and receive a DATA packet.

- Since node participation is dependent on the residual energy.
- If a node has plenty of energy SPIN-EC behaves like SPIN-PP.
- The two drawbacks of waste of resources since each neighbor of a node can receive the packet in each unicast and no mechanism to prevent collisions can be addressed through SPIN-BC, which is developed for broadcast networks.
- In contrast to SPIN-PP, SPIN-BC introduces a randomized backoff mechanism for the nodes before transmitting a REQ packet.
- As a result, if a node has an interest in a packet but hears a REQ packet related to that particular packet, it drops its REQ packet and waits for the DATA packet.
- Upon receiving a REQ packet, a transmitter node broadcasts a single DATA packet which can be received by all the interested neighbors.
- As a result, SPIN-BC decreases the energy consumption and overhead caused by multiple interested neighbors.
- SPIN-RL provides a reliability mechanism to the SPIN-BC protocol such that if a node receives an ADV packet but does not receive a DATA packet due to wireless channel errors it requests the DATA packet from the neighbors that may have received the DATA packet.
- Moreover, SPIN-RL limits the retransmission period of the nodes such that they do not retransmit a DATA packet before a specified period.

POWER-Efficient Gathering in Sensor Information Systems (PEGASIS)

- PEGASIS aims to address the overhead caused by the cluster formation in LEACH by constructing chains of nodes instead of clusters.
- The chain construction is performed according to a greedy algorithm, where nodes select their closest neighbors as next hops in the chain.
- It is assumed that the nodes have a global knowledge of the network and the chain construction starts from the nodes that are farthest from the sink.
- Communication in the chain is performed sequentially such that each node within a chain aggregates data from its neighbor until all the data are aggregated at one of the sensor nodes, i.e., chain leader.
- The chain leader controls the communication order by passing a token among the nodes.

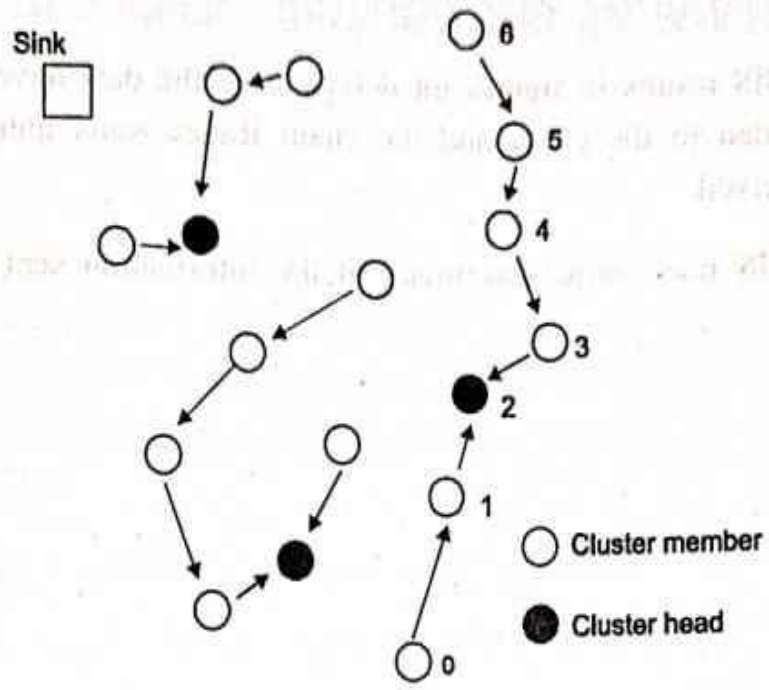


Fig. 2.29 Chain structure of PEGASIS

- An example of chain communication is shown in Fig. 2.29.
- The chain leader in this example is node 2.
- Node 2 first passes the token to node 0 to initiate communication.
- Node 0 transmits its data to node 1, which aggregates these data with its own to create a packet of the same length.
- This packet is transmitted to node 2.
- Once node 2 receives the packet from node 1, it passes the token to the other end of the chain, i.e., node 6.
- Information from nodes 6, 5, 4, and 3 is also aggregated and sent to node 2 in the same fashion.
- Upon receiving the aggregated information in the chain, node 2 uses a single hop communication to transmit the data to the sink.

Advantages

- PEGASIS provides performance enhancement of 100-300% over LEACH in energy consumption.
- Limited overhead

Disadvantages

- PEGASIS results in significant delays since the data have to be sequentially transmitted in the chain and the chain leader waits until all the messages are received.
- PEGASIS may cause inaccuracy in the information sent to the sink.

7. What are the important classes of MAC protocols and explain it in detail?

Important classes of MAC protocols

A huge number of (wireless) MAC protocols have been devised during the last thirty years. They can be roughly classified into the following classes:

- Fixed assignment protocols
- Demand assignment protocols
- Random access protocols

Fixed assignment protocols

- In this class of protocols, the available resources are divided between the nodes such that the resource assignment is long term and each node can use its resources exclusively without the risk of collisions.
- Long term means that the assignment is for durations of minutes, hours, or even longer, as opposed to the short-term case where assignments have a scope of a data burst, corresponding to a time horizon of perhaps (tens of) milliseconds.

- Typical protocols of this class are **TDMA, FDMA, CDMA, and SDMA.**
- The **Time Division Multiple Access (TDMA)** scheme subdivides the time axis into fixed-length superframes and each superframe is again subdivided into a fixed number of time slots. These time slots are assigned to nodes exclusively and hence the node can transmit in this time slot periodically in every superframe. TDMA requires tight time synchronization between nodes to avoid overlapping of signals in adjacent time slots.
- In **Frequency Division Multiple Access (FDMA)**, the available frequency band is subdivided into a number of subchannels and these are assigned to nodes, which can transmit exclusively on their channel. This scheme requires frequency synchronizations to renegotiate the assignment of resources to nodes.
- In **Code Division Multiple Access (CDMA)** schemes, the nodes spread their signals over a much larger bandwidth than needed, using different codes to separate their transmissions. The receiver has to know the code used by the transmitter; all parallel transmissions using other codes appear as noise. Crucial to CDMA is the code management
- Finally, in **Space Division Multiple Access (SDMA)**, the spatial separation of nodes is used to separate their transmissions. SDMA requires arrays of antennas and sophisticated signal processing techniques and cannot be considered a candidate technology for WSNs.

Demand assignment protocols

- In demand assignment protocols, the exclusive allocation of resources to nodes is made on a short-term basis, typically the duration of a data burst. This class of protocols can be broadly subdivided into centralized and distributed protocols.
- In central control protocols the nodes send out requests for bandwidth allocation to a central node that either accepts or rejects the requests.
- In case of successful allocation, a confirmation is transmitted back to the requesting node along with a description of the allocated resource, for example, the numbers and positions of assigned time slots in a TDMA system and the duration of allocation.

- The node can use these resources exclusively.
- The submission of requests from nodes to the central station is often done contention based, that is, using a random access protocol on a dedicated (logical) signaling channel.
- Another option is to let the central station poll its associated nodes.
- In addition, the nodes often piggyback requests onto data packets transmitted in their exclusive data slots, thus avoiding transmission of separate request packets.
- The central node needs to be switched on all the time and is responsible for resource allocation.
- Resource deallocation is often done implicitly: when a node does not use its time slots any more, the central node can allocate these to other nodes.
- An example of distributed demand assignment protocols are **token- passing protocols like IEEE 802.4 Token Bus** .
- The right to initiate transmissions is tied to reception of a small special token frame.
- The token frame is rotated among nodes organized in a logical ring on top of a broadcast medium.
- Special ring management procedures are needed to include and exclude nodes from the ring or to correct failures like lost tokens.
- Token-passing protocols have also been considered for wireless, but they tend to have problems with the maintenance of the logical ring in the presence of significant channel errors.
- In addition, since token circulation times are variable, a node must always be able to receive the token to avoid breaking the logical ring. Hence, a nodes transceiver must be switched on most of the time.

- In addition, maintaining a logical ring in face of frequent topology changes is not an easy task and involves significant signaling traffic besides the token frames themselves.

Random access protocols

- The nodes are uncoordinated, and the protocols operate in a fully distributed manner.

- Random access protocols often incorporate a random element, for example, by exploiting random packet arrival times, setting timers to random values, and so on.

- One of the first and still very important random access protocols is the **ALOHA or slotted ALOHA protocol**, developed at the University of Hawaii.

- In the **pure ALOHA protocol**, a node wanting to transmit a new packet transmits it immediately. There is no coordination with other nodes and the protocol thus accepts the risk of collisions at the receiver.

- To detect this, the receiver is required to send an immediate acknowledgment for a properly received packet.

- The transmitter interprets the lack of an acknowledgment frame as a sign of a collision, backs off for a random time, and starts the next trial. ALOHA provides short access and transmission delays under light loads; under heavier loads, the number of collisions increases, which in turn decreases the throughput efficiency and increases the transmission delays.

- In the class of CSMA protocols, a transmitting node tries to be respectful to ongoing transmissions.

- First, the node is required to listen to the medium; this is called **carrier sensing**. If the medium is found to be idle, the node starts transmission.

- If the medium is found busy, the node defers its transmission for an amount of time determined by one of several possible algorithms.

- For example, in non persistent CSMA, the node draws a random waiting time, after which the medium is sensed again.
- Before this time, the node does not care about the state of the medium.
- In different persistent CSMA variants, after sensing that the medium is busy, the node awaits the end of the ongoing transmission and then behaves according to a backoff algorithm.
- In many of these backoff algorithms, the time after the end of the previous frame is subdivided into time slots.
- In p-persistent CSMA, a node starts transmission in a time slot with some probability p and with probability 1-p it waits for another slot. If some other node starts to transmit in the meantime, the node defers and repeats the whole procedure after the end of the new frame.
- A small value of p makes collisions unlikely, but at the cost of high access delays.
- The converse is true for a large value of p.
- Carrier-sense protocols are susceptible to the hidden-terminal problem since interference at the receiver cannot be detected by the transmitter.
- This problem may cause packet collisions.
- The RTS/CTS handshake as used in IEEE 802.11 is based on the MACAW protocol.
- It uses only a single channel and two special control packets.
- Suppose that node B wants to transmit a data packet to node C as shown in Fig. 2.2.
- After B has obtained channel access (for example after sensing the channel as idle), it sends a Request To Send (RTS) packet to C, which includes a duration field indicating the remaining length of the overall transaction (i.e., until the point where B would receive the acknowledgment for its data packet).
- If C has properly received the RTS packet, it sends a Clear To Send (CTS) packet, which again contains a duration field.
- When B receives the CTS packet, it starts transmission of the data packet and finally C answers with an acknowledgment packet.

- The acknowledgment is used to tell B about the success of the transmission; lack of acknowledgment is interpreted as collision (the older MACA protocol lacks the acknowledgment).

- Any other station A or D hearing either the RTS, CTS, data or acknowledgment packet sets an internal timer called **Network Allocation Vector(NAV)** to the remaining duration indicated in the respective frame and avoids sending any packet as long as this timer is not expired.

- Specifically, nodes A and D send no CTS answer packets even when they have received a RTS packet correctly. This way, the ongoing transmission is not distorted.

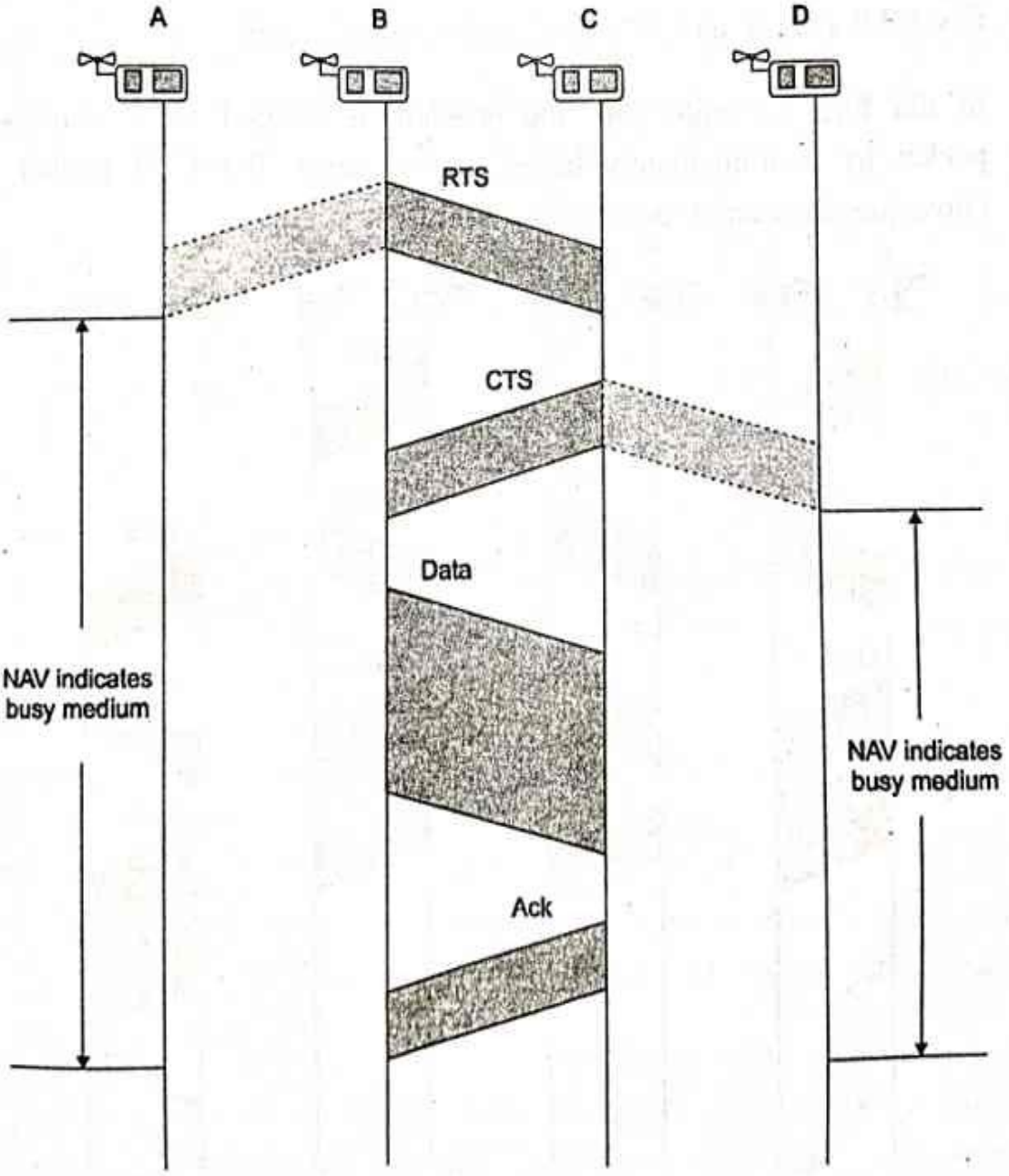


Fig. 2.2 RTS/CTS handshake in IEEE 802.11

- In the left part of the Fig. 2.3, nodes A and B run the RTS-CTS-Data-Ack sequence, and B's CTS packet also reaches node C.
- However, at almost the same time, node D sends an RTS packet to C, which collides at node C with B's CTS packet.
- This way, C has no chance to decode the duration field of the CTS packet and to set its NAV variable accordingly.
- After its failed RTS packet, D sends the RTS packet again to C and C answers with a CTS packet. Node C is doing so because it cannot hear A's ongoing transmission and has no proper NAV entry.
- C's CTS packet and A's data packet collide at B.
- In the Fig. 2.3 right part, the problem is created by C starting its RTS packet to D immediately before it can sense B's CTS packet, which C consequently cannot decode properly.

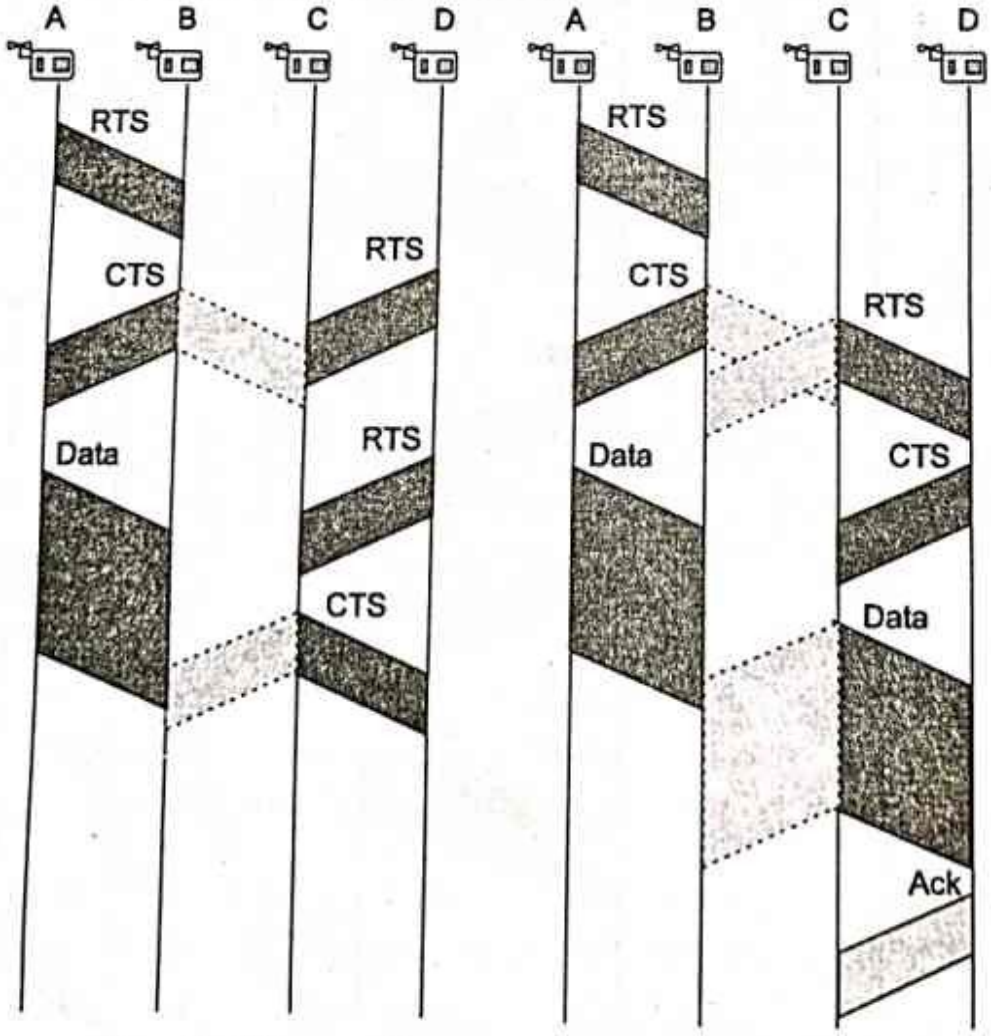


Fig. 2.3 Two problems in RTS/CTS handshake