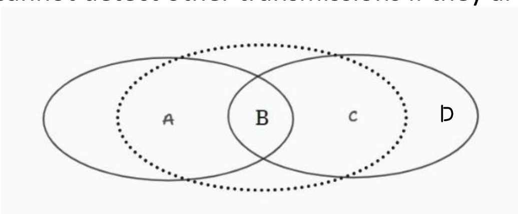
1. "CSMA/CD can't be applied in the MAC layer of wireless communication" - critically comment on the statement. describing the issues with proper examples.

In wired networks, CSMA/CD (Carrier Sense Multiple Access with Collision Detection) operates effectively because devices can listen to the channel while transmitting. If a collision occurs (i.e., two devices transmit simultaneously), both devices can detect it by sensing the voltage levels on the wire. However, in wireless networks, devices cannot transmit and receive simultaneously on the same channel due to hardware limitations. This means that when a device is transmitting, it cannot detect any incoming signals, making collision detection impossible.

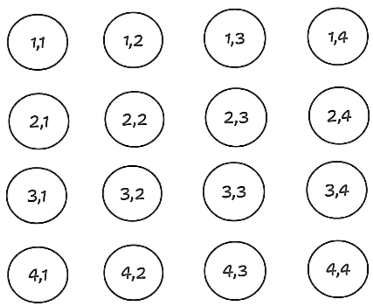
- Hidden Terminal problem
  Wireless nodes cannot detect other transmissions if they are out of range. For example:



  - Consider three nodes A, B, and C, where A and C are out of range of each other, but both are in range of B.
  - A is transmitting to BBB and C also starts transmitting to B
  - C sense a free medium (carrier sense fails)
  - The collision occurs at B but A and C can`t retrieve the collision (CD fails)
  - Here C is Hidden from A.
  -
- Exposed Terminal Problem
  - B sends to A , C can detect this transmission .
  - C wants to send data to D .
  - C sense a busy medium and will wait unnecessarily till B->A ends
  - Here B is exposed to C .

2. Suppose 16 wireless devices are connected in a grid numbered (1,1) to (4,4). Determine hidden nodes and exposed nodes if the node (2,2) wants to send data to node (2,3)

Assumptions: Each node can communicate with other nodes within a 1-hop radius (directly adjacent horizontally, vertically, or diagonally).



The nodes in communication range of (2,2) are:

- (1,1), (1,2), (1,3)
- (2,1), **(2,3)** (intended recipient),
- (3,1), (3,2), (3,3).

Hidden nodes are those that can interfere with the receiver (2,3) but are **not within the range of the sender** (2,2).

Nodes in range of (2,3):
(1,2), (1,3), (1,4),
(2,2) (sender), (2,4),
(3,2), (3,3), (3,4)

Nodes hidden from (2,2) : (1,4),(2,4),(3,4)

Exposed nodes are those that are in the range of the sender (2,2) but are **not interfering with the receiver's transmission**.

Exposed Nodes: (1,1), (1,2), (2,1), (3,1), (3,2).

3. Determine the length of the Aluminium plate needed to generate a Wireless signal of frequency 98MHz using a Half-wave dipole antenna.

"half-wave" term means that the length of this dipole antenna is equal to a half-wavelength at the frequency of operation.

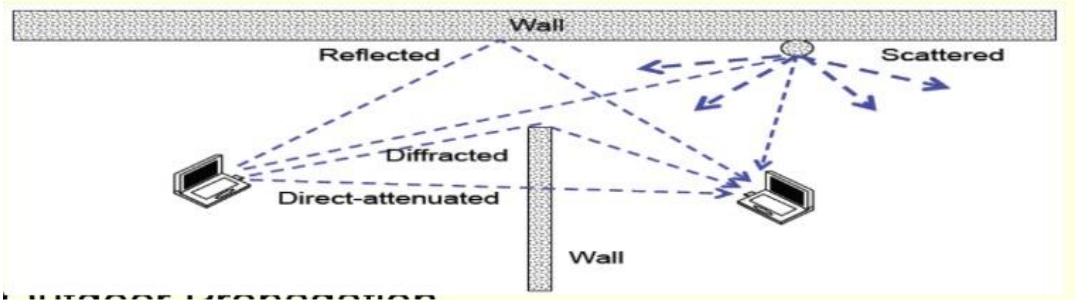
$$\boldsymbol{l = \frac{\lambda}{2}}$$

$$\boldsymbol{\lambda = \frac{c}{f}}$$

Given : f = 98 MHz = $98*10^6$ Hz

$$\boldsymbol{\lambda = \frac{3*10^8}{98*10^6} = 3.062} \qquad \boldsymbol{l = \frac{3.062}{2} = 1.54\, meters}$$

4. with a suitable diagram , describe multipath propagation of wireless signals in indoor environment

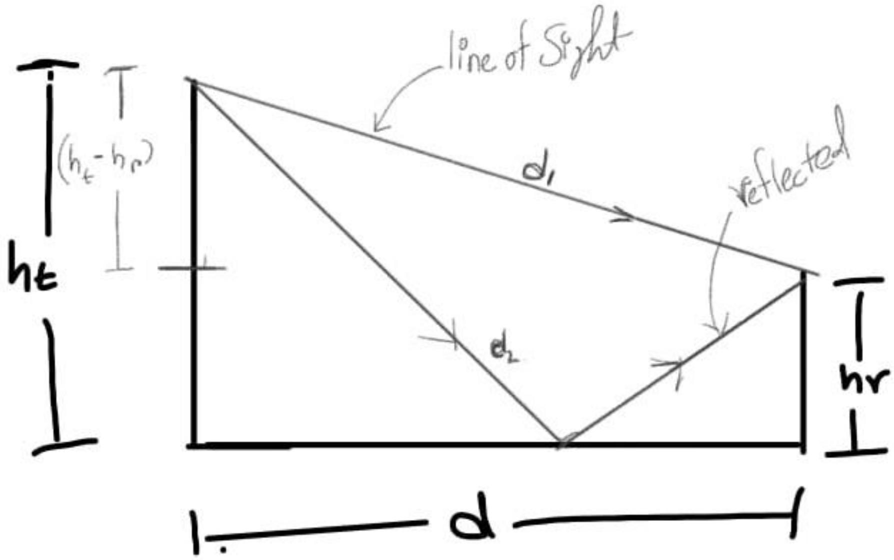


<u>Multipath Propagation</u>

- Reflection: Reflection occurs when a wireless signal encounters a large surface, such as walls, floors, or ceilings, and bounces back. This creates additional paths for the signal to reach the receiver. Here the surface is large enough as compared to the wavelength of the signal.
- Diffraction: Diffraction happens when a signal bends around obstacles (like furniture or walls) that partially block its path. This bending allows the signal to reach areas that are not in a direct line of sight. Here the surface is large enough as compared to the wavelength of the signal.
- Scattering occurs when a signal encounters small objects like rough surfaces, edges, or small obstacles (e.g., decorations or foliage). These objects cause the signal to spread in multiple directions. Here surface size is on the order of the wavelength of the signal or less.

5. State and derive 2-way path loss model.

The two-way path loss model accounts for the attenuation of signal power as it propagates between the transmitter and receiver and back again, incorporating both free-space path loss and additional losses due to reflection, scattering, and other environmental factors.



$$d_1 = \sqrt{(h_t-h_r)^2 + d^2} = d\sqrt{\left(\frac{h_t-h_r}{d}\right)^2+1}$$

$$d_2 = \sqrt{(h_t+h_r)^2 + d^2} = d\sqrt{\left(\frac{h_t+h_r}{d}\right)^2+1}$$

$$\Delta d = d_2 - d_1 = d\left(\sqrt{\left(\frac{h_t+h_r}{d}\right)^2+1} - \sqrt{\left(\frac{h_t-h_r}{d}\right)^2+1}\right)$$

$$(1+x)^n = 1 + nx + \frac{n(n+1)}{2!}x^2 + \dots$$

$$\approx 1 + nx \quad \text{if} \quad x \ll 1$$

So, $$\sqrt{\left(\frac{h_t+h_r}{d}\right)^2+1} = \left(1+\left(\frac{h_r+h_t}{d}\right)^2\right)^{1/2}$$

$$= 1 + \frac{1}{2}\left(\frac{h_t+h_r}{d}\right)^2$$

$$\Delta d = d\left[1+\frac{1}{2}\left(\frac{h_t+h_r}{d}\right)^2 - 1 - \frac{1}{2}\left(\frac{h_t-h_r}{d}\right)^2\right]$$

$$= d\left[\frac{2h_th_r}{d^2}\right] = \frac{2h_th_r}{d}$$

Now Phase difference $\Delta\phi$ for Δd.

$$\Delta\phi = \frac{2\pi \Delta d}{\lambda} \simeq \frac{4\pi h_t h_r}{\lambda d}$$

Now,

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2 \times \left|1 - e^{-j\Delta\phi}\right|^2$$

$$= P_t G_t G_r \left(\frac{\lambda}{4\pi\lambda}\right)^2 \times \left|1-(1-j\Delta\phi)\right|^2$$

$$= P_t G_t G_r \left(\frac{\lambda}{4\pi\lambda}\right)^2 \times \Delta\phi^2$$

$$= P_t G_t G_r \left(\frac{\lambda}{4\pi\lambda}\right)^2 \left(\frac{4\pi h_t h_r}{\lambda d^2}\right)^2$$

$$= P_t G_t G_r \left(\frac{h_t h_r}{d^2}\right)^2$$

6. State Friss Free Space path loss model and Two-Ray path loss model

- The **Friis Free Space Path Loss Model** describes the signal attenuation between a transmitter and receiver in a clear, unobstructed environment. It assumes no interference, reflection, or diffraction and is given by the equation:

$$PL\ (dB) = -10\ log_{10}[\ G_t\, G_r\ \left(\frac{\lambda}{4\pi d}\right)^2\ ]$$

- The **Two-Ray Path Loss Model** improves upon the free space model by considering both the direct line-of-sight path and a reflected path from the ground. It is especially useful for terrestrial communication scenarios.

$$P_r = P_t\, G_t\, G_r\, \left(\frac{h_t\, h_r}{d^2}\right)^2$$

7. How can we convert a wireless signal from an omnidirectional antenna to a directional one?

- **Omnidirectional Antenna:** Radiates signals equally in all directions, providing a 360-degree coverage pattern. Ideal for applications requiring broad coverage.
- **Directional Antenna:** Focuses the signal in a specific direction, enhancing range and strength in that targeted area. Suitable for point-to-point communication.

→ **Methods to Convert Omnidirectional to Directional**

I. **Reflector Design:** One practical method is to create a reflector behind the omnidirectional antenna. This can be done using materials like aluminium foil or metal sheets, which can redirect the signal in a desired direction.

II. **Faraday Cage Concept:** Enclosing the omnidirectional antenna in a cylindrical container (like a Pringles can) with an opening on one side can help narrow the radiation pattern. The antenna is placed at one end of the cylinder, allowing signals to escape primarily through the opening.

8. State the Generalized path loss model ?

The generalized path loss model provides a formula to describe the decrease in signal power as it propagates through space. This model accounts for the variation in propagation conditions and is widely used to approximate signal behaviour in various environments.

The **generalized path loss model** is expressed as:

$$\boldsymbol{P_r(d) = P_t K \left[\frac{d_0}{d}\right]^{\gamma}}$$

Routing Protocols

9. What is Flooding in Computer Network?

Flooding in networking is a method where every incoming data packet is forwarded to all connected nodes except the one from which it was received. This process continues until the packet reaches its destination or a specified condition is met, such as a hop count limit.

Key Features of Flooding:

- **No Routing Table Required**: Flooding eliminates the need for pre-configured routes.
- **High Reachability**: Ensures that packets are delivered to all nodes in the network.
- **Broadcasting Nature**: Suitable for scenarios requiring mass communication.

Explanation of Flooding Mechanism

Step	Action
1. **Packet Entry**	A data packet enters the network.
2. **Broadcasting**	The packet is forwarded to all neighboring nodes.
3. **Loop Prevention**	Hop count or unique identifiers are used to prevent packet loops.
4. **Packet Delivery**	The packet reaches its intended destination or stops after limits.

Disadvantage: A large number of duplicate pkts broadcasted

Sequence number in flooding

Each packet is assigned a unique sequence number. When a node receives a packet:

- It checks the sequence number against the packets it has already processed.
- If the sequence number is new, the node processes and forwards the packet.
- If the sequence number is a duplicate, the node discards the packet.

Example with Sequence Numbers:

- Node A sends a packet to its neighbours with a sequence number SN=1.
- Neighbor B receives the packet, processes it, and forwards it to its neighbours.
- When Node A receives the same packet back from B, it discards it because SN=1 has already been processed.

Hop Counting

Each packet is assigned a **hop count** (TTL: Time-to-Live), which represents the maximum number of hops the packet can travel. The hop count is decremented by 1 at each node, and when it reaches zero, the packet is discarded.

Example with Hop Count:

- Node AAA sends a packet with a hop count of 3.
- Neighbor BBB receives the packet, decrements the hop count to 2, and forwards it.
- Neighbor CCC receives the packet, decrements the hop count to 1, and forwards it.
- Neighbor DDD receives the packet, decrements the hop count to 0, and discards it.

10. "Flooding is a simple strategy for distributing data to one specific node or all remaining nodes in a network." How do sequence numbers contribute to reducing unnecessary transmissions? Are sequence numbers alone sufficient? If not, what other information is needed to use them correctly?

How seq. number helps : (see previous answer)

Are Sequence number alone sufficient ?

- NO, we need another parameter called metric. This matric can be something like number of Hops to destination.
- Upon receiving multiple advertisement packets , a node select route with higher sequence number , but if two advertisement have same sequence number then choose the route with better metric (when metric = #hops to destination , the route having less hops is better choice)

11. Differentiate broadcasting from border-casting

Broadcasting

Definition: Broadcasting is a communication method where a message is sent from one source to all possible recipients within a network or area. It is characterized by its one-to-all approach, meaning that the same message is delivered to every recipient without targeting specific individuals or groups.

Border-casting

Definition: Border-casting refers to a targeted form of broadcasting that focuses on a specific geographic area or demographic group.

Broadcasting	Border-Casting
Transmitting a message to **all nodes** in the network.	Transmitting a message to **specific boundary nodes.**
Network-wide communication.	Targeted communication limited to border nodes.
All nodes in the network, without exception.	Only nodes on the edges or borders of the network.
Inefficient for targeted communication; high redundancy.	More efficient for specific tasks, as it reduces redundancy.
General announcements, such as routing table updates.	Applications like distributing control information to boundary nodes in hierarchical routing.

12. What advantage and disadvantage does multipath routing have ?

Multipath routing is a technique used in networking where multiple paths are established between a source and a destination.

Advantages of Multipath Routing

- **Increased Reliability**: By utilizing multiple paths, the network can maintain communication even if one or more paths fail. This redundancy enhances fault tolerance and ensures continuous data transmission.
- **Load Balancing**: Multipath routing allows for traffic to be distributed across several paths, preventing any single path from becoming a bottleneck. This load balancing can improve overall network throughput and reduce congestion.
- **Higher Bandwidth**: The aggregate bandwidth of the network can be increased by using multiple paths simultaneously. This is particularly beneficial in high-demand scenarios where a single path may not provide sufficient bandwidth.
- **Reduced Latency**: In some cases, using multiple paths can lead to lower end-to-end latency, as packets can take the shortest available routes concurrently.
- **Improved Resource Utilization**: By spreading traffic across various paths, multipath routing can make better use of available network resources, leading to more efficient operation.

Disadvantages of Multipath Routing

- **Increased Complexity**: Managing multiple paths increases the complexity of routing protocols. This complexity can lead to challenges in configuration, maintenance, and troubleshooting.
- **Overhead**: The need to maintain multiple routes can introduce additional overhead in terms of control messages and routing updates, which may consume bandwidth and processing power.
- **Route Coupling Problem**: In scenarios where paths are closely located (such as in wireless networks), the failure of one path may affect others due to interference or shared resources, leading to a phenomenon known as route coupling.
- **Potential for Uneven Load Distribution**: If not managed properly, some paths may become overloaded while others remain underutilized, leading to inefficiencies in resource usage.
- **Security Concerns**: Multipath routing can complicate security measures since data packets may traverse different routes, making it harder to ensure consistent security policies across all paths.

Distance Vector Routing

A distance vector routing algorithm operates by having each router maintain a table (i.e., a vector) giving the best-known distance to each destination and which link to use to get there. These tables are updated by exchanging information with the neighbours. Eventually, every router knows the best link to reach each destination

- How it works :

1. Each router Keeps a table (distance vector table) that contains -
   - The best known distance (usually number of hops) to each possible destinations
   - The direction (next hop) to reach that destination.

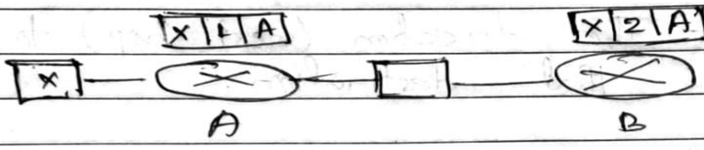
2. Each routers in that network sends their distance vector table to its directly connected neighbours.

3. Neighbour update ~~that~~ their table:
   - Upon receiving a distance vector table from neighbour, the router check if it can reach to a ~~distan~~ destination node through that neighbour with shorter distance.
   - If yes, the router updates its table to reflect better route/path.

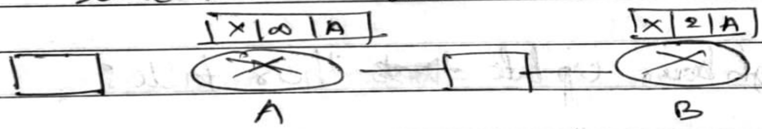
4. As routers exchange table, they ~~all~~ all eventually agree on the shortest path to each destination.

13. Count to infinity problem

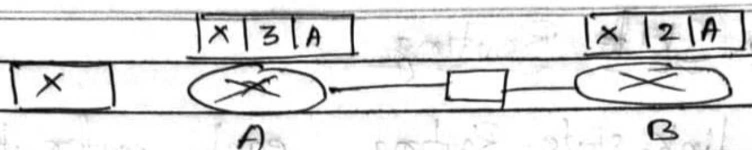
For a routing protocol work properly, if a link is broken every other router should be aware of this immediately, but in distance-vector Routing it takes some time and it fall under counting to infinity problem.



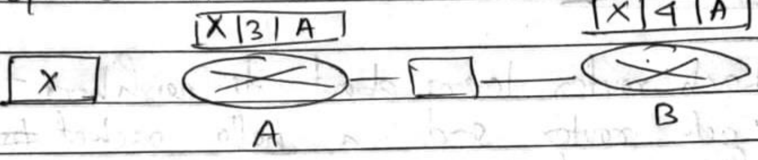
- Initially Both A and B knows how to reach X. But suddenly the link between A and X is broken.



- But before sending this link failure to B by A. A receives distance vector table from B
- A finds out that B can reach out to X by 2 hops. A updates it table not realizing that B's information is outdated.



- Now when B receives A's updated table it assums for some reason the cost to reach to X through A has change and updates it table



- Now again A got updated table from B and update it's table.

This will continue untill the cost to reach X increases gradually untill it reaches infinity.

Link State Routing

Distance vector routing was used in the ARPANET until 1979, when it was replaced by link state routing. The primary problem that caused its demise was that the algorithm often took too long to converge after the network topology changed (due to the count-to-infinity problem)

Link-State Routing

In link-state-Routing, each router tells the whole internet what it knows about it neighbour.

How it works

1. Each router learns about its neighbors -
Each router sends a hello packet ~~to its neighbour~~ and learns about its ~~neighbour~~ neighbour and the cost to reach them.

2. Routers share this information:
Each router sends out ~~the~~ a message called Link State Advertisement (LSA) to every other router in the network using flooding method. LSA contains information about its neighbours, costs ~~and~~ sequence number and age.

3. Routers builds a Complete Map:
with the information received from all routers, each router builds a full network map.

4. Using algorithm like Dijkstra, each router calculates the shortest path to every other router in the network

14. Can a link state routing strategy perform effectively in mobile network? Justify …

Link state Routing is highly efficient in static network but less effective in Mobile network due to several inherent challenges.

1. Frequent Topology Changes :-

- In mobile network, nodes often change their locations, leading to frequent and unpredictable change in topology.

- Link state routing requires ~~to~~ routers to broadcasts every time there is topology changes. In mobile network, this could result in constant flooding of LSA which increases network overhead.

2. High Computational overhead :

- Every time a link state changes, a router must recompute the shortest path using algorithms like Dijkstra.

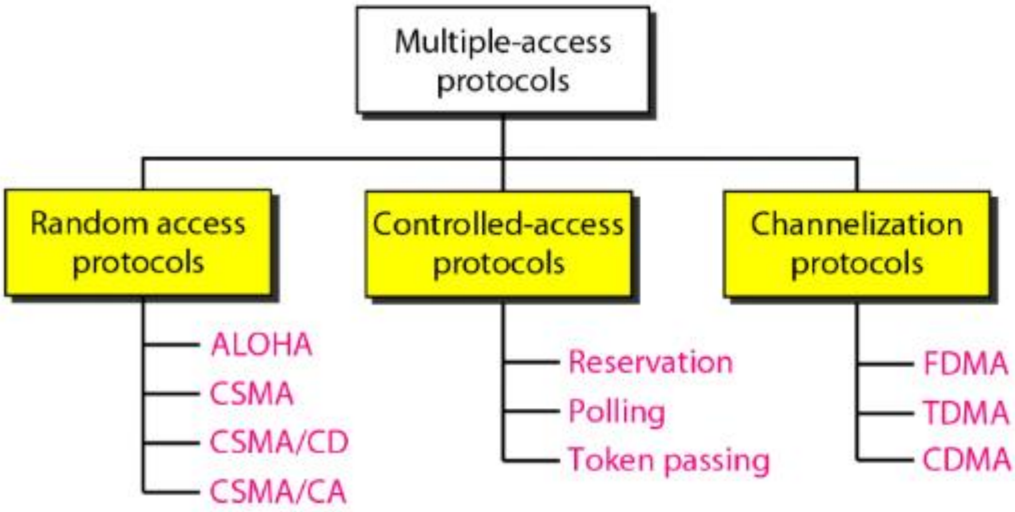
- In mobile networks where topology changes frequently, routers will constantly be Recalculating shortest path, leading to high computation overhead.

15. ‘Link state Routing becomes impractical for a large network ‘ – comment

Link state routing protocols, while efficient and effective for managing routing in networks, face significant challenges as network size increases. Here are the key points regarding the impracticality of link state routing in large networks:

1. **High Resource Requirements**:
    - **CPU Overhead**: Each router must perform complex calculations (e.g., Dijkstra's algorithm) to determine the shortest path, which can be resource-intensive.
    - **Memory Usage**: Routers maintain comprehensive topology databases that can grow significantly with network size, requiring substantial memory.
2. **Increased Bandwidth Consumption**:
    - **Flooding Updates**: Link state protocols rely on sending link state advertisements (LSAs) to all routers in the network whenever there is a change. This can lead to high bandwidth usage, especially in large networks.
3. **Scalability Issues**:
    - The performance of link state routing can degrade in very large networks due to the sheer volume of LSAs and the overhead associated with maintaining accurate topology information.

MAC

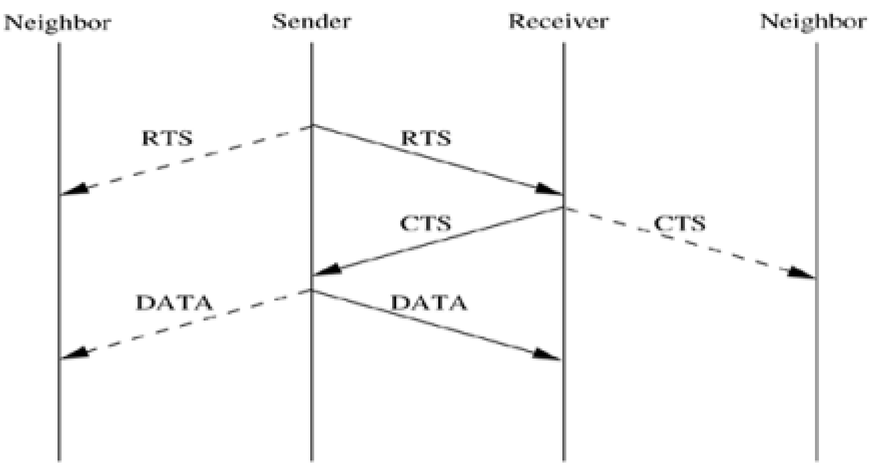


MACA Protocol

The MACA protocol was proposed as an alternative to the traditional carrier sense multiple access (CSMA) protocols used in wired networks. In CSMA protocols, the sender first senses the channel for the carrier signal. If the carrier is present, it retries after a random period of time. Otherwise, it transmits the packet. CSMA senses the state of the channel only at the transmitter. This protocol does not overcome the hidden terminal problem.

MACA uses two additional signaling packets: the request-to-send (**RTS**) packet and the clear to-send (**CTS**) packet. When a node wants to transmit a data packet, it first transmits an **RTS** packet. The receiver node, on receiving the RTS packet, if it is ready to receive the data packet, transmits a **CTS** packet. Once the sender receives the **CTS** packet without any error, it starts transmitting the data packet. This data transmission mechanism is depicted in Figure 6.3.

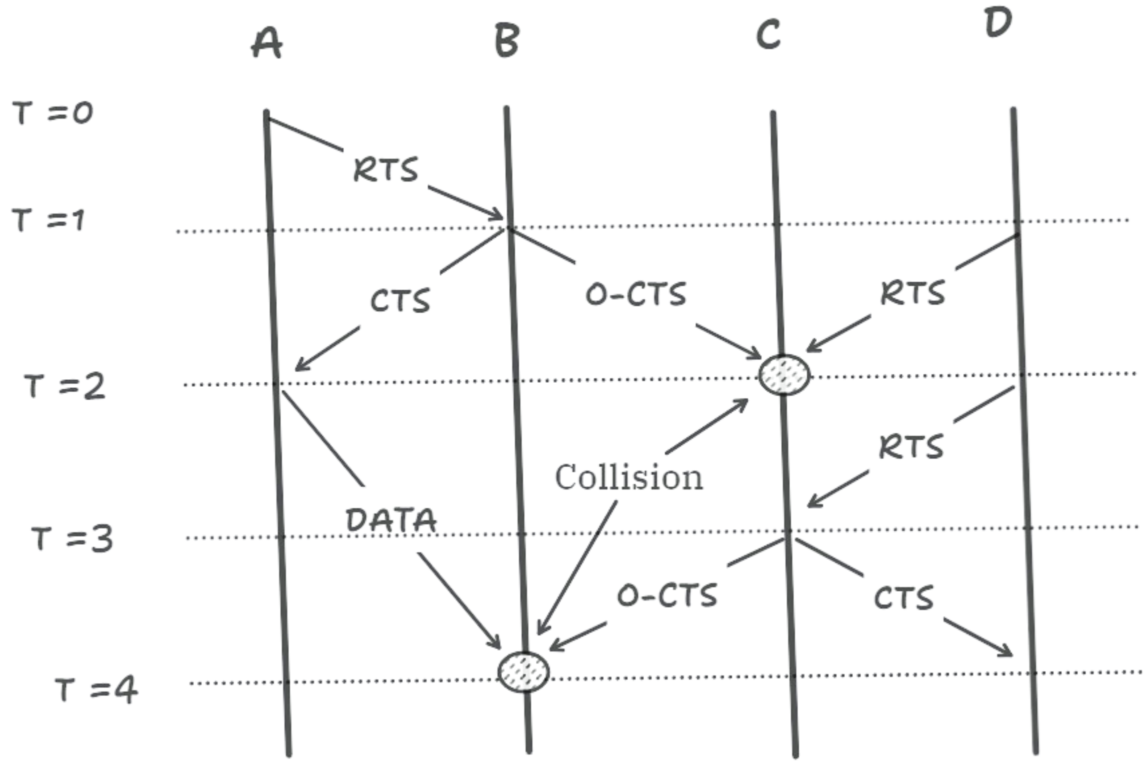
Figure 6.3. Packet transmission in MACA.



16. “MACA partially solves the hidden layer problem” - comment with justification.

MACA reduces collisions but it partially solves the hidden layer problem.
Collisions of RTS / CTS may occur when more than one station send RTS/CTS at same time.
There is no concept of acknowledgement regarding collision to notify the sender.

Consider the following scenario :



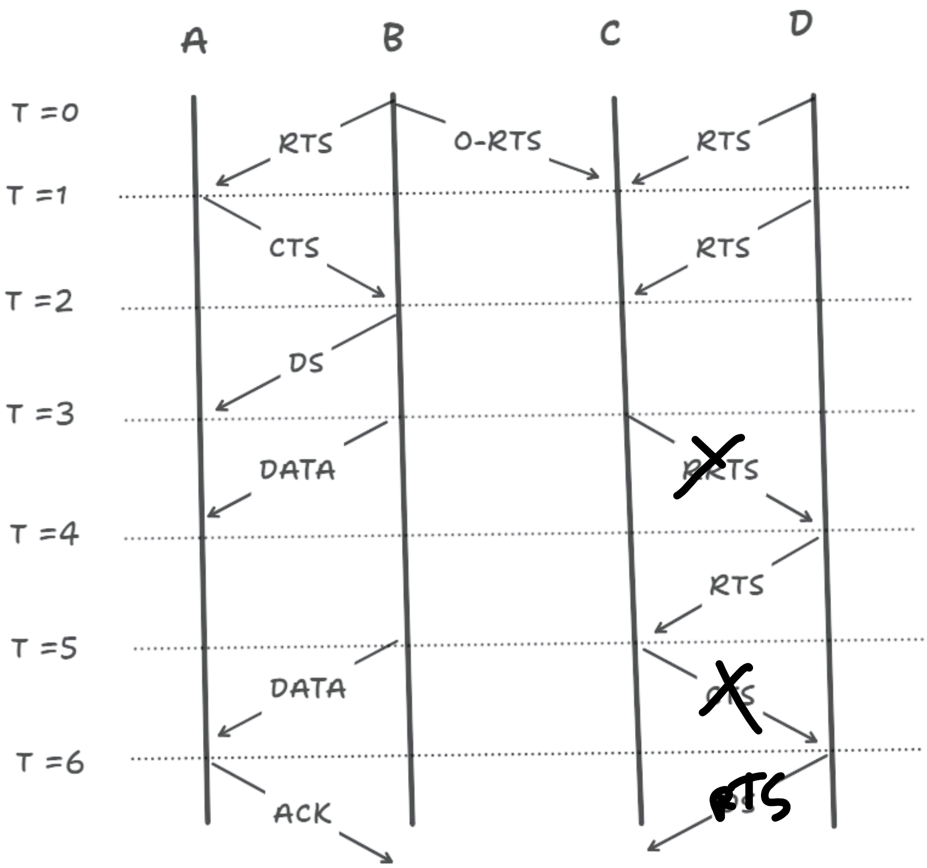
From the above figure (write the answer)

17. Describe the contribution of MACA-W over MACA with necessary illustration

MACA-W resolves the Hidden Terminal problem.

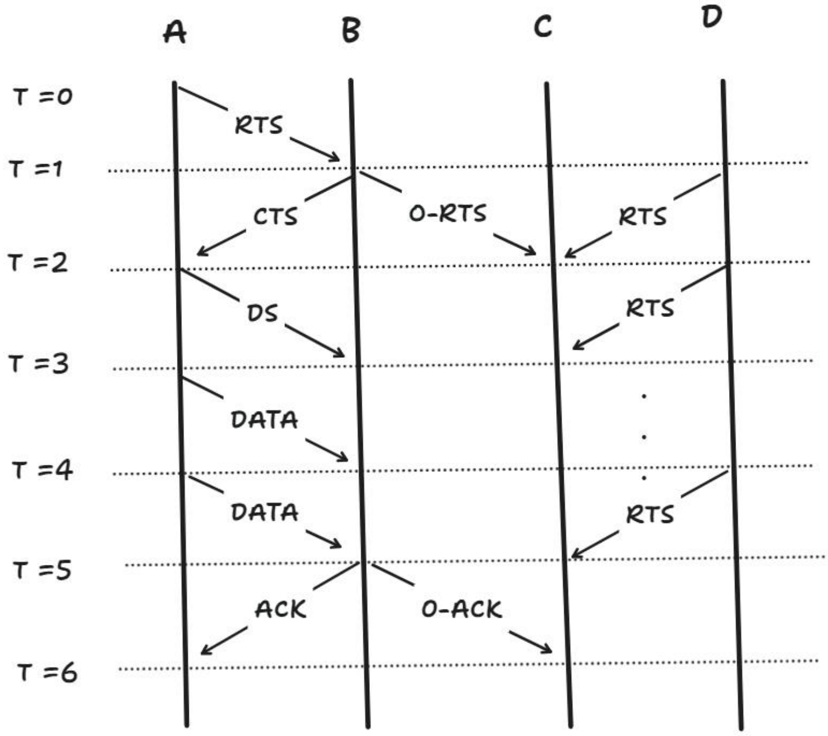
→ New control frame – DS (30bytes) is introduced
→ It informs the length of the actual data frame to be transmitted
→ DS frame indicates successful transmission if RTS/CTS also
→ Deferred transmission until received an acknowledgement frame
→ Introduced RRTS frame (Request to Request to Send)

Illustration



Write the answer below

18. Is MACA-W able to address the exposed station problem? Explain your answer.



19. **State the utility of DS frame in MACA-W protocol.**

20. Discuss, with necessary justification, the relative performance(s) of DSDV and DSR in terms Of End-to-End delay, Power consumption and packet delivery in high mobility.

→ End-to-End Delay

DSDV:

DSDV is a proactive routing protocol, meaning it continuously updates its routing tables and sends periodic updates to maintain the routes. This can lead to increased end-to-end delay, especially in high mobility scenarios where frequent route changes occur.

DSR:

DSR is a reactive protocol that establishes routes only when needed. In high mobility environments, this on-demand nature allows DSR to adapt quickly to changes in the network topology, often resulting in lower end-to-end delays compared to DSDV.

→ Power Consumption

DSDV:

- Due to its proactive nature, DSDV consumes more power because it continuously broadcasts routing updates and maintains active routes. This constant communication can drain battery life quickly, especially in mobile devices that are frequently changing their positions.

DSR:

- DSR tends to consume less power in high mobility scenarios because it only initiates communication when necessary (i.e., during route discovery).

→ Packet Delivery Ratio

DSDV: DSDV provides consistent and reliable routes when mobility is low. However, at high mobility, frequent topology changes can make routing tables outdated, leading to packet loss.

DSR: DSR adapts quickly to topology changes by discovering new routes as needed. However, it may suffer from increased overhead in finding routes during rapid topology changes, occasionally leading to packet loss due to delays.

Metric	DSDV	DSR
End-to-End Delay	Low at low mobility; increases with mobility.	Higher delay due to on-demand route discovery.
Power Consumption	Higher due to periodic updates.	Lower; no periodic updates, only on-demand.
Packet Delivery Ratio	Degrades significantly at high mobility.	Higher at high mobility due to adaptability.

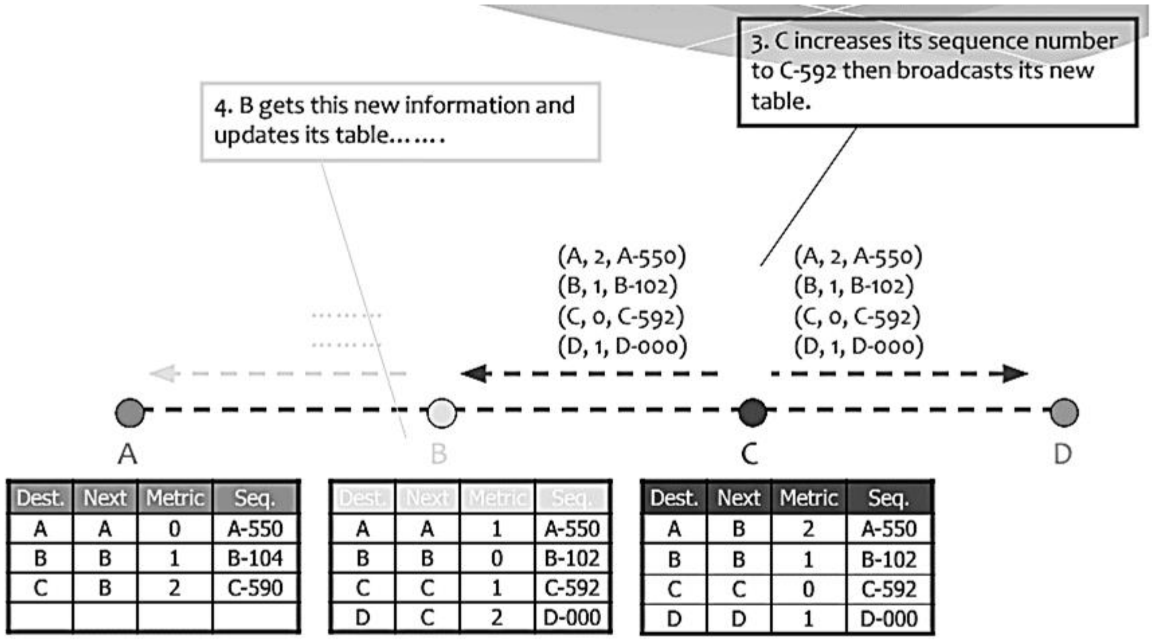
21. Discuss the role of destination sequence number in DSDV in context of 'looping'.

DSDV solves the problem of count-to-infinity or looping that occurs in Distance-Vector routing protocol.

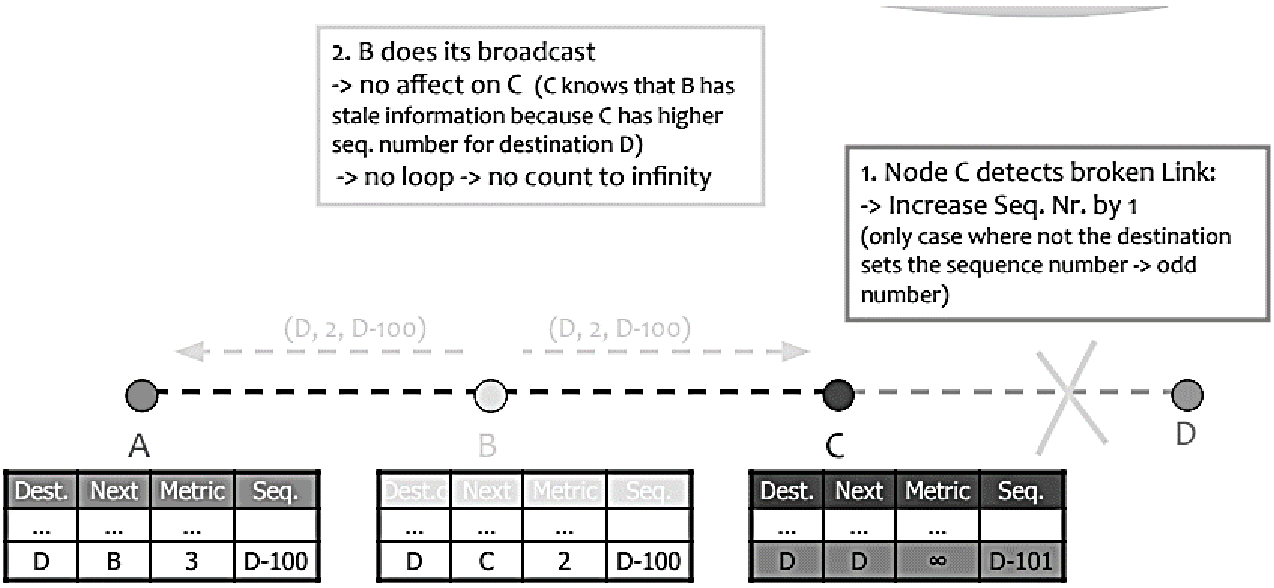
In Distance-vector routing protocol when one nodes links got broken from the network , the delay in broadcasting this broken link information leads to looping problem .

DSDV resolves this issue :

A new node D connect with C , C broadcast the information in the network.



Suppose The link between the C – D got broken, C immediately updates its table , update sequence no, for node by 1 . now even if C receives the information about D from Node B , C will not update its table for D from B node as Sequence No. for D is higher in routing table of C.



22. State the causes for generating 'immediate advertisement' in DSDV Why is it not periodic?

In the Destination-Sequenced Distance Vector (DSDV) routing protocol, immediate advertisements are triggered under specific conditions:

→Information on new Routes

When a node finds a previously unreachable destination, it generates an immediate advertisement to inform its neighbours about this new route.

→broken Links

When a mobile node detects a significant change in the network topology, such as a node moving into or out of range or a link becoming unavailable, it generates an immediate advertisement. This ensures that neighboring nodes are promptly informed of the new routing information to maintain efficient communication.

→metric change

If a node discovers a route with a better metric (e.g., lower hop count) than an existing route to a destination, it will immediately advertise this new route. This helps optimize routing decisions and improves overall network performance

23. Is there a chance of collision route request packets in DSR? If yes, how can It avoided?

Yes, there is a chance of collision of route request packets in the Dynamic Source Routing (DSR) protocol, particularly during the route discovery phase when multiple nodes may simultaneously broadcast Route Request (RREQ) packets.

Solution:

***Insertion of Random Delays**:*

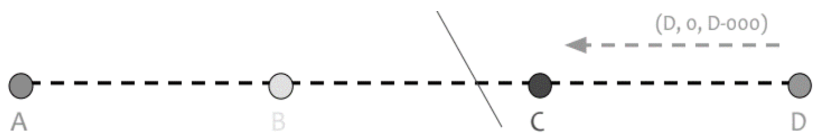
- *To mitigate collisions, nodes can implement a random back-off mechanism before broadcasting their RREQ packets. By introducing a random delay, nodes reduce the chances of simultaneous transmissions, thereby decreasing collision occurrences.*

24. Illustrate the role of Destination Sequence no. in DSDV through an example.

The Destination-Sequenced Distance Vector (DSDV) routing protocol uses a destination sequence number to maintain the freshness of routes and to avoid routing loops. Each entry in a node's routing table includes a sequence number that is incremented every time the destination node sends out an update.

Route Update Example

- D broadcast for first time with seq. no
- C insert entry for D with its seq. no. then immediately broadcast its own table

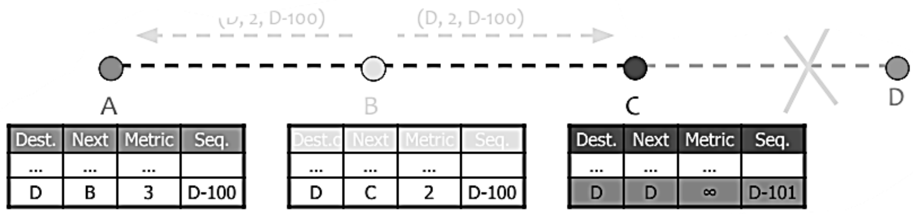


Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-590

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-590
D	D	1	D-000

Avoid routing loops



- Upon link failure of a node(D) the adjacent node(C) updates its routing table and increase the sequence number of the broken link by 1.
- On receiving a route information of D , C doesn’t update its routing table as C has grater sequence number for D in comparison of B`s routing table .

IF Two route have same metric, than update table with route having latest sqn. No

25. How can the performance of a reactive protocol (say DSR) be improved using location information

The performance of the **Dynamic Source Routing (DSR)** protocol can be significantly enhanced by incorporating **location information.** This approach reduce overhead, and improve overall efficiency in mobile ad hoc networks (MANETs).

<u>Key Improvements</u>

➢ **Reduced Route Discovery Overhead**:

- By using location information, nodes can make more informed decisions about which routes to initiate. For instance, if a source node knows the approximate location of the destination, it can limit the route discovery process to a specific area rather than flooding the entire network with Route Request (RREQ) packets.

➢ **Enhanced Route Selection:**

- Location information allows nodes to select routes that are not only shorter in terms of hops but also more efficient in terms of distance. This can lead to lower latency and improved packet delivery ratios.

➢ **Improved Cache Management:**

Nodes can maintain a cache of routes based on proximity and historical location data. This enables them to quickly retrieve routes that are likely to be valid and efficient without needing to initiate a new route discovery process.

➢ **Faster Adaptation to Mobility:**

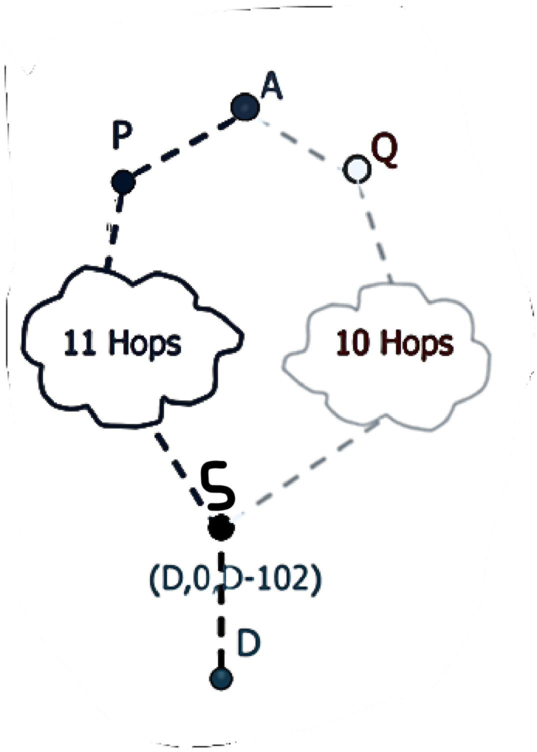
In high-mobility scenarios, knowing the locations of neighboring nodes helps in quickly adapting routing paths as nodes move. This reduces the time taken for route repairs and minimizes disruptions in communication.

26. How can the packet generation be minimized within the route discovery phase in DSR?

- Caching of Routes:
  - Nodes can cache previously discovered routes and use them for subsequent communications without initiating a new route discovery. If a node has a valid cached route to the destination, it can use that route instead of generating new RREQ packets.
  - Example: If Node C has previously communicated with Node D, it can use the cached route instead of sending a new RREQ when it needs to send data again.
- Use of Location Information:
  - By leveraging location information, nodes can limit the scope of Route Request (RREQ) broadcasts to only those nodes that are within a certain geographical area. This targeted approach reduces the number of RREQ packets sent across the network.
  - Example: If Node A wants to communicate with Node B and knows that B is located within a specific region, it can send RREQs only to nodes within that region instead of broadcasting to all neighbours.

27. Discuss the problem of fluctuation in DSDV. Also suggest a solution to overcome this.

Fluctuation:



- Consider the network in the diagram
- Now consider Entry for D in A`s routing table

Dest.	Next	#Hops	Seq. no.
...	...	...	...
D	Q	14	D-100

- D makes a broadcast with new seq. no. D-102 (D , 0 , D-102)
- A receives the broadcast msg from P and its routing table. Update: (D, 15, D-102)

Dest.	Next	#Hops	Seq. no.
...	...	...	...
D	p	15	D-102

- A must propagate this route immediately.
- Again A receives the broadcast msg from Q with same seq. no. Thus Update (D, 14, D-102)

Dest.	Next	#Hops	Seq. no.
...	...	...	...
D	Q	14	D-102

- A must propagate this route immediately.

- ➢ This can happen every time D or any other node does its broadcast and lead to unnecessary route advertisements in the network, so called fluctuations.

Solution:

- Record last and avg. Settling Time of every Route in a separate table. (Stable Data)
- Settling Time = Time between arrival of first route and the best route with a given seq. no.
- A still must update his routing table on the first arrival of a route with a newer seq. no.,
- but he can wait to advertising it. Time to wait is proposed to be 2*(avg. Settling Time).
- Between this waiting the best route to D will be reached to A, and then A only will advertise the Best Route to the network.
- Like this, fluctuations in larger networks can be damped to avoid unnecessary advertisement, thus saving bandwidth.

27. 'Route caching can reduce route discovery overhead in DSR' – Explain

Dynamic Source Routing (DSR) employs route caching as a fundamental mechanism to minimize route discovery overhead, thereby enhancing the efficiency of the protocol.

- When a node discovers a route to a destination through the route discovery process (i.e., sending RREQ and receiving RREP), it caches this route information.
- For example, When node S finds route [S,E,F,J,D] to node D, node S also learns route [S,E,F] to node F .
- This cache can allows quick access in future communications without regenerate the path from node S to node D.
- If a node needs to send data to a destination it has previously communicated with, it can use the cached route instead of initiating a new route discovery. This significantly reduces the number of RREQ packets generated, minimizing network traffic and control overhead.
- For Example , node F forwards Route Reply (**RREP)** [S,E,F,J,D], node F learns route [F,J,D] to node D, now in future when Node F needs to send data to node D it can use the cached route instead of initiating a new route discovery.
- This significantly reduces the number of RREQ packets generated, minimizing network traffic and control overhead.

28. Why is the DSR termed as "source routing"?

Dynamic Source Routing (DSR) is termed "source routing" because the entire routing information, including the complete path that packets should take from the source to the destination, is included in the packet header by the source node itself.

29. Asymmetric (or unidirectional) links occur when node A can hear node B, but B cannot hear node A. Is it a problem for the AODV protocol? If so. how this can be addressed?

Yes, asymmetric (or unidirectional) links can pose a problem for the Ad hoc On-Demand Distance Vector (AODV) routing protocol.

1. **Route Discovery Issues**:
    - When a source node sends a Route Request (RREQ) to a destination node over an asymmetric link, the destination may not be able to send a Route Reply (RREP) back if the link is unidirectional. This prevents the source from establishing a valid route.

Solution:

Use Reverse Path Hints

- Nodes can include information in the RREQ message about potential reverse paths, helping other nodes assess bidirectionality.

30. In AODV, is it possible that route discovery packets travel in the network forever? Why or why not?

No, in **AODV (Ad hoc On-Demand Distance Vector)**, route discovery packets do not travel forever.

Sequence Numbers

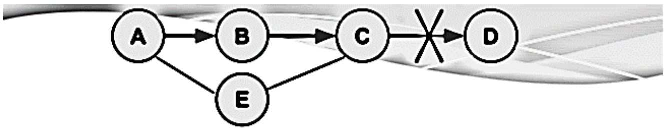
- AODV uses sequence numbers to uniquely identify RREQ messages:
    - Each RREQ is associated with a **unique sequence number** generated by the source node.
    - Intermediate nodes maintain a table of recently seen RREQs and their sequence numbers.
    - If a node receives a duplicate RREQ (with the same source and sequence number), it discards the duplicate.

31. Is it possible to form a loop (count to infinity) while using AODV? Explain your answer through an example ..

Yes, it is possible for the **Ad hoc On-Demand Distance Vector (AODV)** protocol to experience routing loops, particularly in certain scenarios. However, AODV is designed to minimize the occurrence of such loops through the use of **destination sequence numbers**.

❖ **Stale Routing Information**:

- If nodes have outdated routing information due to delays in receiving route updates, they might forward packets using routes that are no longer valid. This can create a situation where packets circulate between nodes without reaching their intended destination.



* Assume, link C-D fails, and node A does not know about it (route error packet from C is lost).
* C performs a route discovery for D.
* Node A receives the route request (via path C-E-A)
* Node A replies, since A knows a route to D via node B
* Results in a loop: C-E-A-B-C

32. Discuss the basic principle of data transfer in TORA

The **Temporally Ordered Routing Algorithm (TORA)** is a source-initiated on-demand routing protocol designed for mobile ad hoc networks (MANETs). Its primary objective is to efficiently manage data transfer while adapting to the dynamic nature of wireless networks.

key principles guiding data transfer in TORA:

❖ **Directed Acyclic Graph (DAG)**:

- TORA constructs a **Directed Acyclic Graph** rooted at the destination node. Each node in the network maintains a height metric that determines its position in the DAG. Data packets can flow from nodes with higher heights to those with lower heights, ensuring that information flows "downhill" towards the destination.

→ The idea is to first build a DAG from the source to the destination.

• Then as links fail, it might be necessary to recompute a DAG in order to find a route. (Link Reversal algorithms are used for this)

• If network gets partitioned, erasures of routes is required.

• TORA uses three kinds of messages:

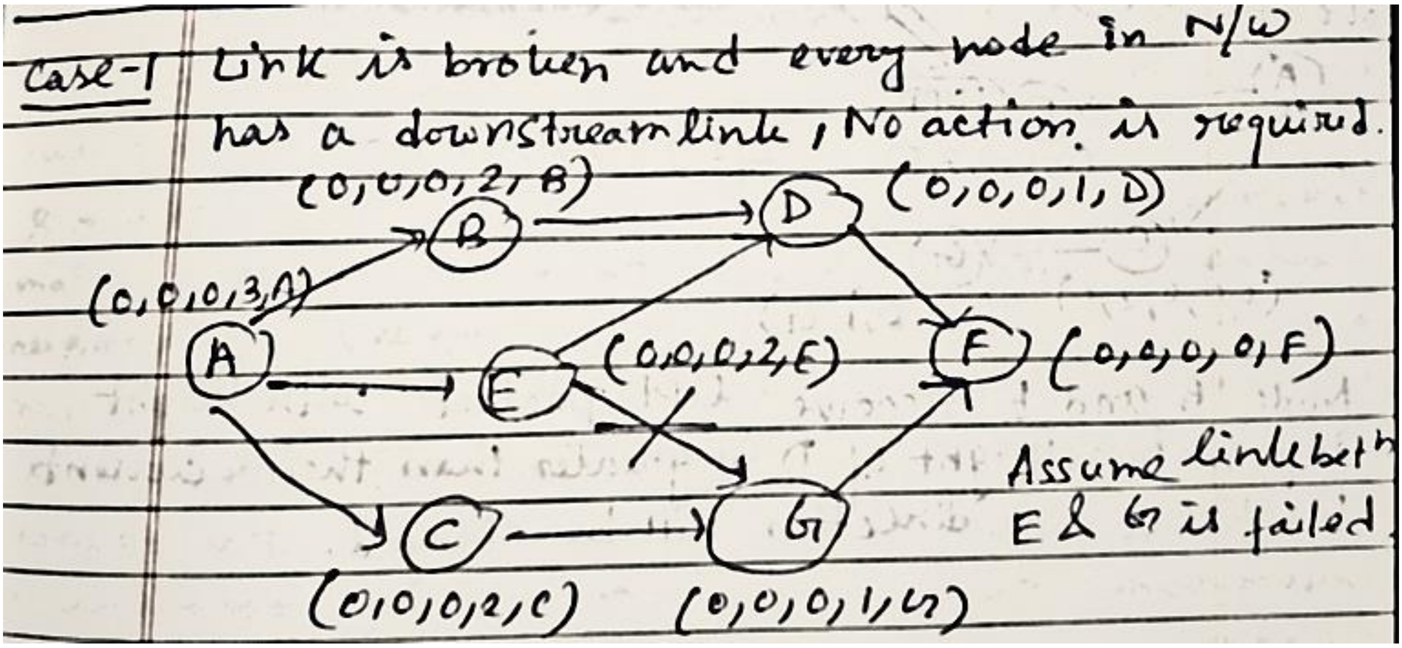
  - The **QRY** message for creating a route.
  - The **UPD** message for both creating and maintaining routes.
  - The **CLR** message for erasing a route.

→ **For what type of network, it performs better than others**

  - **Temporally Ordered Routing Algorithm (TORA)** performs particularly well in **mobile ad hoc networks (MANETs)**, especially in environments characterized by high mobility and dynamic topologies.

33. What will be the reaction for TORA protocol, when topological changes make a route invalid?

When topological changes occur in a network using the Temporally Ordered Routing Algorithm (TORA), such as a link failure, the protocol reacts through a series of defined mechanisms to maintain routing integrity and ensure data can still be transmitted effectively.



Case 2