Full dump →

Proactive Routing protocols →

Destination Sequenced Distance Vector (DSDV)

In this each node keeps record of route information in the form of routing table.

TABLE Consists of

Destination ID

Next Node

Distance (No. of hops)

Sequence No.

Route Broadcast msg

Destination node

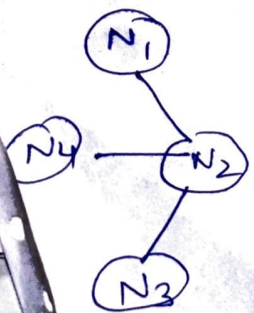
next hop

Recent seq. no.

Distance

UPDATES → Full dump ~~Incre~~ Incremental update

Each node exchanges its updated routing table with each other



Routing table of N1

Dest	Next node	dist	Seq. No
N2	N2	1	14
N3	N2	2	18
N4	N2	2	20

Each node has its own routing table

Adhoc On-Demand Distance

Full dump →
Entire routing table is shared with neighbours.

Incremental update →
Only entries that are changed are exchanged

Table maintainance in DSDV →

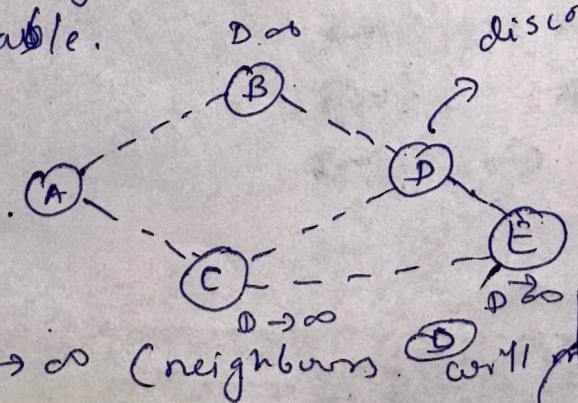
i) Each node receives the route information with most recent seq. no. from other nodes and updates its table.

ii) Node looks at its routing table in order to determine shortest path to reach all the destinations

iii) Each node constructs another routing table based on shortest path information.

iv) New pending table will be broadcast to all neighbours.

v) Neighbour nodes updates its routing table.



NODE A

Dest	next hop	dist.	seq. no.
B	B	1	B340
C	C	1	164
D	B	2	115
E	C	2	20
D	C	3	121

Discarded

* Flooding

ODV routing → Adhoc On-Demand Distance Vector (AODV)

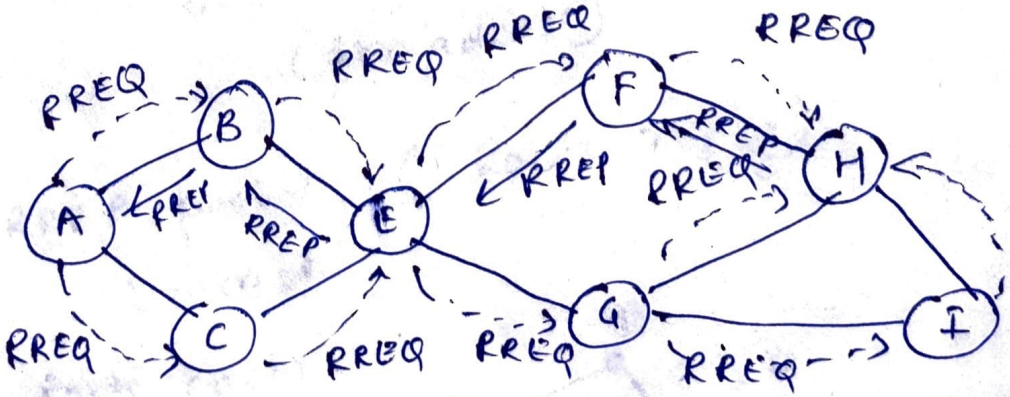
Routing protocol → Reactive routing protocol

Operates in two phases → Route discovery
Route maintanance

* Source node will not carry the complete path. [Each node maintains route cache]
* Each node only knows its previous and next hop information.

Route discovery →

RREQ → Source Node ID
Destination Node ID
recent seq. no.
Broadcast ID
Hop count
TTL



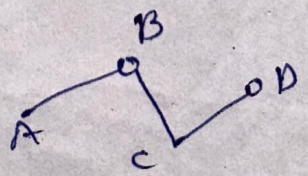
Route 1 : A → B → E → F → H } 4
Route 2 : A → C → E → G → H } 4
Route 3 → A → C → E → G → I → H } 5

selected

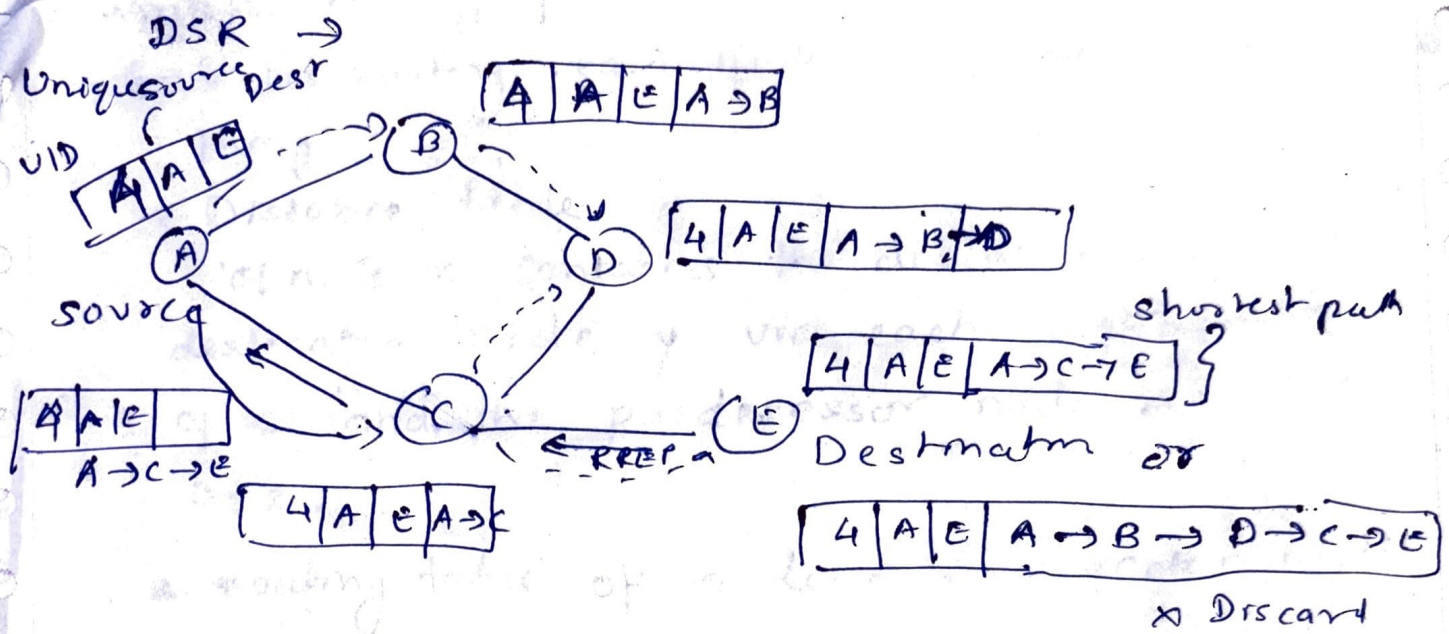
Dynamic Source routing →

* Discovers the route betn source and destnatim when requrred.
* Operatim is based on source routing.
* sender knows the complete path.
* Intermediate nodes do not maintain routing information to route the packets to the destnatim.
* less nw overhead as the no. of message exchanged betn node is very low.
* RERR message (Route Error)
* RREQ
  Source node destnatim
  ID Node ID
  (Broadcast)
* RREP packet (Route reply)
  Unicast

Route cache
Stores the path
(A - B - D)



Route discovery
Route maintainance (RERR)



In AODV, the packets carry the destination address whereas in DSR full information regarding the routes are transfered.

DSR has a large header size

AODV has a small header size.

Wireless Routing protocol →

~~Four~~ For routing, each node maintains four things

* Distance table
  of node x contains the distance of each destination node y via each neighbour z of x and the predecessor node reported by z.
* routing table of node x is a vector with an entry, for each known destination

* Each node maintains information about its neighbours and their neighbours in a table called neighbour's neighbour table. (NNT)
* It periodically transmits a beacon containing a changed neighbours - information.

Three phases of routing →
* route establishment
* route selection
* route maintainance

Algorithm for preferred links computation
NDPL
(1) based on degree of neighbour nodes (no. of neighbour nodes)
(2) based on whether links are stable / unstable
stability is based on the weight given to the links.
WDPL

OLSR → * type of table driven routing
* multipoint relaying
* By reducing size of control packets
* By reducing no. of links that are used for forwarding the link state packets.

* Flooding →

* Routing protocols with efficient flooding mechanism →

Flooding of control packets results in
* significant amount of redundancy
* wastage of BW
* increase in no. of collisions
* Broadcast storms
  ↳ means the presence/origination of a large no. of broadcast control packets for routing due to the high topological instability occurring in the network as a result of mobility.

PLBR → Preferred Link Based Routing protocols.
OLSR → Optimized link~~ed~~ state Routing protocol

PLBR →
* A node selects a subset of node from its neighbours list (NL) subset of nodes is called PL (preferred list)
* Selection of this subset may be based on link or node characteristics.
* All neighbours receives Route Request packets because of broadcast radio channel., but only neighbours present in PL forward them further.
* The packet is forwarded by le neighbours, where le is the maximum no-of neighbours allowed in the PL.

Hierarchical routing protocols →

* reduction in the size of routing tables.
* better scalability.

Hierarchical state Routing protocol →

* clustering at different levels
* with efficient membership management at ~~each~~ every level of clustering.
* enhances resource allocation and management.
* Elected leaders at every level forms the members at the ~~inter~~ immediate higher level.
* physical clustering
* logical clustering
* Every node maintains information about all the neighbours and the status of links to each of them.
* This information is broadcast within the cluster at regular intervals.
* The cluster leader exchanges the topology and link state routing information among its peers in the neighbourhood clusters.

Fisheye State Routing Protocol →

* FSR uses the fisheye technique to reduce information required to represent graphical data, to reduce routing overhead.

*

Cryptography and n/w security →

Week 1 :-

Data integrity :- message is not altered. → hash functions

Authentication :- just cryptography

Confidentiality :- Encryption/decryption cannot do need some other technique.

Undeniability :- digital signatures

Data Integrity → Hash functions

Authentication, undeniability → digital signatures

Confidentiality → Encryption, Decryption, Cryptography

In public key cryptography: Receiver generates public key P_k, Secret key S_k

Symmetric key cryptography is faster than public key cryptography.

Replay attack →
send a same message again after some time by impersonating someone.

A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8

J	K	L	M	N	O	P	Q
9	10	11	12	13	14	15	16

R	S	T	U	V	W	X	Y	Z
17	18	19	20	21	22	23	24	25

CRYPTOGRAPHY

17 16

2 + 18 = 20 mod 26

IP Spoofing →

Attackers create packets with false IP addresses and then exploit applications which use authentication based on IP address.

IPsec is an internet standard for network layer security.

IP Security provides additional security to the applications.

Strengths of IPsec →

* Multivendor
* Scalability

VPN products use IPsec protocols.

Services which are provided by IPsec are

* Data authentication
* Data origin authentication
* Integrity using hash function
* Data encryption to provide privacy.
* Protection against replay attacks
* Provide confidentiality to the traffic flow.
* Transport and tunnel modes to meet different network needs.

Applications of IPsec →

* VPN
* allows remote access over internet.
* bank sector
* distributed applications.