Adhoc and Sensor Networks

Unit-I

* Introduction

- An adhoc network is a collection of wireless mobile nodes (or routers) dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. The routers are free to move randomly & organize themselves arbitrarily.
- An adhoc network is self-organizing & adaptive.

* Adhoc Networks Characteristics

- Mobility
- Multihopping (A multihop network is a n/w where path from source to destination traverses several nodes)
- Self-organization (The adhoc n/w must autonomously determine its own config. parameters)
- Energy conservation (Most adhoc nodes have limited power supply so energy efficient protocol design is critical for longetivity)
- Scalability (In some applications the adhoc n/w can grow to several 1000 nodes)
- Security (Challenges of security are ability of the intruders to eavsdrop & jam/spoof the channel or active and passive attacks)
- Connection To the Internet (Ex:- Reach of domestic LAN can be extended as needed with portable routers)

* Applications of Adhoc Wireless Networks

- Temporary Network Deployment
- Disaster Relief Operations
- Smart Buildings (A large no. of sensors & actuators can be deployed without installing any infrastructure to create smart surroundings of a sentient computing environment)
- Cooperative objects (COs) (COs are entities that are composed of sensors, actuators & COs are capable of communicating & interacting with each other & with the environment in a smart & autonomous way to achieve a specific goal)
- Health care
- Military applications
- Emergency operations (such as search & rescue, crowd control, & commando operations)

* Difference b/w Cellular & Adhoc Wireless Networks

Cellular Networks	Adhoc Wireless Networks
- Fixed infrastructure-based	- Infrastructure-less
- Single-hop wireless links	- Multi-hop wireless links
- Guaranted Bandwidth (designed for voice traffic)	- Shared radio channel (more suitable for best-effort data traffic)
- Centralized Routing	- Distributed routing
- Circuit-switched	- Packet-switched
- Seamless connectivity	- Frequent path breaks due to mobility
- High cost & time of deployment	- Quick & cost-effective deployment
- Reuse of frequency spectrum through geographical channel reuse	- Dynamic frequency reused based on carrier sense mechanism
- Easier to achieve time synchronization	- Time synchronization is difficult & consumes bandwidth
- Easier to deploy bandwidth reservation	- Bandwidth reservation requires complex medium access control (MAC) protocols
- Application domain include mainly civilian & commercial sectors	- Application domains include battlefields, emergency search & rescue operations, & collabarative computing.
- High cost of n/w maintenance	- Self-organization & mainterance properties are buiet into the n/w
- Mobile hosts are of relatively low complexity	- Mobile hosts require more intelligence (should have transceiver as well as routing/switching capability)
- Major goals of routing & call admission are to maximize the call acceptance ratio & minimize the call drop ratio	- Main aim of routing is to find path with minimum overhead & also quick reconfiguration of broken paths.
- Widely deployed & currently in the third generation of evolution	- Several issues are to be addressed for successful commercial deployment even though wide-spread use exists in defence

* Issues in Adhoc Wireless Networks

- **Scalability**: Adhoc n/ws suffer from the scalability problem in capacity as overhead increases with n/w size growing.
- **MAC Protocol Research Issues**: IEEE 802.11 WLAN with CSMA, CSMA-CD, CSMA-CA and use of bluetooth is not optimized in multihop environment
- **Networking Issues**: N/w protocols need to be designed - location services to map n/w dynamically.
- **Adhoc Routing & forwarding**: The highly dynamic nature of a mobile

adhoc n/w results in frequent & unpredictable changes of n/w topology, adding difficulty & complexity to routing among mobile nodes.

→ Location Based Routing : During forwarding operation, these protocols use node position provided by GPS or other mechanism. It doesn't require route establishment & maintenance. No routing information is stored

→ Three main strategies can be identified in location-aware routing protocols.

Greedy Forwarding: In this, a node tries to forward packet to the closest neighbour closest to destination. If multiple nodes found then different choices. If no neighbour found, new rules applied to find alternative route.

Direct Flooding: Nodes forward the packets to all neighbours that are located in the direction of the destination.
Ex:- Distance Routing Effect Algorithm for Mobility (DREAM) & Location Aid Routing (LAR)

Hierarchical Routing: Routing is structured in two layers. Location-aware routing for routing on longer distance & a proactive distance-vector scheme adopted when packet arrives closer to destination.
Ex:- Location Proxy Routing Protocol & Terminode Routing Protocol

— TCP Issues: The mobile multihop adhoc environment brings fresh challenges to the TCP protocol: impact of mobility, node interaction MAC layer, Impact of TCP congestion window size & Interaction b/w MAC protocols

— Network Security: • Different Security Attacks:

Impersonation # DOS (#Disclosure attack : Reveal something about location of nodes or structure of n/w)

• Attacks Using Fabrication

→ Resource Consumption Attack (Malicious node deliberately tries to consume resources of other nodes in n/w)

→ Rushing Attack (Attacker node that receives request packet quickly floods packet throughout n/w before other nodes. Nodes that receive legitimate route request discard packet assuming it duplicate. Thus attacker node become an intermediate node)

→ Black Hole Attack (Malicious node advertises a good path to the destination node which could hamper path-finding process or interrupt all ~~nodes~~ data packets being sent to destination)

• Security at Data-link layer

• Secure Routing (SRP [Secure Routing Protocol], ARAN [Authenticate Routing for Adhoc N/w], SEAD [Secure Efficient Adhoc Distance], SAODV [Secure Adhoc On-Demand Distance Vector])

→ ~~AEEI~~ Ariadne is a secure adhoc routing protocol based on DSR & timed efficient stream loss-tolerant authentication (TESLA) protocol).

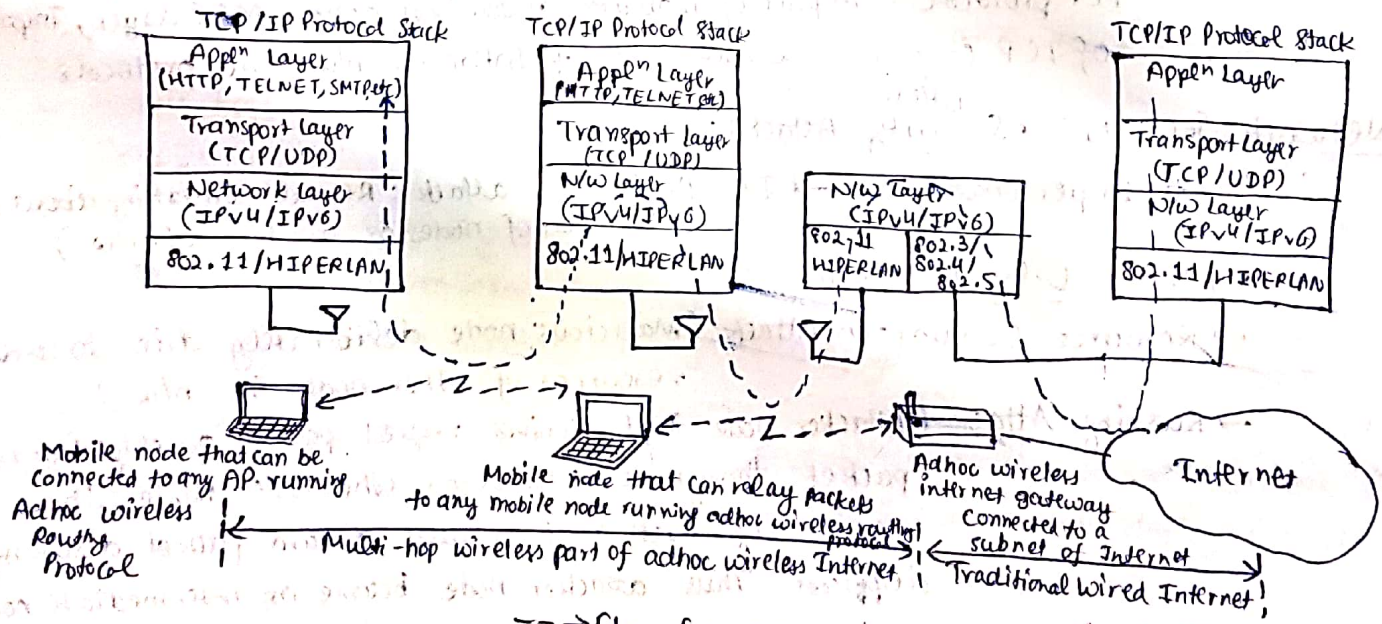
- Quality of Service (QOS) : → Client-server Model Shift
→ Interoperation with the Internet
→ Energy Consumption
→ Self-organization

* Major Issues in Deploying an Adhoc Wireless Network

1. Scenario of Deployment
   - (a) Military Deployment : Data centric or user-centric n/w
   - (b) Emergency Operations Deployment
   - (c) Commercial wide-area deployment
   - (d) Home network deployment
2. Required Longevity of Network
3. Area of Coverage
4. Service Availability
5. Operational Integration with other infrastructure
6. Choice of Protocol

* Adhoc Wireless Internet

- The adhoc wireless Internet extends the services of Internet to end users over an adhoc wireless n/w.



- Major Issues considered for a successful adhoc wireless Internet are the following :

(i) Gateways (ii) Address Mobility (iii) Routing
(iv) Transport Layer Protocol (v) Load Balancing (vi) Pricing / Billing
(vii) Provision of security (viii) QOS support (ix) Service, address & location ~~delivery~~ discovery

* Issues in Designing a MAC protocol for Adhoc Wireless Network

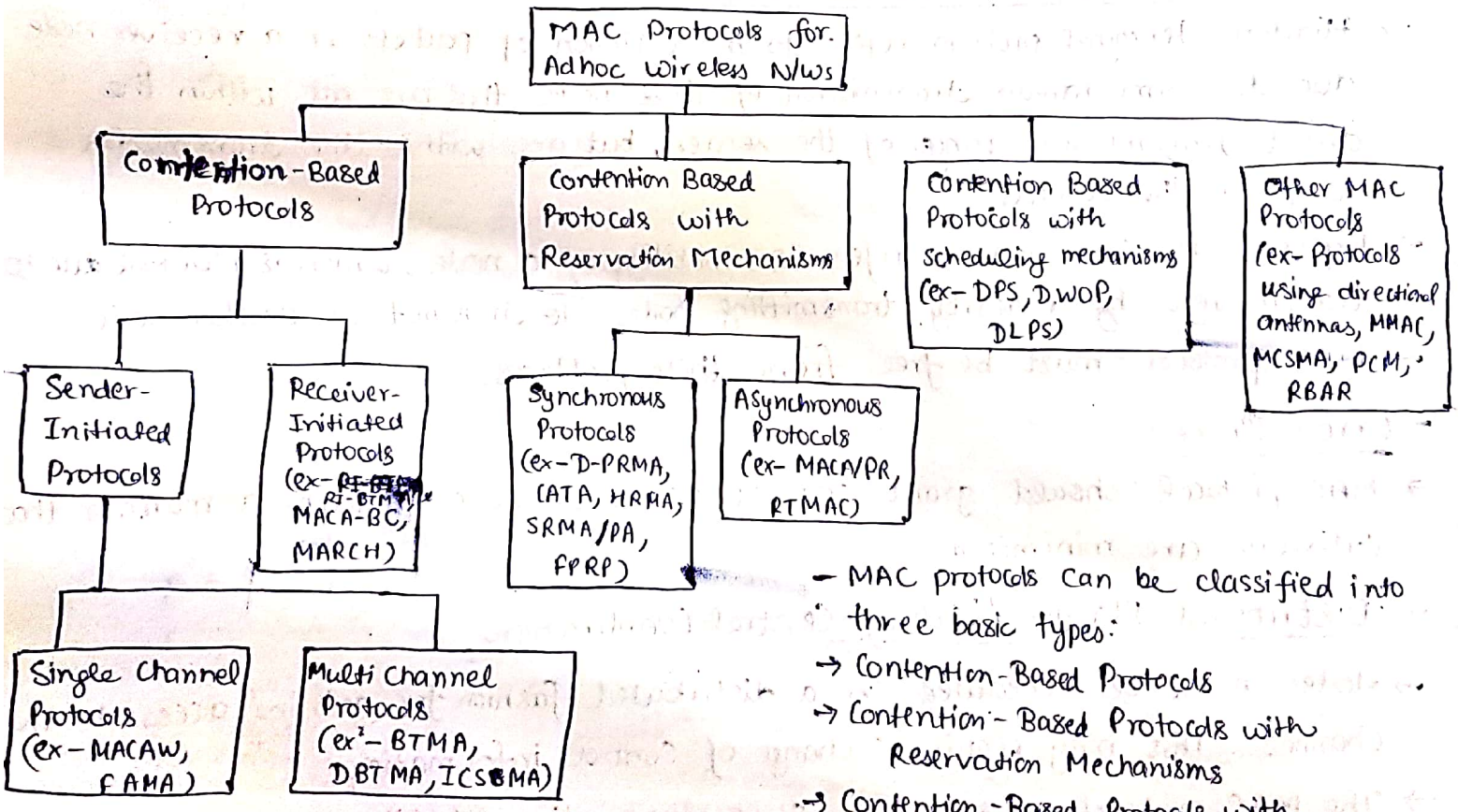
- **Bandwidth Efficiency**
  → Bandwidth available for communication is very limited. The MAC protocol must be designed in such a way that the scarce bandwidth is utilized in an efficient manner. The MAC protocol must try to maximize this bandwidth frequency.
- **Quality of Service Support**
  → MAC protocol must have some kind of a resource reservation mechanism that makes into consideration the nature of the wireless channel & mobility of nodes.
- **Synchronization**
  → MAC protocol must take into consideration the synchronization b/w nodes in the network.
- **Hidden and Exposed Terminal Problem**
  → Hidden terminal problem refers to the collision of packets at a receiver node due to simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.
  → Exposed terminal problem refers to inability of a node, which is blocked due to transmission by a nearby transmitting node, to transmit to another node
  → MAC protocol must be free from these problems.
- **Error Prone**
  → MAC protocol should grant channel access to nodes in such a manner that collisions are minimized.
- **Distributed Nature / Lack of Central Coordination**
  → Nodes must be scheduled in a distributed fashion for gaining access to the channel. This may require exchange of control information.
  → The MAC protocol must make sure that the additional overhead, in terms of bandwidth consumption, incurred due to this control information exchange is not very high
- **Mobility of Nodes**
  → The MAC protocol must take mobility factor into considerations so that the performance of the system is not significantly affected due to node mobility

* Design Goals of a MAC protocol for Adhoc Wireless Networks

- The operation of the protocol should be distributed
- The protocol should provide QoS support for real time traffic

- The access delay which refers to average delay experienced by any packet to get transmitted, must be kept low.
- The available bandwidth must be utilized efficiently.
- The protocol should ensure fair allocation of bandwidth to nodes
- Control overhead must be kept as low as possible.
- The protocol should minimize the effects of hidden & exposed station problems
- The protocol must be scalable to large n/ws.
- The protocol should have power control mechanisms
- The protocol should have mechanisms for adaptive data rate control.
- The protocol should try to use directional antennas.
- The protocol should provide synchronization among nodes

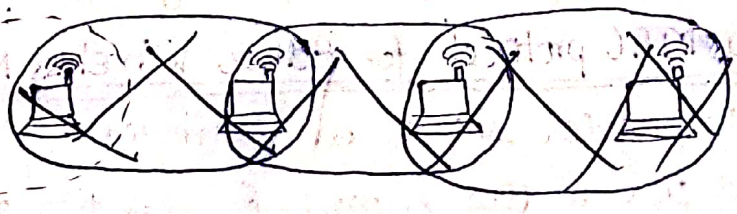
* Classification of MAC Protocols

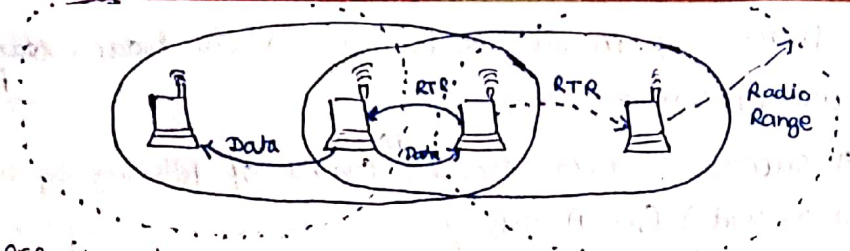


- MAC protocols can be classified into three basic types:
  → Contention-Based Protocols
  → Contention-Based Protocols with Reservation Mechanisms
  → Contention-Based Protocols with Scheduling Mechanisms

* Contention-Based Protocols

- These protocols follow a contention-based channel access policy. A node does not make any resource reservation a priori.
- Receiver-Initiated MAC Protocols
  → Receiver first has to contact the sender informing the sender that it is ready to receive data.





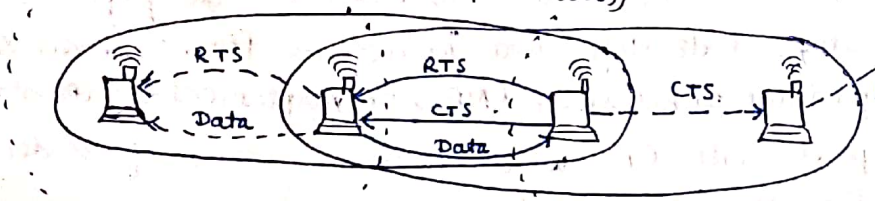
RTR - Ready to Receive

→ There is only one control message used. Ex:- MACA-BI

– Sender-Initiated MAC protocols

→ It requires sender to initiate communications by informing receiver that it has data to send.

→ Ex:- MACA (Multiple Access with Collision Avoidance)
FAMA (Floor Acquisation Multiple Access)



RTS - Ready To send
CTS - Clear To send

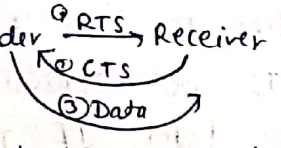
→ Sender-initiated protocols further divided into two categories:

① Single-channel Sender-Initiated Protocol

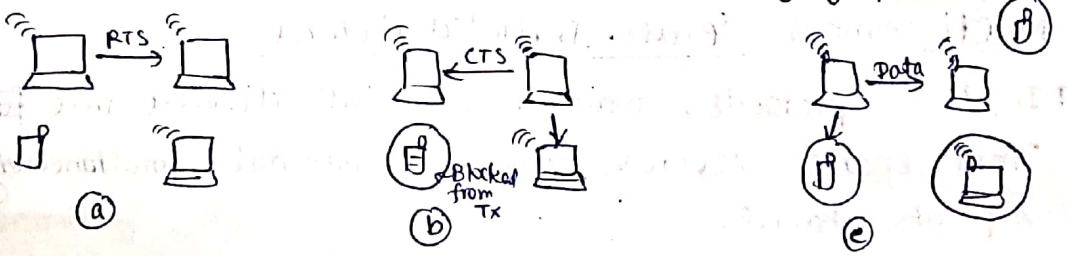
In these protocols, the total available bandwidth is used as it is, without being divided. A node that wins the contention to the channel can make use of the entire bandwidth.

MACA (Multiple Access with Collision Avoidance)

⇒ MACA uses a 3-way handshake, RTS-CTS Data.



⇒ MACA inhibits a transmitter when a CTS packet is overheard so as to temporarily limit power O/P when a CTS packet is overheard. This allows geographic reuse of channels.



Control Handshake Used in MACA

⇒ Collisions do occur in MACA, especially during RTS-CTS phase. There is no carrier sensing. The slot Each host basically adds a random amount of time to minimum interval time required to wait after overhearing an RTS or CTS control msg.

⇒ If two or more stations transmit an RTS concurrently, resulting in collision, they will wait for randomly chosen interval, doubling avg interval on every attempt.

⇒ Weaknesses:- Hidden Terminal Problem, No ACK of data transmission

MACAW (MACA wireless)

⇒ It is slotted MAC protocol widely used in Adhoc n/w. It uses RTS-CTS-DS-DATA-ACK frame sequence for transmitting data, sometimes

preceded by RTS-RRTS frame seq. in view to provide sol^n to hidden station problem.

⇒ MACAW doesn't make use of carrier sense.

⇒ Principle of operation: A successful data transfer $^{(A \to B)}$ consists of following seq. of frames:

(i) RTS (Request to send) from A to B
(ii) CTS (Clear to send) from B to A } Frame ~~Message~~
(iii) DS (Data sending) from A to B
(iv) Data fragment from A to B
(v) ACK frame from B to A

FAMA (Floor Acquisation Multiple Access)

⇒ It requires every transmitting station to acquire ctrl of floor (wireless channel) before it actually sends any data. To "acquire floor", sender sends an MTS. using nonpersistent packet sensing (NPS) or nonpersisent carrier sensing (NCS).

⇒ The receiver responds with CTS which contains address of sender to tell which station has acquired floor.

⇒ FAMA requires that collision avoidance be performed at Tx & Rx node.

FAMA - Non Persistent Transmit Request (FAMA-NTR):

⇒ It combines NCS along with RTS-CTS ctrl pkt exchange mechanism.

⇒ Before sending, sender senses channel. If busy, backs off for random time period & retries later. If free, transmit RTS pkt.

⇒ After transmitting RTS, sender listens to channel for one round trip time in addition to time required by receiver to transmit CTS.

⇒ If CTS not received within this time or found corrupted, ~~node~~ sender backs off & retries later. If received without error, transmit data & releases channel after transmission.

(ii) Multi-channel Sender-Initiated Protocol

In these protocols, available bandwidth divided into ~~further~~ multiple channels. This enables several nodes to transmit simultaneously, each with a separate channel.

BTMA (Busy Tone Multiple Access) (No ack required)

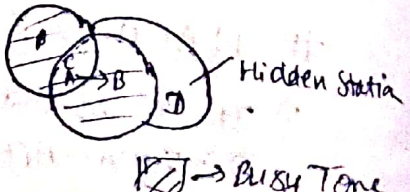
⇒ It divided total available bandwidth into two channels: a msg channel for data & a narrow busy-tone channel for collision avoidance.

⇒ With BTMA,

★ A station senses the msg channel when it is idle. If transmission ongoing, it transmit a busy-tone signal in busy tone channel.

★ when sender ready to transmit, it first senses busy-tone channel to be idle for a predetermined time & then transmit pkt.

★ If busy channel occupied, ~~stati~~ sender wait for random time & reschedules transmission



⇒ BTMA can't effectively solve hidden & exposed terminal problems.

DBTMAP (Dual Busy Tone Multiple Access Protocol) (No ack required)

⇒ It uses two control channels to further improve channel performance: one for transmitter busy tone (BT_t) & other for receiver busy tone (BT_r)

⇒ To start a transmission,

★ A station checks both busy tone channels. If either one busy, back off & try later. Else, sends RTS pkt on data channel & turns on BT_t signal which is turned off at end of RTS transmission & the sender monitors BT_r.

★ As soon as receiver hears RTS, it turns on BT_r signal for a period long enough to cover intended data transmission. Once sender receives signal, it waits double propagation time & then starts the transmission.

★ If sender fails to receive BT_r signal, it gives up & retransmits later.

Transmitter Busy Tone
Receiver busy Tone

⇒ This protocol can work for multi-hop radio n/ws as well as for single-hop fully connected n/ws.

— Receiver Initiated MAC protocols

RI BTMA (Receiver Initiated BTMA)

⇒ Based on the idea that collision only happens at receiver side, a receiver RI-BTMA protocol to address hidden station problem

⇒ Divided available bandwidth into two channels – busy-tone & msg channel.

⇒ Station ready to transmit senses busy-tone first.

★ If channel busy, reschedule transmission. otherwise, preamble containing RX address on data channel & then listens to busy-tone channel.

★ If Receiver hears preamble correctly, transmit busy tone on busy tone channel.

★ After hearing busy tone, sender start to transmit data. As long as the sender is transmitting, the receiver keeps sending busy tone.

★ If on other hand, sender doesn't receive busy tone, it defers its data transmission & tries again later.

Busy Tone

⇒ The operation of RI-BTMA protocol two types:

★ The basic protocol (No backlog buffers pkts that suffer collisions can't be retransmitted)

★ The controlled protocol (Backlogged mode; backlog buffer is non-empty)
transmitting a backlogged pkt in next time slot with prob q
probability

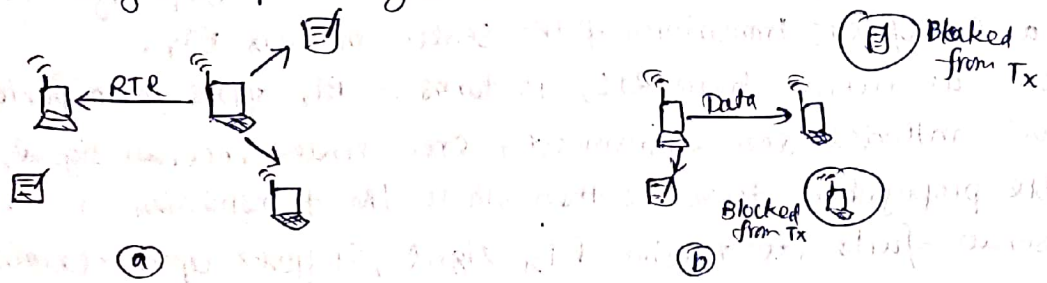
★ Non-backlogged mode (Transmitting a non-backlogged pkt in next time slot with p probability)

MACA-BI (MACA-By Invitation) Protocol

⇒ It requires a receiver to send data by using RTR (Ready To Receive) pkt instead to RTS & CTS pkts. It is a 2-way exchange (RTR-data).

⇒ A node can't transmit data unless it has received an Invitation from receiver. Receiver needs to predict if indeed the node has data to transmit to it.

⇒ Under non-stationary traffic situation, a node may still transmit an RTS if the tx queue length or pkt delay exceeds a certain threshold before RTR is issued.



MABI Ctl Handshake

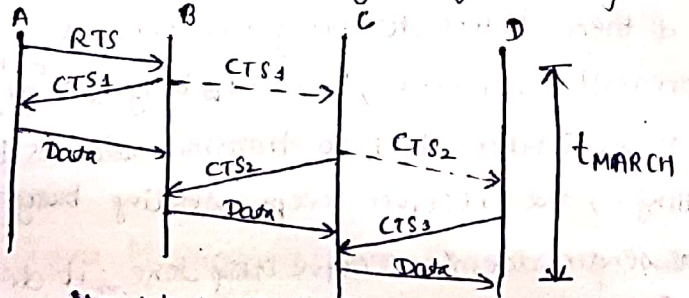
⇒ MACA-BI results in reduced tx/rx turnaround time. Every transmission should be delayed by tx-to-rx turnaround time to allow previous transmitter to switch to receive mode.

MARCH (Media Access with Reduced Handshake) Protocol.

⇒ Unlike MACA-BI, it doesn't require any traffic prediction mechanism. It exploits the broadcast nature of traffic from omnidirectional antennas to reduce the no. of handshakes involved in data transmission.

⇒ In MARCH, RTS pkt is used only for first pkt of stream unlike MACA which uses RTS-CTS exchange before ~~every~~ transmission of every pkt. From second pkt onward, only CTS pkt is used.

⇒ It operates without resorting to any traffic prediction. A node has knowledge of data pkt arrivals at its neighbouring nodes from overhead CTS pkts.



Handshake Mechanism in March

⇒ It can be viewed as a request-first, pull-later protocol since the subsequent nodes in the path just need to send invitations to pull the data toward the destination node. The RTS-CTS msg in MARCH contains

★ MAC addresses of Tx & Rx

★ Route Identification No. (RI_{II})

* Contention-Based Protocols with Reservation Mechanisms

- Though these protocols are contention-based, contention occurs only during the resource (bandwidth) reservation phase. Once bandwidth reserved, node gets exclusive access to the reserved bandwidth. Hence QOS support for real-time traffic can be provided.

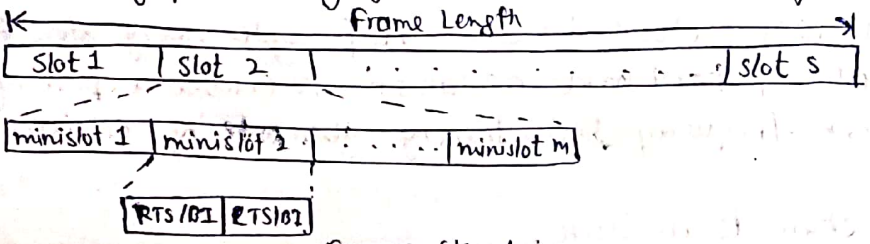
- **Distributed Pkt Reservation Multiple Access (D-PRMA) protocol**

→ It extends centralized PRMA scheme into distributed. It is a TDMA based scheme

→ Channel divided into fixed & equal-sized frame along time axis. Each frame composed of 'S' slots & each slot consists of 'm' minislots.

→ Each minislot is further divided into RTS/BI & CTS/BI control fields which are used for slot reservation & overcoming hidden terminal problem.

→ All nodes having pkt ready for transmission contend for 1st minislot of each slot.



Frame structure

→ Remaining 'm-1' ~~slot~~ minislots granted to winner. The same slot in subsequent frame can be reserved by winner until it completes it pkt transmission session.

→ Within reserved slot, communication b/w sender & receiver takes place by means of TDD or FDD.

→ A certain period at beginning of each slot is reserved for carrier sensing.

→ In order to prioritize nodes, two rules:

1st rule → ~~If~~ Voice nodes allowed to contend for minislot 1 with probability p=1. others p<1.

2nd rule → If winner is voice node, permitted to reserve same slot in each subsequent frame.

→ In order to avoid hidden terminal problem, all nodes hearing CTS sent by receiver are not allowed to transmit during remaining period of that same slot. In order to avoid exposed station problem, a node hearing RTS but not CTS is still allowed to transmit.

- **Collision Avoidance Time Allocation Protocol (CATA)**

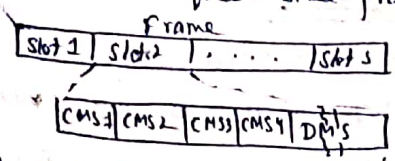
→ Based on dynamic topology-dependent transmission scheduling. Nodes contend for & reserve time slots by means of a distributed reservation & handshake mechanism.

→ operation based on 2 principles:

Receiver must inform potential sender about reserved slot on which it is receiving pkts & sender need to inform about interferences in slot to receiver.

Usage of -ve ack for reservation requests, & the pkt transmission at beginning of each slot, for distributing slot reservation info to senders of broadcast or multicast sessions.

→ Time → Equal-size frame → 'S' slots → each slot → 5 mini slot.
(First 4 called CMS (Control mini slot for transmission of ctrl pkt) & last called DMS for data)



→ Each node that receives data during DMS of current slot transmit a slot reservation (SR) pkt during CMS1 of slot for potential receiving Request-to-send pkt.

→ Every sender transmit data during DMS of current slot transmit a RTS pkt.

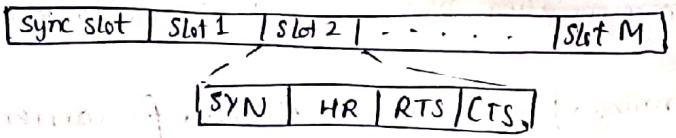
→ Receiver node of unicast session transmit CTS pkt. on receiving CTS, sender understands that reservation success & can transmit data during DMS of that slot.

→ Do not transmit anything during CMS3 & sender alone transmit not-to-send (NTS) pkt during CMS4 which acts as negative ack.

→ Worst case value of frame length = $\min(d_2 + 1, N)$ d is max degree of node
→ works single-channel half duplex radios. N is total nodes

Hop Reservation Multiple Access Protocol (HRMA)

→ A multichannel MAC protocol based on half duplex, very slow FHSS radios.
→ Uses a reservation & handshake mechanism to enable a pair of communicating nodes to reserve frequency hop, thereby guaranteeing collision-free data transmission.
→ 'L' frequency channels available.
one frequency channel 'f_0' for dedicated syncing channel
L-1 frequencies are divided into $M = \left(\frac{L-1}{2}\right)$ frequency pairs.

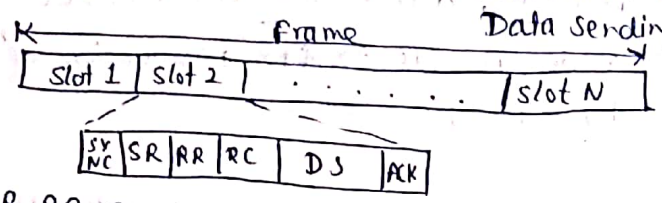


→ Time is slotted & each slot assigned separate frequency hop. Each slot into four periods (SYN-sychronizing, HR, RTS, CTS period)
→ During SYN, all nodes exchange syncing info.
→ New nodes gain sync info by remaining on f_0 for long period of time
If no info, assumes only node in n/w.
→ When node receives data to be transmitted, first listens to HR period of immediately following slot. If it finds free channel during HR period, transmit RTS pkt to receiver during RTS period & waits for CTS pkt send by receiver during CTS period. On receiving CTS pkt ~~during CTS period~~ correctly, sender & receiver reserved current hop successfully & then transmit data & receive ACK.

Soft Reservation Multiple Access with Priority Assignment (SRMA/PA)

→ Nodes use a collision-avoidance handshake mechanism & a soft reservation mechanism.
→ Soft reservation capability for distributed and dynamic slot scheduling

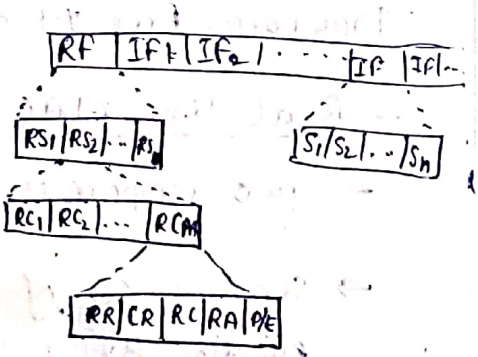
→ Time into frames → slots → 6 different fields (SYN, Soft Reservation (SR), Reservation Request (RR), Reservation Confirm (RC), Data sending (DS), ACK)



→ SR, RR, RC & ACK for controlling pkts. SYN for synching purpose.
→ DS for data transmission
→ SR serves as busy tone & access priority.
→ Idle node → RR packet in free in RR field of free slot (Free slot detect using SR)
→ In case voice node then tries to take ctrl of reserved slot by data node if priority level of voice higher than data. This is called soft reservation. Priority initially assigned based on class & process voice priority > data priority.
→ In order to avoid collision, a binary back-off algo. is used for non-real time conn. & a modified binary back-off algo. for real time conn.

– Five-Phase Reservation Protocol (FPRP)

→ A single-channel TDMA based broadcast scheduling protocol. Nodes use a contention mechanism in order to acquire time slots. Protocol is fully distributed, i.e., multiple reservation can be simultaneously made throughout n/w.
→ No ordering among nodes is followed. Nodes need not wait for making time slot reservation.
→ Time into frames → Information frame → N Info slots (IS)
→ Reservation frame → N Reservation slots (RS), M Reservation Cycle (RC)



→ In order to reserve an IS, node need to contend during corresponding RS based on these contentions, TDMA schedule generated in RF & used in subsequent IFs until next RF. During each IS, node in one of three states: Transmit (T), Receive (R) or blocked (B).

→ Reservation cycle (RC) has 5 phases:
(i) Reservation Request (RR) phase → To make reservation request
(ii) Collision Report (CR) phase → To report collisions
(iii) Reservation Confirmation (RC) phase → To make confirmations of request
(iv) Reservation Ack. (RA) phase → Ack of reservation
(v) Packing & Elimination (P/E) phase → Two kinds of pkt transmitted. Packing pkt serves to make the broadcasting pattern denser in given slot. Elimination pkt to remove possible deadlock (DL) b/w adjacent broadcast nodes.

- MACA with Piggy-backed Reservation (MACA/PR)

→ Main components are: a MAC protocol, a reservation protocol, a QOS routing protocol
→ Time divided into slots. Each node records Tx & Rx reservations of its neighbours in a reservation-table (RT).
→ For Real Traffic:
Sender first send RTS pkt for which receiver respond with CTS pkt.
Now sender sends first Data pkt of real time session. Reservation info for next Data pkt is piggy-backed on this current Data pkt.
On receiving this Data pkt, receiver updates its reservation table with piggy-backed reservation info & then sends ACK pkt to sender.
Receiver piggy-backs the reservation confirmation info. on ACK pkt.

Advantage: Doesn't require global Sync among nodes
Drawback: Free slot can be reserved only if it can fit RTS-CTS-DATA-ACK exchange.

→ for non real-time traffic:
Sender transmit non-real time pkt, finds free slot in table & then waits for same slot the next time around. If it is still free then RTS pkt in slot, expects CTS pkt & then sends data & receives ack still in same slot. RTS & CTS pkt contains time that data transmission is going to take place. In this way, neighbours of source & destination nodes can update their tables.

Advantage: Doesn't require global sync among nodes
Drawback: Free slot can be reserved only if it can fit RTS-CTS-Data-ACK exchange.

- Real-Time MAC protocol (RTMAC)

→ Two components : MAC for best-effort traffic & Reservation protocol for real-time traffic.
→ Separate set of ctrl pkts (ResvRTS, Resv CTS & ResvACK) is used for effecting BW reservation for real time packets.
→ RTS, CTS & ACK ctrl pkt for transmitting best effort packets.
→ Time into superframes. Flexibility of slot placement in the superframe due to variable length time slots.
→ Each superframe consists of no. of reservation slots (resv-slot) whose time duration is 2x max. propagation delay.
→ Data transmission normally requires a block of resv-slots.
→ A node that needs to transmit real-time pkts. first reserves a set of resv-slots & this set is called conn. slot. Each node maintains a resv. table.
→ No time sync is assumed. Main advantage is BW efficiency.
→ A 3-way handshake protocol for effecting the reservations.

* Contention-Based MAC protocols with Scheduling Algorithm Mechanisms

– Distributed Priority Scheduling (DPS) & Medium Access in Adhoc Nlws

→ DPS defines two mechanisms in order to provide QOS.

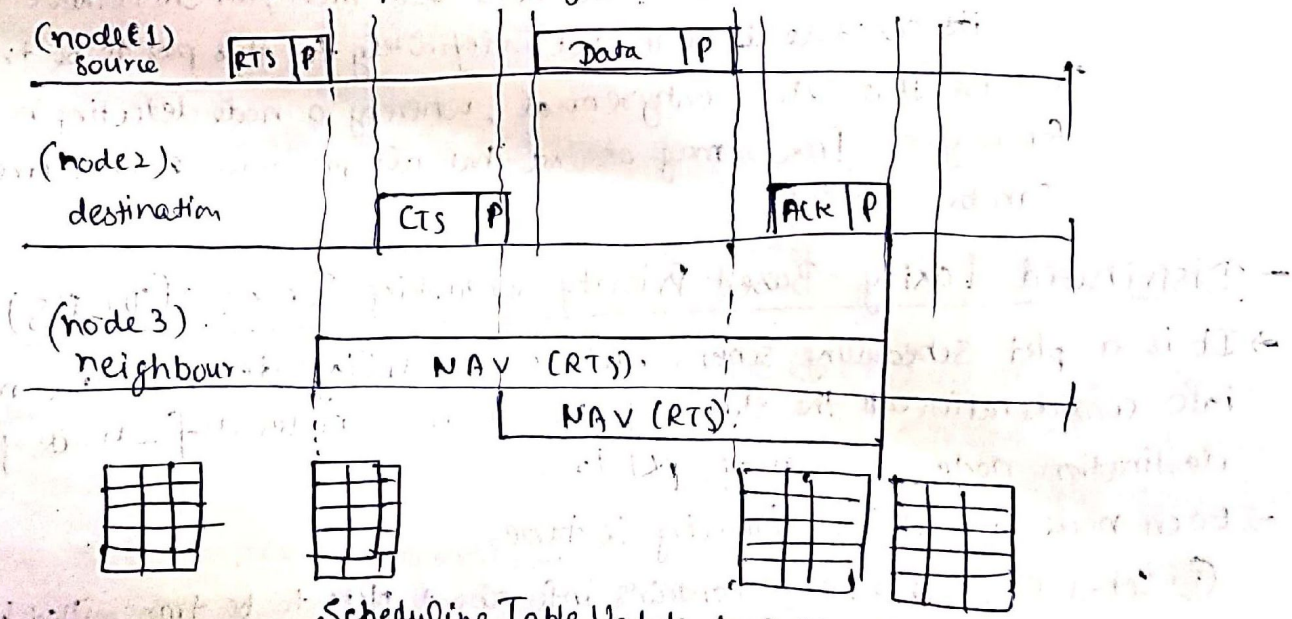
→ The first scheme is the distributed priority scheduling; a technique that piggybacks the priority tag of a station's HOL (Head-of-Line) pkt onto ctsl of data transmitted packet.

Each pkt has associated priority index based on local info.
HOL pkt of a station refers to pkt with highest priority that is queued locally.

When a source station transmits a DATA pkt, its HOL info is piggybacked on transmitted DATA pkt. This info is copied by receiver onto ACK pkt it sends. Neighbours hearing Data & Ack pkts retrieve piggybacked info & update their scheduling table accnly.

When a station (sender) hears an ACK pkt, it removes from its scheduling table any entry made earlier for corresponding DATA pkt.

→ # Distributed Priority Scheduling MAC (DPS-MAC) uses DPS based on the basic RTS/CTS/Data/ACK pkt exchange mechanism.



Scheduling Table Update in DPS-MAC

→ The second scheme is multi-hop coordination. When an intermediate station receives a Data pkt, it receives its priority index piggyback. The station updates the priority index of the pkt. Through priority update scheme, if a pkt suffers due to excessive delay at upstream stations, downstream stations will increase pkt priority index so that the chance that pkt meets it end-to-end delay requirements is increased.

– Distributed Wireless Ordering Protocol (WHOP)

→ It tries to achieve fifo fairness by transmitting pkts acc^n to their time of arrival.

→ An exchange consists of: RTS-CTS-DATA-ACK pkts. RTS & CTS pkts contain info on next pkt's time of arrival. Data & ack pts contain info on current pkt's time of arrival.

→ Every node must maintain a schedule where it logs time of arrival info from overheard transmissions. When a node overhears an RTS or CTS it adds an entry to its schedule. When a node overhears a Data or ACK pkt it deletes an entry from its schedule.

→ Two problems:

(i) Asymmetric Info & Receiver's Participation: Node keep only schedule of immediate neighbour, sender can know if it has highest priority pkt in the neighbourhood of receiver. If receiver receiver CTS & aware that a higher priority pkt in neighbourhood, it doesn't ignore pkt, rather send a CTS & allow transmission to continue disturbing fairness. To ~~avoid this~~ restore fairness, receiver participants add notice to ACK pkt which tells transmitter to backoff by a some time.

(ii) Perceived Collisions & Stale Entry Detection: A problem occur if node misses Data or ACK pkt. It can happen when two ~~sender~~ transmissions take place around same node at same time & is referred to as a perceived collision. The node will then fail to remove entry from its schedule & will wait indefinitely for this pkt to be transmitted. To solve this stale entry removal, whereby a node detecting new entry for a given flow, may assume that all previous entries are stale & can be deleted.

- Distributed Laxity-Based Priority Scheduling Scheme (DLPS)

→ It is a pkt scheduling scheme, where scheduling decisions are made taking into consideration the states of neighbouring nodes & feedback from destination nodes regarding pkt losses

→ Each node maintains following 2 tables:

(i) Scheduling Table (ST) contains info about pkts to be transmitted by node & pkts overheard by node

(ii) Pkt Delivery Ratio Table (PDT) contains count of data pkts transmitted & count of ack pkts received

→ Incoming pkts to a node are queued in node's I/P queue acc^n to arrival times

→ Scheduler sorts pkt acc^n to priority values & inserts them into transmission queue

→ Highest priority pkt from this queue is selected for transmission. The receiver initiates a feedback by means of count of data pkts received by it conveyed to the source through ACK pkts. Feedback info handler (FIH) using priority func^n module (PFM) calculate priority indices of pkts in ST.

* MAC Protocols that use Directional Antennas

- Several advantages over omnidirectional transmissions such as reduced signal interference, increase in system throughput & improved channel reuse.

- MAC protocol using Directional Antennas

→ Directional antennas attain higher gain & restrict broadcast to a meticulous direction thus it becomes possible that two pairs of nodes located in each other's vicinity be in contact simultaneously.

→ The use of higher frequency bands will reduce the size of directional antennas.

→ Many schemes have been proposed with this idea:

Slotted Aloha
Directional MAC (DMAC) [RTS-CTS-Data-Ack sequence → only pkt sent using directional antenna]
IEEE 802.11 protocol
Multihop RTS MAC (M-MAC) for transmission on multihop paths.

→ Directional antennas brings in 3 new problems:

New kinds of hidden terminals
Higher directional interference
Deafness (where routes of two flows share a common link)

- Directional Busy Tone Based MAC (DBTMA) protocol

→ The nodes use directional antennas for transmitting & receiving data pkts, reducing their interference to other neighbour nodes.

→ The protocol works as follows:

1. A source transmits an RTS addressed to the receiver on all its antennas (omnidirectional transmission)
2. On receiving this RTS, the receiver determines the antenna-element on which the RTS is received with maximum gain.
3. The receiver sends back a directional-CTS (D-CTS) to source using selected antenna-element. It also turn on busy tone BT_R in direction towards source.
4. On receiving CTS, source turns on busy tone BT_t in direction towards receiver.
5. Once pkt transmission is over, source turns off BT_t signal.
6. After receiving the Data pkt, receiver turns off BT_r signal.

(For a unicast transmission, only a single antenna element is used. For broadcast transmission, all the N antenna elements transmit simultaneously)

* Other MAC protocols

- Multichannel MAC Protocol (MMAC)

→ Its target is to solve multichannel hidden node problem when the IEEE 802.11 MAC is applied for multichannel operation.

→ Multichannel Hidden Node Problem:

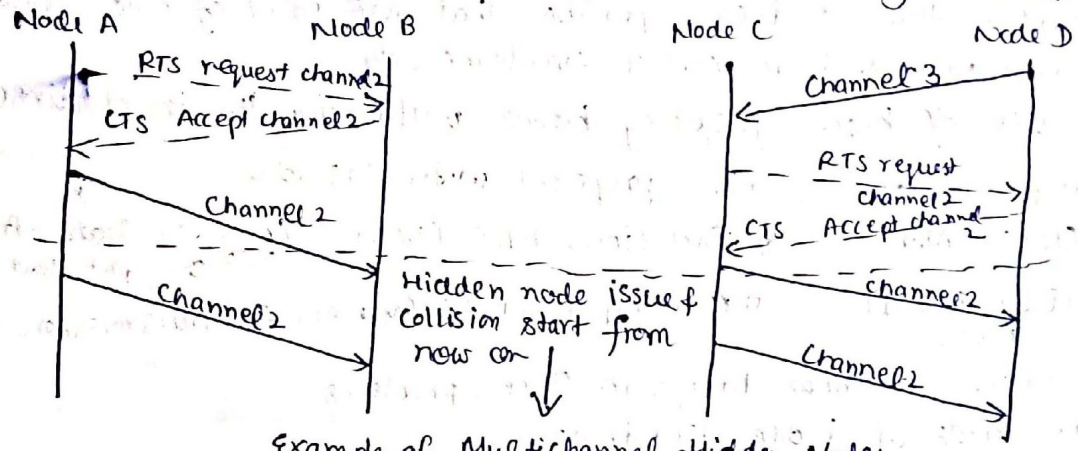
In multichannel operation, any two nodes must negotiate for a channel.

, a negotiation process must make sure that the neighbouring nodes are not using the same channel, in order to avoid collisions. However, a negotiation process, even one based on RTS/CTS, can't achieve this goal.

The hidden nodes exists because of two problems:

① Single transceiver limits the capability of a node in listening different channels

② Different channels in different pair of nodes are not synchronized.

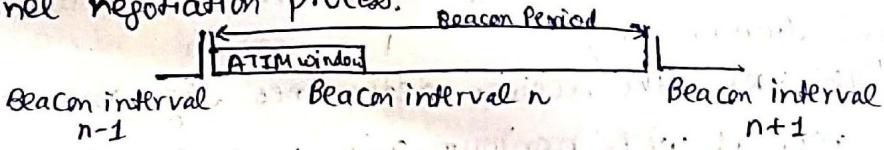


Example of Multichannel Hidden Nodes

→ Procedures of MMAC

MMAC solves multichannel problem based on simple mechanism: the RTS/CTS based channel negotiation process is sure to be synchronized among all nodes. In such a way, channels for different pairs of communicating nodes will not interfere with each other.

An announcement traffic indication msg (ATIM) window in each beacon excludes transmission of regular date pkts. ATIM window is reserved for ctrl msgs for channel negotiation process.



Since start & end pts of ATIM window in all nodes can be synchronized through Time "Sync" Fun^{n} (TSF) & beaconing procedures, the channel negotiation process in all nodes is thus synchronized.

→ Next step in MMAC after solving hidden node problem is to develop a scheme to select best channel. Two factors are taken into account:

Preferable Channel List — High preference, Medium preference, Low preference

Traffic Load in a channel.

→ Procedure: Source S to Destination D

(i) Node S sends ATIM request to Node D

(ii) Node D selects a channel

(iii) Node D sends ATIM-ACK to inform S of selected channel

(iv) Node S sends an ATIM-RES msg to Node D to reserve channel for Nodes S & D.

→ After a channel has been successfully selected blw S & D, both nodes can be switched to selected channel & can start transmissions using CSMA/CA Protocol

- Multichannel CSMA MAC protocol

→ It breaks the total available BW equally into N-non overlapping channels by using either FDMA or CDMA schemes.

→ Stations in the n/ws should be able to scan all N sub-channels continously. For each sub-channel scanned, if total received signal strength is above predefined threshold, the station thinks there is an ongoing transmission & marks it "busy". Otherwise, marked "idle" & put into free-channel list of this station.

→ To transmit a pkt, a station checks its free channel list first:

If most recently used sub-channel that carries a successful transmission is free, the channel is chosen again for transmission; otherwise the station randomly selects an idle sub-channel for transmission.

If free-channel list: empty, station waits for a sub-channel to be idle first & then keeps monitoring till it is: idle for Long interframe space & a random backoff period before a transmission is initiated.

If received signal strength goes over threshold during waiting time, implying an ongoing transmission, the station quits its transmission attempt & schedules a new backoff where there is an available sub-channel again.

- Power Control MAC protocol (PCM) for Adhoc N/w

→ It provides a MAC layer soln for localized power control by varying the transmission power to reduce overall energy consumption.

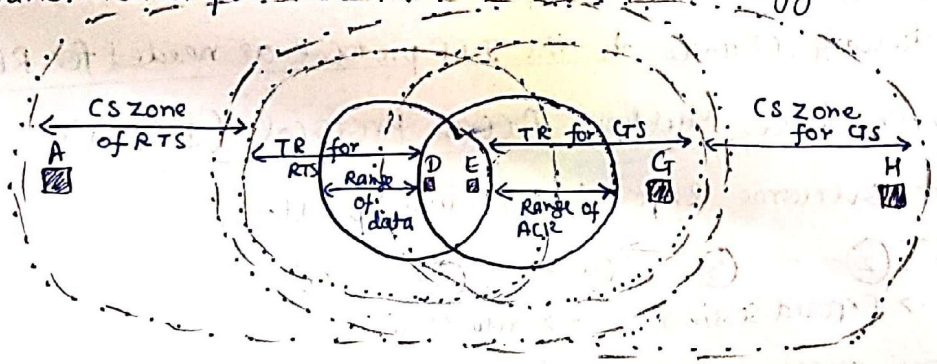


Illustration of Power Ctrl scheme : CS = Carrier Sense & TR = Transmission Range

→ PCM exploits the signal level of received RTS for calculation of $P_{desired}$ combination with some well known min. threshold for received signal strength RX_{thresh} that is necessary for correctly decoding the msgs. The transmission power is calculated using eqn:

$$P_{desired} = \frac{P_{max}}{P_{r \to received}} RX_{thresh} \times C$$

→ In PCM, RTS & CTS pkts are sent by means of max power on band while data & ACK pkts are sent by min. power needed for communication.

→ PCM extracts knowledge from monitoring & analyzing received RTS/CTS msgs which represent behaviour & cond"s of surrounding environment.

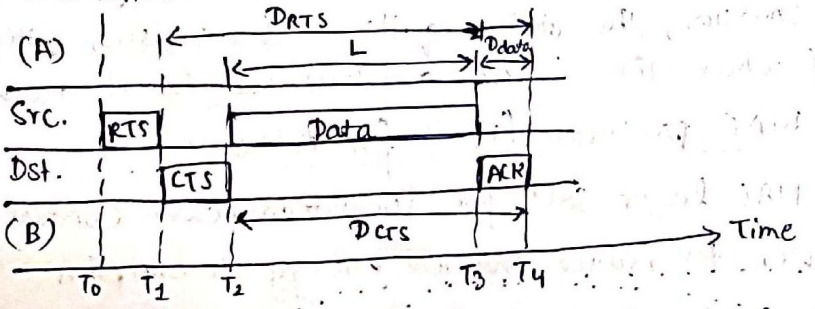
– Receiver-Based Autorate Protocol (RBAR)

→ The RBAR protocol is a rate adaptation algorithm whose goal is to optimize the appln thoroughput.

→ The core idea of RBAR is to allow the receiver to select appropriate rate for a data pkt during RTS & CTS pkt exchange.

→ A pair of RTS & CTS ctrl frames are exchanged b/w source & destination nodes prior to start of each data transmission. The receiver of RTS-frame calculates transmission rate to be used by upcoming data-frame transmission on basis of the signal-to-noise ratio (SNR) of the received BTS-frame & on a set of SNR thresholds calculated with reliable knowledge of an priori wireless channel model.

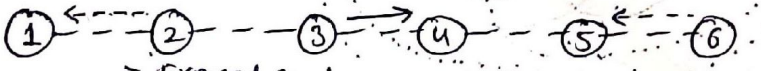
→ The rate used is then sent back to source in CTS pkt. The RTS, CTS & data frames are modified to contain info^n on size & rate of data transmission in order to allow all nodes within the transmission range to correctly update the NAVs.



Timeline showing changes to the DCF protocol as needed for RBAR protocol

– Interleaved Carrier-Sense Multiple Access Protocol (ICMA)

→ It is designed to overcome exposed terminal problem.



→ when there is an ongoing transmission b/w node 3 & 4, other nodes in n/w, i.e., nodes 2 & 6 are not permited to transmit to nodes 1 & 5 respectively. This is because of two reasons:

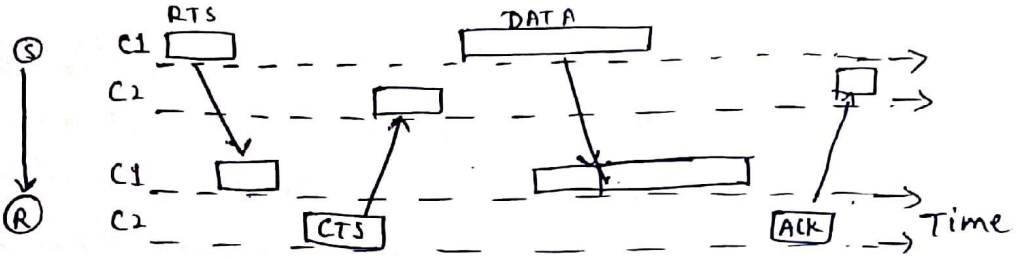
ⓐ any simultaneous transmission from Node 2 is prevented by its own carrier sense mechanism and

ⓑ the ack pkt received by node 3 may also be collided by transmission from node 2.

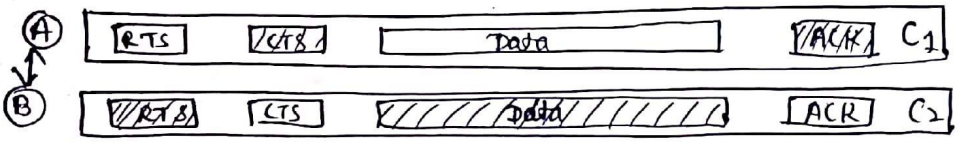
Similarly, node 6 is prevented by transmission because ack pkt originated by node 5 may collide with data pkt reception at node 4.

Therefore, nodes 2 & 6 are designated, as sender-exposed & receiver-exposed nodes, respectively.

→ ICSMA is a two-channel system with similar pkt exchange, RTS-CTS-DATA-ACK as that of CSMA/CD. The handshaking process is interleaved b/w two channels. This simple mechanism of interleaving carrier sense enhances the thoroughput achieved by two-channel.



Interleaved Pkt Transmission in ICSMA



Simultaneous Data Transmission b/w Two nodes

Operation of ICSMA protocol

→ ICSMA uses an extended n/w allocation vector (ENAV) to determine whether a particular channel is free for transmission. The ENAV is an extended form of NAV used for CSMA/CA schemes.

route discovery overhead.

Unit - II

* Issues in Designing a Routing Protocol for Adhoc Wireless N/w

- Mobility
- Bandwidth Constraint
- Error prone shared broadcast radio channel
- Hidden & exposed Terminal problems
- Resource Constraints

* Characteristics of Adhoc Routing Protocols

- Distributed Routing
- Adaptive to topology changes
- Proactive / Reactive Operation
- Loop-free routing
- Localized state maintenance
- Robust route computation & maintenance
- Optimal usage of resources
- Sleep mode operations
- Quality of service
- Security

* Responsibilities of Routing Protocols

- Performance
- Decision Time
- Decision Place
- Information Source
- Routing Strategy
- Adaptive Update Strategies

* Classifications of Routing Protocols

- Classified into four categories:

(i) Based on Routing Information Update Mechanism

(A) Proactive or Table-Driven Muting Protocols

→ Every node maintains the n/w topology info. in form of routing tables by periodically exchanging routing info.
→ Routing info. is generally flooded in whole n/w
→ whenever a node requires a path to a destination, it runs an appropriate path-finding algo. on the topology info. it maintains

(B) Reactive or on-demand routing protocols

→ Do not maintain the n/w topology info.
→ Obtain necessary path when it is required, by using a conn. establishment process

(C) Hybrid Routing Protocols

→ Combine best features of above two categories.
→ Nodes within a certain distance from node concerned, or within a particular geographical region, are said to be within routing zone of given node
→ For routing within this zone, a table-driven approach is used.
→ For nodes that are located beyond this zone, an on-demand approach is used.

(ii) Based on Use of Temporal Info. for Routing

(A) Routing Protocols using past temporal info

→ Use info about past status of links or status of links at time of routing to make routing decisions.

(B) Routing Protocols that use future temporal info

→ Use info about expected future status of the wireless links to make approx routing decisions.

→ Apart from lifetime of wireless links, the future status info also includes info regarding the lifetime of the node, prediction of location & prediction of link availability.

(ii) Based on Routing Topology

(A) Flat Topology Routing Protocols

→ Make use of a flat addressing scheme similar to the one used in IEEE 802.3 LANs

→ It assumes the presence of a globally unique addressing mechanism for nodes in an adhoc wireless n/w.

(B) Hierarchial Topology Routing Protocols

→ Make use of a logical hierarchy in the n/w & an associated addressing scheme.

→ The hierarchy could be based on geographical info or it could be based on hop distance

(iv) Based on Utilization of Specific Resources

(A) Power-aware Routing

→ Aims at minimizing consumption of battery power

→ Routing decisions based on minimizing power consumption either logically or globally in the n/w.

(B) Geographical Info Assisted Routing

→ Improves performance of routing & reduces the ctrl overhead by effectively utilizing the geographical info available.

* Table-Driven Routing Protocols

(i) Destination Sequenced DVR Protocol (DSDV)

- Based on RIP & only makes use of bidirectional links
- Pkts routed b/w nodes using Routing Table (RT) stored at each node. Each RT contains list of addresses of every other node in n/w & also the address of next hop for pkt to take in order to reach node.
- Every time n/w topology changes are detected, RT needs to be updated. RT maintain route metric (no. of hops) & route sequence no.
- Periodically or immediately if topology change, each node will broadcast an RT update pkt. To distinguish stale update pkt from valid ones, each update pkt is tagged by original node with a seq no.

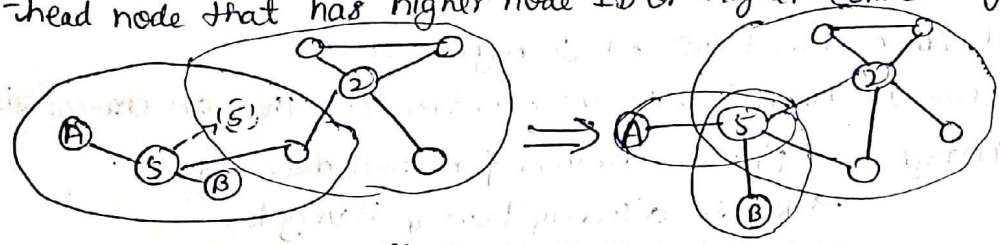
- Each time an update pkt forwarded, pkt also contains address of transmitting node apart from destination. Address of transmitting node entered into RT as next hop.
- Broken link detected by communication b/w or infered if no broadcast received for a while from former neighbour. Broken link described as metric of ∞ which causes RT entries of lost node to be flushed out.
- To avoid conflicts in seq. no., when topology changes, node generate even seq. no. for themselves & neighbours corresponding to link changes only generate odd seq no.
- RT updates can be sent into two ways:
  ⓐ Full Dump → send full RT to neighbours
  ⓑ Incremental Dump → only those entries sent that are changed since last update.
- Advantages: → Efficient Protocol for route discovery
  → Route discovery latency is very low
  → loop free paths guaranteed
- Disadvantages: → To maintain n/w topology, DSDV needs to send a lot of control tries
  → Generates high volume of traffic for high density & highly mobile n/ws.

(ii) Wireless Routing Protocol (WRP)

- Using WRP, each node maintains distance table, routing table, link-cost table & message retransmission list (MRL). An entry in RT contains distance to destination node, predecessor & successor along paths to destination & a tag to identify its state.
- Storing predecessor & successor in RT helps to detect loop & avoid count to ∞ problem.
- Entry in link cost table contains cost of link connecting to neighbour & no. of timeouts since an error-free msg was received from that neighbour.
- In WRP, using update msgs, mobile nodes exchange routing. Updated messages can be sent either periodically or whenever link-state changes happen. To ensure connectivity, if there has no change in its RT since last update, node required to send a "Hello" msg.
- On receiving update msg, node modifies its distance table & looks for better routing paths acc^n to updated info.
- Update msgs propagate from node to its neighbour only. An update msg contains following info:
  → identifier of sender → seq. no. assigned by sender
  → Update list of 0 or more updates or ACKs to update msgs
  → Response list of 0 or more nodes that should send an ACK to update msg.
- Advantages (unique from DSDV advantages): → Faster convergence & involves fewer table updates
- Disadvantages: → Demand more memory & processing power
  → Not suitable for highly dynamic & for very large adhoc wireless n/w

(iii) Cluster-Head Gateway Switch Routing Protocol (CGSR)

- Employs use of a hierarchial n/w topology
- Structure nodes in a given coverage area forms themselves into clusters.
- Each cluster provides coordination functionality b/w all nodes in cluster via a management node called 'Cluster-Head' which is elected dynamically by employing a 'least cluster change' (LCC) algorithm. LCC algo. determines that cluster-head node will change status if comes into range of another cluster-head node that has higher node ID or higher connectivity algo.



Cluster-Head Status change

- When routing info b/w clusters, it is called a cluster gateway.
- Clustering achieves allocation of BW b/w clusters by allowing different clusters to operate at different spreading codes (channels) on CDMA system.
- Cluster-Head responsibility to coordinate channel access via use of 'token-based' protocol.
- This protocol assumes all communications within cluster passes through cluster-head & any communication b/w clusters are routed via cluster-gateways.
- Every member node maintains a RT containing destination cluster-head for every node in n/w & also maintains a RT containing list of next hop for reaching every destination cluster.
- When node needs to transmit pkts, it must first be issued with a token from cluster-head, then obtain destination cluster head & next hop node from its cluster ~~head RT~~ member RT & destination RT before it can transmit.
- Adv :- Enables a level of coordination & efficient BW utilization
- Dis :- Problems of WRP & DSDV in highly mobile environment

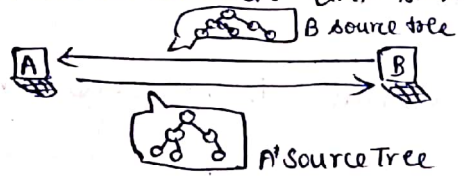
Source-Tree Adaptive Routing Protocol (STAR)

- Based on link-state algo that minimizes no. of routing updates pkts disseminated into n/w to save BW at expense of not maintaining optimum routes to destinations.
- It is a table-based Routing protocol, but aims to implement LORA. LORA attempts to minimize control overhead by :

(1) Maintaining path info only for dest. the router needs to support, i.e, active routes

(2) Using path found after flood search as long as paths are still valid, even if paths are not optimum.

- In STAR, each adhoc node maintains a source tree [The set of links used by router in its preferred path to a destination]. In STAR, a node knows its adjacent links of source trees reported by its neighbours. Each node runs a route selection algo on its own source tree to derive a RT that specifies successor to each destination
- STAR uses seq. nos. to validate link-state updates (LSUs).



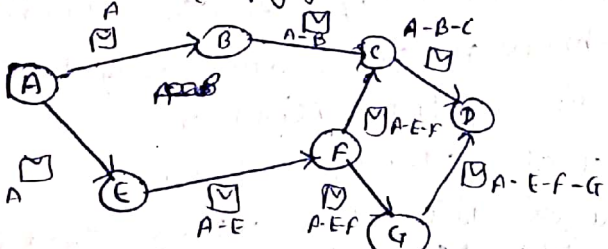
- STAR must perform ORA table-driven-based routing to construct source trees. Thereafter, LORA table-driven routing can be used to selectively perform updates.
- STAR has very low communication overhead among all table-driven routing protocols. LORA approach use reduces avg. ctl overhead to several other on-demand ~~RPs~~ routing protocols.

* On Demand Routing Protocols

(i) Dynamic Source Routing Protocol

- It is composed of the two mechanisms of Route Discovery & Route maintenance which work together to allow nodes to discover & maintain source routes to ~~arbitrary~~ arbitrary destinations in the n/w.
- Route Discovery

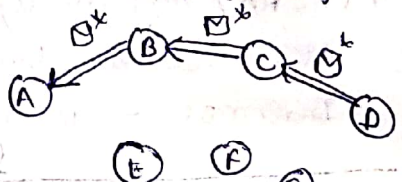
→ when a node has a pkt to send to some destination, it first checks its route cache to determine whether it has ~~a~~ route to the destination. If it has an unexpired route, it will use this route to send the pkt to destination. Otherwise, it initiates route discovery by broadcasting a route request pkt & reply is unicasted back to source (reply from dest. or intermediate node which knows path to dest.).



Propagation of Req. Pkt

A → D

→ propagation of Route Req. Msg.



M^x = A-B-C-D

⇒ Propagation of Rout reply. Msg

- Route Maintenance

→ carried out by use of route-error pkts & acks.

→ Route error pkt generated at node when data link layer encounters a fatal transmission problem. On receiving error pkt, a node removes hop in error from its route cache. It also truncates all routes containing the erroneous hop.

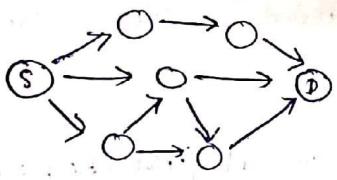
→ Acknowledgements are used to verify route links are operating correctly.

Adv: Routes maintained only b/w nodes which need to communicate reducing overhead of route maintenance. Route cache reduces route discovery overhead.

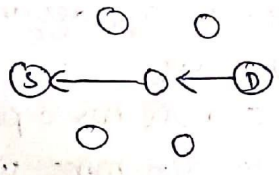
- Dis: Pkt header size grows with route length which leads to scalability problem.

(ii) Adhoc On-Demand DVR Protocol (AODV)

- Like DSDV, AODV provides loop-free routes in case of link breakage but unlike DSDV, it doesn't require global periodic routing advertisement.
- A feature of AODV is ability to provide unicast, multicast & broadcast communication
- Route Discovery process only initiated when routes are not used &/or they expired & consequently removed.
- AODV uses a broadcast route discovery algo & then unicast route reply msg.
- Route Discovery:
  - → when a node wants to send a pkt to some destination node & does not locate a valid route in its RT for that dest, it initiates route discovery process.
  - → Source Broadcasts route request (RREQ) pkt to its neighbours which forward it to its neighbours & so on. Source node uses an expanding ring search technique to ctrl n/w-wide broadcasts of RREQ pkts. In this technique, initially some TimeToLive (TTL) value set by source. If no reply within discovery period, TTL incremented by fixed amount & this process continued until threshold value reached.
  - → when an intermediate node forwards RREQ, it records address of address from which RREQ is received thereby establishing a reverse path.



RREQ propagation



RREP propagation

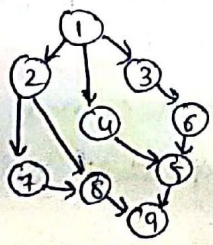
- Route Maintenance:
  - → If soure node move, reinitiate route discovery. If destination node or intermediate node move, nodes upstream of break remove routing entry & send route error (RERR) msg to affected active upstream neighbours.
- Adv: More Scalable than DSR & all advantages of DSR
- Dis: Intermediate nodes can lead to stale entries due to source seq. no. very old.

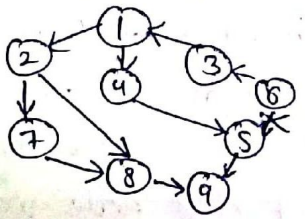
Comparison b/w DSR & AODV

Property	DSR	AODV
Loop free	Yes	Yes
Multicast routes	Yes	No
Distributed	Yes	Yes
Unidirectional Link Support	Yes	No
Multicast	No	No
Periodic Broadcast	No	Yes
QoS Support	No	No
Route Maintained In	Route Cache	Routing Table
Reactive	Yes	No

(iii) Temporally Ordered Routing Algorithm (TORA)

- Its intended use is for IP datagrams within an autonomous system. Depending upon topological changes, ordering of algo reactions will change subsequently.
- TORA was designed with following properties:
  - → Distributed in nature
  - → Establishes routes quickly
  - → Provides loop free & multiple routes
  - → Minimizes communication
- TORA can be separated into three basic func^{n}s: creating routes, maintainging routes & erasing routes:
  - → Creating routes require establishment of seq. of directed links leading from node to destination & only initiated when a node with no direct link require route. It uses query/reply process to build DAG rooted at destination.
  - → Maintaining routes refers to reacting to topological changes in n/w in a manner such that routes to dest. are re-established within finite time.
  - → Erasing Routes: Upon detection of n/w partition, all links must be marked as undirected to erase invalid route.
  - → TORA uses three ctrl pkts: Query (QRY) → for creating routes
    Update (UPD) → for maintaining routes
    Clear (CLR) → for deleting routes
- The general idea of this protocol is to build and maintain Directed Acylic Graph (DAG) routed at destination.
- A node receiving QRY does following:
  - (i) If RR (Route Request) flg = 1, discard QRY pkt.
  - (ii) If RR=0 & no downstream links for dest. exists, broadcast QRY pkt.
- A node receiving UPD does following:
  - (i) If RR = 1 & reflection bit of neighbour height = 0, increments value of neighbour's height in pkt & stores this as height. It then send updated UPD msg which includes its height to its neighbour.
  - (ii) If RR = 0 & reflection bit set, only updates neighbour's entry in table.
- When a node detects n/w partition, it generates CLR pkt which is flooded in n/w.





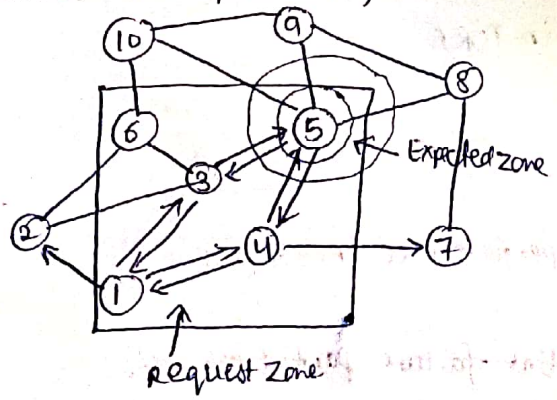
Directed Paths in TORA

- Adv:
  - → creates DAG when necessary
  - → reduces n/w overhead
  - → perform well in dense n/w
- Dis:
  - → not used because DSR & AODV perform well than TORA.
  - → It is not scalable
  - → Long time taken to converge if link failure partitions n/w.

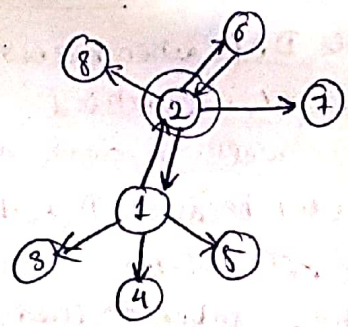
Property	DSDV	DSR	TORA
Category	Proactive	Reactive	Hybrid
Metrics	Shortest path	Shortest path next available	Shortest path next available
Route Recovery	Periodic broadcast	New route, notify source	Reverse Link
Route Repository	Routing Table	Route Cache	Routing Table
Broadcasting	Simple	Simple	Simple
Loop free	Yes	No provision for it	Yes
Communication Overhead	High	High	High
Feature	Distributed Algo.	Completely on demand	Ctrl pkts localized to area of topology change

(iv) Location-Aided Routing (LAR)

- It makes use of GPS. Using GPS, it is able to obtain info^n regarding location of a node.
- In sensor n/w, every node configured with directional antenna & few sensor (called anchor nodes) nodes have GPS receivers. These nodes help other normal nodes to localize them based on reference info provided by these anchor nodes.
- For localization, s/w used in two phases:
  - → First one queries sensor n/w & gathers info about neighbours, distance & angle
  - → Second one is used to compile s/w for sensor nodes.
- In LAR scheme, routes established using flooding in intelligent way; when a path is broken or when a node needs to establish a route to dest. then it initiates route discovery by using route request msgs.
- When an intermediate node receives same RREQ from 2 different nodes, it discards one of them & forwards other msg. When it receives RREQ, it compares address with its own & finding it is intended dest., it triggers RREP pkt in reverse direction otherwise route discovery.
- Timeout specified to receive RREP pkt other route discovery again.
- LAR use expected zone & request zone. Expected zone may be defined as a circular region within which dest. node is expected to be present; it is just an estimation region in which dest. node may be present.
- Request zone is defined as rectangular region within which a node forwards pkt. The size of request zone is dependent on "avg speed of node & time elapsed since last position of dest. node was found out."



LAR1 scheme

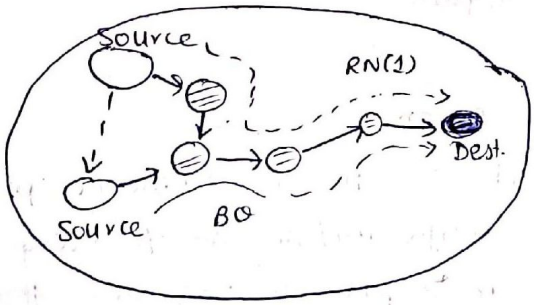


LAR2 scheme

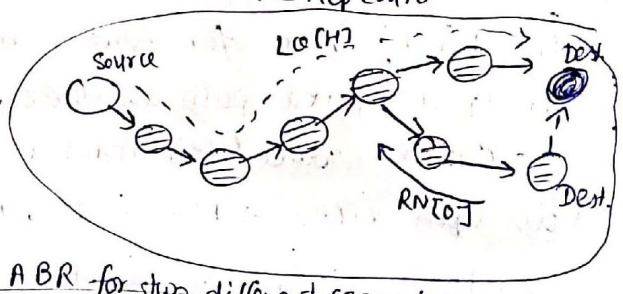
- In LAR1 scheme, node broadcast to nodes within request zone & nodes outside request zone discard the pkt.
- In LAR2 scheme, it is assumed that location of dest. is known to source node. Intermediate nodes in path check if distance ~~mentioned in RREQ~~ calculated ⇐ is less than distance in RREQ, the pkt is forwarded else discarded.
- Adv: Reduce ctrl overhead, increased use of BW utilization
- Dis: Can't be used in situations where no GPS info available

(v) Associative-Based Routing

- It also uses source-initiated method, i.e., only maintains routes for sources that actually desire routes.
- 3 phases of ABR are: → Route Discovery → Route Reconstruction (RRC) → Route Deletion
- Route discovery phase is accomplished by broadcast query (BQ) & a wait reply cycle (REPLY)
- A node desiring a route broadcast BQ msg. All nodes receiving BQ append their addresses & their associativity ticks with neighbour along BQS info to BQ pkt. Successor node erases its upstream node neighbour associativity & retains only entry concerned with itself & its upstream node.
- If multiple path with same associativity, then route with min no. of hops selected & REPLY pkt unicasted along selected path & intermediate nodes of selected path mark their routes valid.



RN = Remove ~~invalid~~ node (used to remove invalid route)
LQ[H] = Localized Query
H = Hop Count



Route Maintenance in ABR for two different scenarios

- Adv: Routes selected tend to long-lived
- Dis: Scalability problem due to limited BW

(vi) Signal Stability-Based Adaptive (SSA) Routing protocol

- SSA is a variant of AODV protocol to take advantage of info available at link level. Both signal quality of links & link congestion are taken into consideration when finding routes.
- Path with strong signal links are favoured over optimal paths.
- It is an on-demand routing protocol that selects routes on the basis of the signal strength b/w nodes & a node's location stability.
- It is composed of two cooperative protocols:
  → Dynamic Routing Protocol (DRP) & Static Routing Protocol (SRP)

- DRP maintains Signal stability Table (SST) & RT. SST stores signal strength of neighbouring nodes obtained by periodic beacons from link layer of each neighbouring node. Signal strength either recorded as strong or weak channel. All transmissions are received by DRP & processed. After updating the appropriate table entries the DRP passes pkt to SRP.
- SRP passes pkt up stack if intended receiver. If not looks for dest. in RT & forwards pkt. If no entry for dest in RT then initiate route search process to find route using RREQ. If source time out before receiving reply, it changes PREP field in header to indicate weak channels are acceptable.
- When link failure, intermediate nodes send error msg to source indicating which channel ~~fails~~ failed. Then source send erase msg to notify all nodes of broken link & initiate a new route search to find new path to dest.
- Adv: More stable routes find compared to DSR & AODV.

Dis: Puts strong RREQ forwarding Cond^n which results in RREQ failures.

(vii) Flow-Oriented Routing Protocol (FORP)

- It uses a prediction based scheme for selecting & maintaining routes in case of link failures. It has unique prediction based mechanism that utilizes mobility & location info if each node to estimate link expiration time (LET). This protocol frequently predict a route expiration time (RET) for given path & finds alternate path before expiration of current used path.

- Route Establishment
  - (i) First source node check for route in RT. ~~If un~~
  - (ii) If unexpired path available, use it else broadcast Flow-REQ pkt which carrier source/dest. nodes & flow identification / seq no for every session.
  - (iii) Upon receiving Flow-REQ, if seq no. > previous node value then update address on pkt else discard request.
- Flow-setup Pkt
  - (i) When REQuest received at dest, Calculate RET acc^n to REQ is better than RET value of currently used path then originate Flow-setup pkt.
- Route Maintenance
  - (i) If dest. detects route break about to occur, it send Flow-Handoff pkt to src. node (similar to Flow-REQ mechanism). ~~When src nod~~
  - (ii) When src node receives Flow-Handoff pkt, Calculate RET for each path & select new path.

Adv: Reduces path breaks & their associated ~~side~~ ill effects.

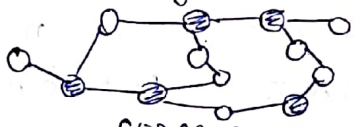
Dis: Requirement of time sync increase ctrl overhead.

Parameter	On-Demand Routing	Table-Driven Routing
Availability of Routing Info	Available when needed	Always available regardless of need
Routing philosphy	Flat	Mostly Flat
Periodic Mute Update	Not required	Required
Mobility Handling	Use localized route discovery	Inform other nodes to achieve a consistent Routing Table
Congestion	Less Congestion	More congestion due to periodic update of route
Delay	More end-to-end delay as each time route be discovered first	Less end-to-end delay as route is already created
Routing Attack	Less prone to routing attacks as route is created on demand	More prone to routing attack

* Hybrid Routing Protocols

① Core Extraction Distributed Adhoc Routing (CEDAR) protocol

- Based on on-demand routing protocol to reduce problems is follows:
  - Ⓐ Node mobility difficulty for real time applications & for routing computation & update
  - Ⓑ How to find an effective route in current topology of n/w & QOS is a big &
  - Ⓒ Flooding of pkts is a problem if every node request info to whole n/w.
- Key components of CEDAR are core extraction, link state propagation & computation
- Core Extraction
  - → CEDAR selects a subset of the nodes of adhoc n/w as core nodes, which form Core set of the n/w. The core set is an approx of min. dominating set (MDS) & (Dominating set ~~is a set~~ of neighbour is a set of nodes such that every node in n/w is either DS or is a neighbour of Ⓓ a node in DS)



→ Part of Core

CEDAR Core set

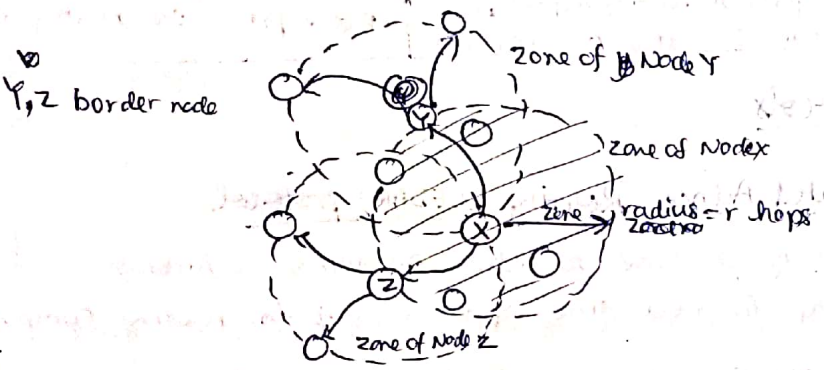
- Link State Propagation
  - → CEDAR requires core node to have up-to-date info about its local topology & also maintain link state of stable high-BW links further away in n/w. This ensures adaptability in a highly dynamic n/ws & approach optimal route computation in highly stable n/ws.
  - → Goal of stability & BW based link-state propagation is achieved by CEDAR using so-called increase & decrease waves. An increase wave propagates an increase of BW & decrease wave propagates a decrease of BW on a certain link.
- Route Computation
  - → on-demand routing algo for QOS route computation. Either a suitable path to dest. node is found or local path calculations will fail to provide a path with requested QOS.
  - → In case of success, concatenation of partial paths calculated by core node provides endtoend QOS path.

Adv: Perform both routing & QOS path optimization very efficiently with help of core nodes.

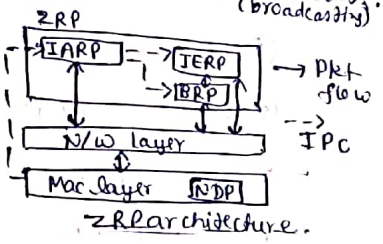
- Dis: Movement of core nodes adversely affects the performance of the protocol.

(ii) Zone Routing Protocol (ZRP)

- Hybrid routing protocol conceived to tackle demerits of reactive & proactive routing approaches.
- ZRP utilizes zone concept in which proactive routing is exploited within zone & reactive is employed out of the zone.



Hybrid Approach ZRP



ZRP architecture.

- Construction elements of ZRP are as follows:

(A) Neighbour discovery protocol at MAC layer (NDP)

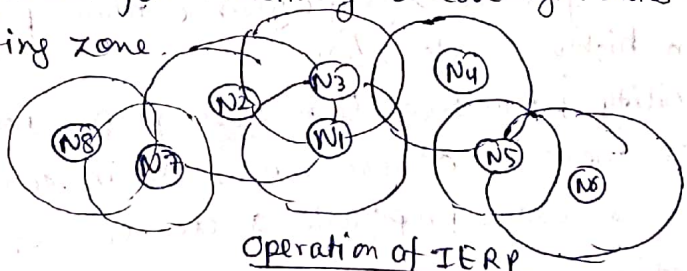
→ It helps nodes identify their neighbours through broadcasting hello beacons.

(B) Intra-Zone Routing Protocol (IARP)

→ In ZRE each node maintains the routing info of all nodes within its routing zone. Node learns the topology of its routing zone through a localized proactive scheme refered as IARP.

(C) Inter Zone Routing Protocol (IERP)

→ It is responsible for reactively discovering routes to destination beyond a node's routing zone.



Operation of IERP

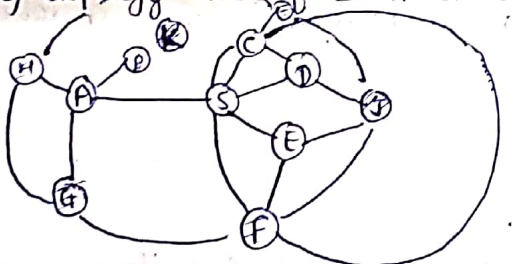
(D) Border-Cast Routing Protocol (BRP)

→ The broadcasting pkt delivery service is provided by BRP.

- Adv: Reduces ctrl overhead compared to RREQ flooding mechanism
- Dis: In absence of query ctrl, it tends to produce higher ctrl overhead.

(iii) Zone-Based Hierarchial Link State Routing Protocol (ZHLS)

- It is a zone based hierarchial LSR protocol that makes use of location info in a novel peer-to-peer hierarchial routing approach.
- N/w is divided into zones that do not overlap. Initially, each node knows its own position & therefore zone ID through GPS. After n/w is established, each node knows ~~its own position & therefore zon~~ the low level topology (node level) about node connectivity within its zone & high level (zone level) topology about zone connectivity of whole network.
- A pkt is forwarded by specifying the hierarchial address - zone ID & node ID - of a destination node in pkt header. No cluster heads in this protocol. ZHLS is a hybrid reactive/proactive scheme. It is proactive if dest. within same zone of src. else reactive because need to search location to find zone ID of dest.
- It requires GPS & maintains a high level hierarchy for interzone routing. Location search is performed by unicasting one location request to each zone. Routing is done by specifying zone ID & node ID of dest.
- Each node determines its zone ID by mapping its physical location to a zone map whose size depends on node mobility, n/w density, transmission power & propagation characteristics.
- Two levels of topology are defined in ZHLS: node level topology & zone level topology.



Node Level Topology

- Adv: Reduces storage requirements & communication overhead created because of mobility, zone level topology robust & resilient to path breaks, intra-zonal topology changes do not generate n/w-wide ctrl pkt transmissions
- Dis: Additional overhead in creation of zone-level topology.

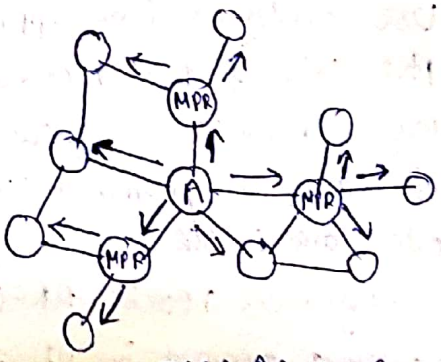
* Routing Protocols with Efficient Flooding Mechanisms

(i) Preferred Link-Based Routing Protocols

- Use preferred link approach in an implicit manner by processing a Route Request (RREQ) pkt only if it is received through a strong link.
- Here a node selects a subset of nodes from its Neighbours List (NL). This subset is referred to as 'preferred list' (PL), selection of this subset may be based on link or node characteristics.
- All neighbours receive RREQ pkts because of broadcast radio channel, but neighbours present in PL forward them further.

- Each node maintains info about its neighbours & their neighbours in a table. Called 'Neighbour's Neighbour Table (NNT). It periodically transmits a beacon containing the changed neighbour's information.
- Route Establishment
→ If dest. is in src's NNT, route is established directly. Otherwise, src transmits a RREQ pkt. A node is eligible for forwarding a RREQ only if
present in NL # TTL of pkt > 0
If dest. in NNT, RREQ unicasted to the neighbour (whose NL contain dest.)
If computed PL empty, RREQ discarded & marked sent.
→ If RREQ reaches dest., route is selected by route selection procedure.
- Route Selection
→ When multiple RREQ reach dest, route selection procedure selects best route among them. Criteria for selection can be shortest path or least delay path or most stable path. (After 1st RREQ, dest starts timer after which no RREQ accepted.
→ After selecting a route, all subsequent RREQ pkt for same src discarded.
→ If node delay flag set, route selection procedure omitted & first RREQ route of reaching dest is selected as route.
- Algo for Preferred Link Computation: Neighbour Degree Based Preferred Link Algo (NDPL), Weighted Based Preferred Link Algo (WBPL)
- Adv: → minimizes broadcast storm problem so highly scalable
→ reduction in ctrl overhead results in decrease in no. of collisions & improvement in efficiency of protocol.
- Dis: Computationally more complex

9. (ii) Optimized Link State Routing
- It is a proactive protocol based on Link state Algo. In link-state routing protocols, nodes transmit routing advertisement (LSA - Link State Advertisement) listing their neighbours by flooding throughout n/w.
- It incorporates concept of multipoint relays (MPRs) which optimize flooding of link-state update.
- Each node assigns task of propagating its LSAs only to few of its one-hop symmetric neighbours. These special nodes are selected in a way that ensures that LSAs will reach all of its two-hop neighbours. Those node selected for relaying the LSAs are MPRs.
- Each node transmits hello msgs periodically.
- Hello msg enable a node to discover its one-hop neighbours.
- Link-state updates are transmitted through n/w via a msg that is called a topology control (TC) msg.
- TC msgs are flooded throughout n/w & every node can then recalculate its own RT using this info.



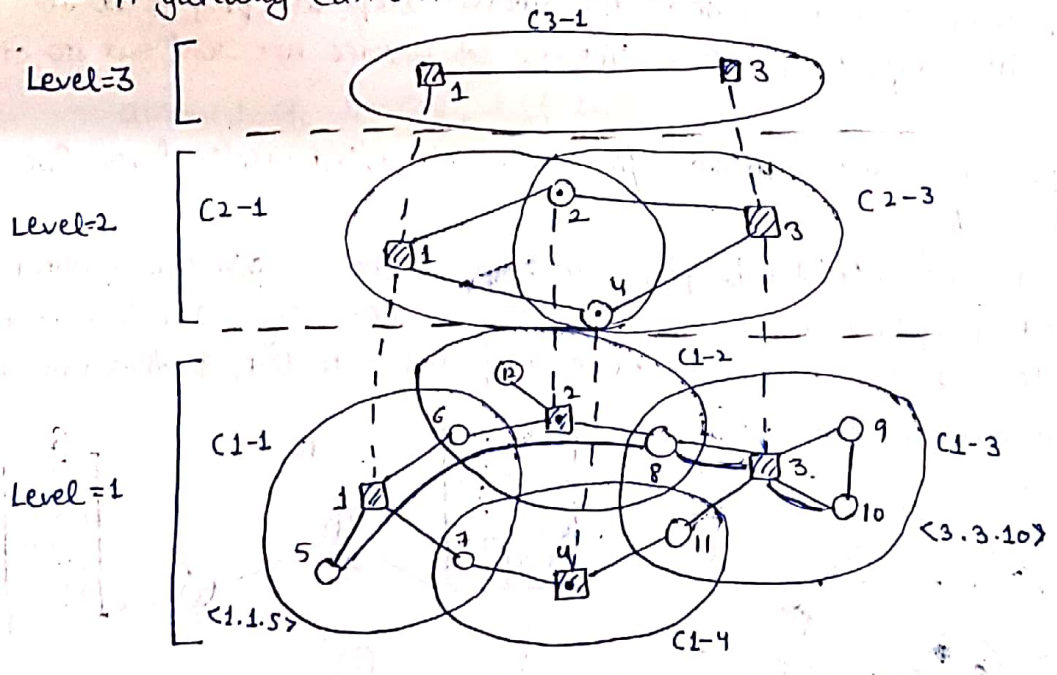
OLSR Protocol

- OLSR also includes two additional msg types: host & n/w association (HNA) msgs that are used by nodes for advertising connectivity to external networks & the multiple interface declaration (MID) msgs that are ~~stored~~ used only by nodes that have multiple interfaces that are participating in OLSR protocol.
- Adv: → Reduces Routing overhead & no. of broadcasts done.
  → Low connection setup time & reduce ctrl overhead

* Hierarchial Routing Protocol

(i) Hierarchial State Routing Protocol (HSR)

- Characteristic features are multilevel clustering & logical partitioning of mobile n/w nodes.
- Cluster heads at low level becomes member of next higher level. These new virtual cluster member organize themselves again into clusters & so on.
- The IDs at level 0 are physical addresses. ~~Higher level IDs~~ Those upper level clusters are only virtual with so-called virtual links b/w nodes.
- A node in a virtual cluster floods info that it obtains to its lower level so each node has a hierarchial address called HID (Hierarchial ID) which can be considered as a series of MAC addresses.
- A gateway can have more than one HID.



▣ – Clusterhead ⊙ – Gateway node ○ – Internal node

<x.y.z> Hierarchial ID. — Path path from S to 10

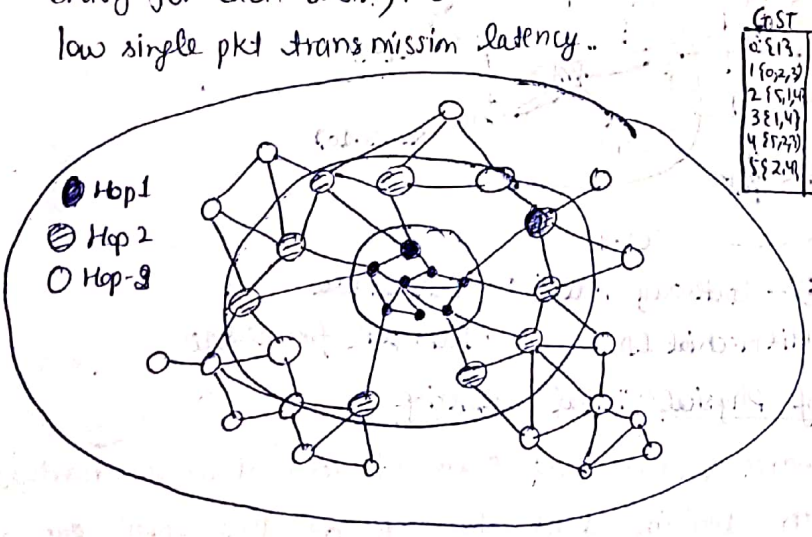
Example of Physical/Virtual Clustering

- Nodes within a cluster exchange virtual link state info as well as summarized lower level cluster info. After obtaining link state info at this level, each virtual node floods it down to nodes within lower level of cluster. As a result, each physical node has a "hierarchial" topology info, as opposed to a full topology view as in flat LS schemes.
- The hierarchial address is sufficient to deliver a pkt to its dest. from anywhere in the n/w using HSR tables.

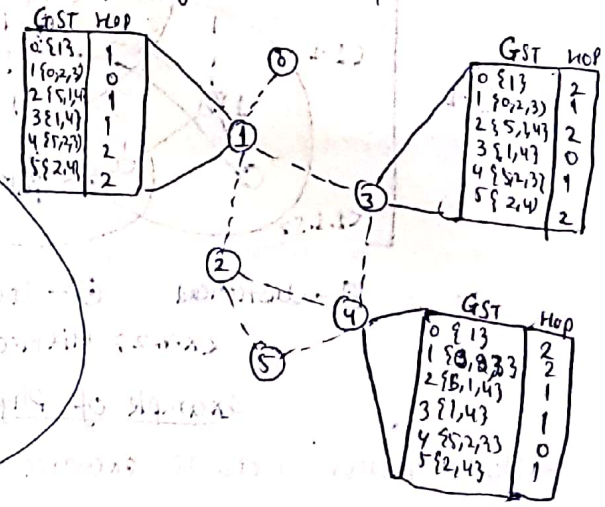
- Adv: A flat LS requires $O(N^M)$ entries, Hierarchial routing only requires $O(N \times M)$ entries in hierarchical map. Thus RT storage greatly reduced.
- Dis: Need to maintain a longer (hierarchical) address & cost of continuously updating the cluster hierarchy & hierarchial address as nodes move.

(ii) Fisheye State Routing Protocol (FSR)

- Uses "fisheye" technique (details decrease as distance from focal pt. increases). In routing, fisheye approach translates to maintaining accurate distance & path quality info about immediate neighbourhood of node with progressively less detail as distance increases.
- FSR built on top of Global State Routing (GSR):
  - → GSR maintains a topology map at each node similar to LSR. In LSR, link state pkts generated & flooded in n/w whenever topology change detected. In GSR, link state pkts not flooded. Instead, nodes maintain a link state table based on up-to-date info received from neighbouring nodes & periodically exchange it with their ~~inner~~ local neighbours only (no flooding)
  - → LSR causes excessive overhead & GSR avoids this problem.
- FSR protocol
  - → Entries corresponding to nodes within the smaller scope are propagated to the neighbours with highest frequency. The rest of entries are sent out ~~to~~ at a lower frequency.
  - → This strategy produces timely updates from near stations, but creates large latencies that from stations afar.
- FSR scales wells to large n/w by keeping link state exchange ~~of~~ ~~low~~ without compromising route compilation accuracy when dest. is near. By retaining a route entry for each dest., FSR avoids extra work of "finding" the dest. & thus maintains low single pkt transmission latency.



Scope of fisheye



Msg Reduction using Fisheye

- Adv: Significantly reduce BW consumed by link state update pkts, suitable for large & highly mobile adhoc wireless n/w.

* Power-Aware Routing Protocols

(i) Power-Aware Routing Metrics Considered in Power-Aware Routing Protocol

- Minimal Energy Consumption per pkt
  → It aims at minimizing power consumed by a pkt in traversing from src to dest.
- Maximum N/w Connectivity
  → This metric attempt to balance routing load among cutset.
- Maximum Variance in Node Power levels
  → This metric proposes to distribute load among all nodes in n/w so that power consumption pattern remains uniform across them.
- Minimum Cost Per Pkt
  → In order to maximize life of every node in n/w, this routing metric is made as a func^n of state of the node's battery.
- Minimize Maximum Node Cost
  → This metric minimizes the max cost per node for a pkt after routing a no. of pkts or after a specified period.

(ii) Routing Protocols Based on Node Energy Status

Routing protocols in this category take into account the node energy status using residual energy or energy drain rate. Residual energy gives the amount of battery power left before a node dies down, & drain rate specifies energy dissipation rate of a node.

- Minimum Battery Cost Routing (MBCR) → considers residual energy of node as routing metric
- Min-Max Battery Cost Routing Scheme (MMBCR) → Extension of MBCR
- Device-Energy-Load-Aware Relying Framework (DELAR) → Exploits feature of device heterogenity in an adhoc n/w & routing metric are residual energy & congestion status of node
- Location-Based Link Stability & Energy-Aware Routing (LAER) → Routes selected on minimizing energy consumption & maximizing link stability. Using multi-objective model, LAER able to address appl^{n}s with different QOS constraints.
- Energy-Efficient (EE) mechanism → Provides balanced usage of node residual energy & reduces failure degree of node. Select energy optimized route from set of multiple routes with min hop count & high residual energy.
- Power & Mobility-Aware Routing (PMAR) → A dual metric involving both energy & transmission power.
- M-channel framework for MANETs → Two modules: (a) Energy module involves path selection based on min energy drain rate of a node. (b) Delay module (b) Delay-aware module computes delay metric with help of OLSR Hello & Ack pkts.

(iii) Routing Protocols Based on Transmission Control Power

- Minimum Total Transmission Power Routing ~~scheme~~ (MTPR): Attempts to minimize total energy consumption of nodes participating in selected route.
- Power-Aware Routing Optimization (PARO): where neighbouring nodes listen to an ongoing ~~transmission~~ communication & inserts itself in b/w if it can lead to energy savings for transmissions.
- Conditional MMBCR (CMMBCR): Considers both total transmission energy consumption of routes & residual energy of nodes
- Energy-Aware Geolocation-Aided Routing (EAGER): Energy based routing scheme which dynamically adjust cell size based on msg arrival ~~time~~ rate & topological variation rate.
- Location-Aided Power-Aware Routing (LAPAR): Location-based greedy routing strategy that uses relay regions as a medium for forwarding pkts to dest.
- Small Minimum Energy Communication N/w (SMECN)

Classification of Power Aware Protocols

Routing Protocol	Class	Multiple Metrics	Delay Aware	Topology Control	MANET size support scall
DELAR	Proactive	Yes	Yes	No	Medium
LAER	Location-based greedy routing	Yes	No	No	Medium
DPC	Protocol Independent	No	No	Yes	Medium
EAGER	Hybrid	No	Yes	Yes	Large
E2	Protocol Independent	No	Yes	No	Small
PMAR	Location-based reactive routing	Yes	Yes	No	Small
Ext MChannel	Proactive	Yes	Yes	No	Medium
PEER	Reactive	No	Yes	No	Medium
LAPAR	Location-based greedy routing	No	No	Yes	Medium
SMECN	Location-based	No	Yes	Yes	Large

* Issues in Designing a Transport Layer Protocol for Adhoc Wireless N/ws

(i) **Induced Traffic**: In a path having multiple link, the traffic at any given link (path) due to traffic through neighbouring links (or paths) is referred as induced traffic.

(ii) **Induced Throughput Fairness**: It refers to throughput unfairness at transport layer due to throughput unfairness existing at the lower layer such as n/w & MAC layer

(iii) **Separation of Congestion Control, Reliability & Flow Control**: The protocol can provide better performance if reliability, flow-control & congestion ctrl are handled separately.

(iv) Power & Bandwidth Constraints

(v) Interpretation of Congestion

(vi) Completely Decoupled Transport Layer

(vii) Dynamic Topology

* Design Goals of a Transport Layer Protocol for Ahoc Wireless Networks

(i) It should maximize throughput per connection.

(ii) It should provide fairness across competing flows.

(iii) It should have reduced e-connection setup & connection maintenance overheads.

(iv) It must facilitate scalability in large n/ws by reducing requirements for setting up & maintaing connections.

(v) It should offer both reliable & unreliable connections.

(vi) It should be able to adapt to mobility & change in topology of adhoc wireless n/w.

(vii) It should be aware of limitations & resource constraints.

(viii) It should make use of information from lower layer.

(ix) It should offer a well-defined cross-layer interaction framework.

(x) It should also maintain end-to-end semantics.

* TCP Over Adhoc Wireless N/w

- TCP doesn't perform well when it is used in wirelessadhoc n/ws (WAH Ns) because of following:
  - → Misinterpretation of packet loss
  - → Frequent path loss
  - → Effect of path length
  - → Misinterpretation of congestion window
  - → Asymmetric Link Behaviour

* Classification of Transport Layer Sol^{n}s

- Based on Layered Architecture of OSI stack

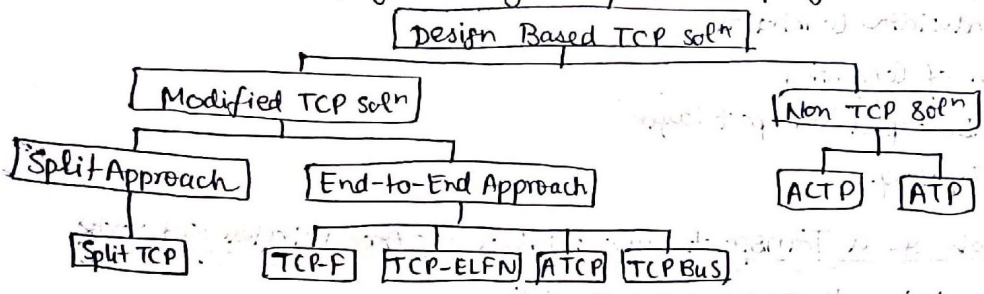
Cross-Layer Soln: Dependent on interaction b/w any two layers of OSI stack.
(i) TCP & n/w (ii) TCP & link (iii) TCP & physical (iv) N/w & physical

(B) Single-Layered Soln: Rely on adapting a layer of OSI stack in isolation that is independent of any other layer.
(i) TCP layer (ii) N/w layer (iii) Link layer

— Based on Engineering or Design Approach

(A) TCP over Adhoc N/ws or Modified TCP soln's: Obtained by tweaking existing TCP

(B) Non-TCPs: Developing entirely new protocols specific to need WAHNs.



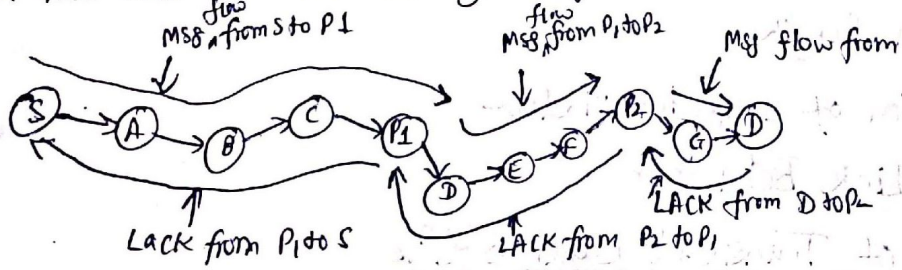
— Split Approaches: The fairness and throughput of TCP suffer when it is used in mobile area n/ws, i.e., as length of path increases, overall degradation of throughput also increases

① Split TCP: → The scheme splits the transport layer objectives into congestion ctrl & reliable pkt delivery.

→ Split-TCP splits long TCP connections into shorter localized segments or zones. This is done in order to improve the performance in terms of fairness.

→ It uses a no. of selected intermediate node b/w these localized segments known as proxy node. If a pkt needs to be transmitted, proxy node receives TCP pkt; when it intercepts TCP pkt, it reads ~~it read~~ the content of pkts, buffers them in local buffer & send ack to src or previous proxy node. This ack is known as local ack (LACK) & proxy node takes responsibility of delivering pkt further, at an appropriate rate, to next local segment.

→ Upon receipt of LACK, a proxy will purge pkt from its buffer. The forwarded could possibly be intercepted again by another proxy & so on. No change in the end-to-end ack system of TCP.



TCP with proxies P1 & P2

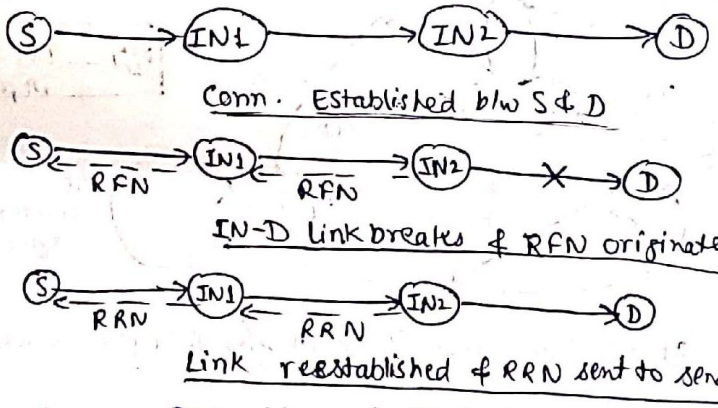
→ End-To-End Approach: Addresses problem of TCP's misinterpretation of pkt losses due to n/w congestion in mobile adhoc networks.

① TCP Feedback (TCP-F)

→ Employs feedback based approach & intends to minimize the throughput degradation resulting from rapid change in mobility of topology due to mobility of mobile hosts.

→ Whenever an intermediate node detects line break, the intermediate node sends a route failure notification (RFN) pkt toward sender. This intermediate node maintains info about all the RFN pkts it has originated so far & updates its RT acc"ly.

→ When sender receives RFN, it goes into snooze state in which it stops sending any more pkts to dest., freezes all its timers & congestion window & setups a route failure timer (time required to reestablish ~~connection~~ route). When this timer expires, sender changes state to active state & receive info about route from intermediate node through Re-Establishment Notification (RRN) pkt.



Operation of TCP-F

→ Advantages: # Simple feedback brings a good soln to minimize problem due to frequent failure in links
Good congestion ctrl mechanism

→ Disadvantage: # Implementation of TCP-F requires modification of existing TCP libraries.

② TCP with Explicit Link Failure Notification (TCP-ELFN)

→ It is an interface b/w TCP & routing protocol. The interface plans to update the TCP agent on route failures when they arise.

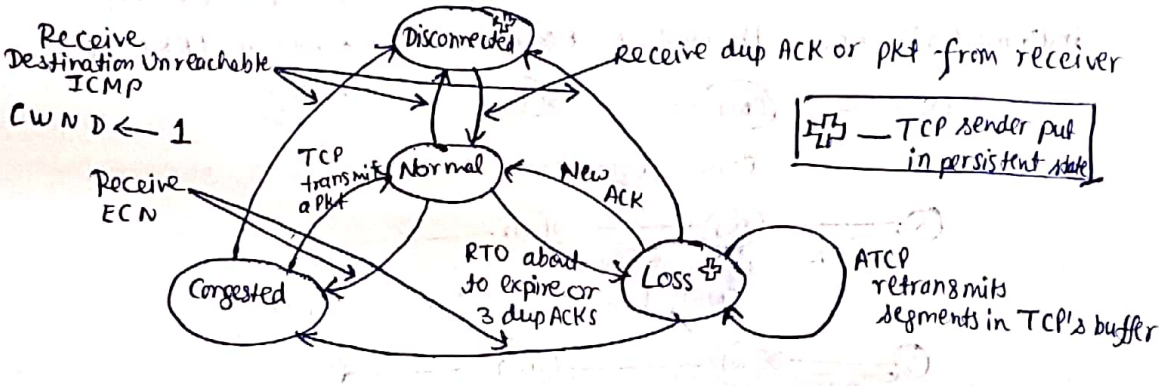
→ To execute ELFN msg, DSR error route msgs are adapted to carry a payload. As a TCP sender gets an ELFN, it stops its retransmission timers & enters a "standy-by" mode (similar to snooze mode in TCP-F). Link breakage info in ELEN is carried with adapted route error msgs. The link failure is moved up to transport layer only at TCP sender.

→ Adv: Improves TCP performance, less dependent on routing protocol & requires only link failure notification about path break.

→ Disadv: # when n/w temporarily partitioned, path failure may last longer.
Congestion window used after new route obtained may not reflect achievable transmission rate acceptable to the n/w & TCP receiver.

(3) Adhoc TCP (ATCP)

→ It also uses a n/w layer feedback mechanism to make TCP sender aware of status of the n/w path over which TCP pkts are propagated.
→ Based on feedback info received from intermediate nodes, TCP sender changes its state to the persist state, congestion state, or retransmit state.
→ When an intermediate node finds n/w partitioned, TCP sender changed to persist state where it avoids unnecessary retransmissions. TCP congestion window size reduced to one which forces TCP to probe correct value of Congestion window to be used for new route.
→ If an intermediate node loses a pkt due to error, sender immediately retransmits it without invoking congestion ctrl algo.



State Transition Diagram for ATCP at sender

→ Adv: # Significant improvement in TCP performance while maintaining end-to-end semantics of TCP.
Compatibility with Traditional TCP.
→ Disadv: # Dependence on n/w layer to detect route failure & n/w partitions
Inclusion of a think ATCP layer to TCP/IP protocol stack that need changes in inter foretimes.

(4) TCP-BuS

→ In TCP-BuS proposal an explicit route disconnection notification (msg) (ERDN) is generated at an intermediate (pivoting node) node upon detection of route failure. This msg propagated to source which then stops transmission. Pkt Transmission is resumed after a partial path has been reestablished from node which detected route failure to dest. & that info. is relayed to TCP sender in an explicit route successful notification (ERSN).
→ Five enhancement features in TCP-BuS are:
Explicit Notification: Route failure → ERDN to sender by pivoting node

Route re-establish → ERSN to sender

Extending Timeout Values: Buffered pkts transmission delay may cause TCP sender to timeout, TCP-BuS avoids this timeout by doubling the transmission timeout value associated with these buffered pkts.

Avoid Unnecessary Requests for fast retransmission: TCP-BuS works with ABR mechanism to suppress duplicate ACK msg originated due to buffered pkts.

Reliable retransmission of ctrl msg: Reliability is achievable through overhearing the wireless communication channel after transmitting ctrl msgs.

→ Adv: # Improved performance
Uses of buffering, seq. no. ing & selective ack nowledge, thus avoiding fast retransmission

→ Disadv: # More dependency on routing; protocol & buffer at intermediate node
Performance adversly affected, in event of failure of intermediate nodes

Comparison b/w Different End-to-End Approaches

	TCP-F	TCP-ELFN	ATCP	TCP-BuS
High BER pkt loss	Not handled	Not handled	Handled	Not handled
Route Failure (RF) detection	RFN pkt freezes sender state	ELFN pkt freezes TCP sender state	ICMP "Destination unreachable" freezes TCP sender state	ERDN pkt freezes TCP sender state
Route Reconstruction (RR) detection	RRN pkt resumes TCP to normal state	Probing mechanism	Probing mechanism	ERSN pkt resumes TCP to normal state
Packet ordering	Not handled	Not handled	Handled	Not handled
Congestion window (CW) & Retransmission Time-out (RTO) after RR	Old CW & RTO	Old CW & RTO	Reset for each new route	old CW & RTO
Reliable transmission of ctrl messages	Not Handled	Not Handled	Not Handled	Handled
Evaluation	Emulation; no routing protocol considered	Simulation	Experimental; no routing protocol considered	Simulation

* Other Transport Layer Protocols for Adhoc Wireless N/ws

① Appl^n Controlled Transport Protocol (ACTP)

- ACTP is lightweigh & not an extension of TCP.
- Supports priority of pkts to be sent but lower layer responsibility to actually provide DS (Differential services) based on priority.
- Executed as a layer b/w appl^n & n/w layer.
- Scalable for large ~~nos~~ n/ws
- Allows appl^n complete ctrl in deciding the level of reliability & QOS for different portions of a data stream.
- Adv: # Freedom of choosing required reliability level to the appl^n layer.
Scalable to large n/ws
- Disadv: # Not ~~Compatibi~~ compatible with TCP

② Adhoc Transport Protocol (ATP)

- Not a variant of TCP
- Major aspects:
  → Coordination among multiple layers → rate based transmissions
  → decoupling congestion ctrl & reliability → assisted congestion ctrl.
- ATP uses services from n/w & MAC layers for improving its performance
- Uses info from lower layers for estimation of initial transmission rate, detection, avoidance & control of congestion, & detection of path breaks
- Relies on cross-layer info sharing
- Employs explicit feedback from other n/w nodes to assist in the transport layer mechanisms
- Intermediate Nodes in ATP maintain state information for queuing & delay, aggregated for all pkts traversing the node.
- Adv: # Improved performance, decoupling of congestion ctrl & reliability mechanisms, & avoidance of congestion window fluctuations
- Disad: # Lack of interoperability with TCP

* Security in Adhoc Wireless Networks

- Devices like firewalls & unified threat management (UTM) boxes installed in routing devices, like switch, gateways, etc., may be highly effective in blocking any intrusion from outside.
- The peer-to-peer multi-hop used in WAHNs assumes a completely trusted environment for its basic functioning. This assumption is impractical.

* Network Security Requirements

- Authentication
- Confidentiality
- Non-repudiation
- Integrity
- Availability

* Issues & Challenges in Security Provisioning

- Shared broadcast radio channel
- Insecure operational environment
- Lack of central authority
- Lack of Association
- Limited Resource Availability
- Physical Vulnerability

* Network Security Attacks

① Active Attack & Passive Attack

Passive : Eavsdropping, Traffic Analysis, Monitoring
Active : Jamming, Spoofing, Modification, Replaying, DOS

② Internal & External Attack

Internal Attack: Attacker belong to same domain as mobile hosts
External Attack: Attacker doesn't belong to same domain as mobile hosts

Layer	Attacks
Appln	Repudiation, Data corruption
Transport	Session hijacking, SYN flooding
N/w	wormhole, blackhole, byzantine, flooding, resource consumption, location disclosure attacks
Data Link	Traffic Analysis, monitory, disruption MAC (802.11), WEP weakness
Physical	Jamming, Interceptions, Eavsdropping

③ Layer-Specific Attacks : Each layer faces different types of attack

- Stealthy vs non-stealthy attacks
- Cryptography vs non-cryptography related attacks

Cryptographic Primitive Attack	Examples
Pseudorandom number Attack	Nonce, Timestamp, Initialization vector (IV)
Digital Signature Attack	RSA signature, ElGamal signature, digital sign standard (DSS)
Hash collision attack	SHA-0, MD4, MD5, HAVAL-128, RIPEMD

3.1 Network Layer Attack

→ Wormhole Attack: In the attack, an adversary receives data pkt at one end in n/w & tunnel pkts to other end in n/w. Further, the pkt are replayed into n/w & tunnel b/w two adversaries is known as wormhole.

→ Byzantine Attack: A compromized intermediate node or a set of compromised intermediate nodes works in collusion & carries out attacks such as creating routing loops, routing pkts on non-optimal paths & selectively dropping pkts. Byzantine attacks are hard to detect.

→ Information Disclosure: A compromised node may leak confidential or sensitive info to unauthorized nodes in n/w.

→ Resource Consumption Attack: A malicious node tries to consume/away resources of other nodes present in the n/w.

→ Routing Table Overflow Attack: A malicious node advertises route that go to non-existent nodes to the authorized nodes present in the n/w.

→ Routing cache poisoning Attacks: Attackers take advantage of promiscuous node of RT updating, where a node overhearing any pkt may add the routing info contained in that pkt header to its own route cache, even if that node is not on the path.

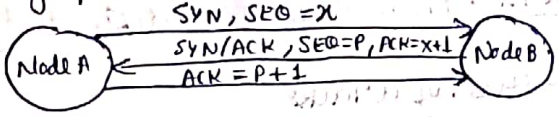
→ Attacks at the Routing Maintenance Phase: Attacks that target the route maintenance phase by broadcasting false ctrl msgs, such as link-broken error msgs, which cause the invocation of the costly route maintenance or repairing problem.

→ Attacks at Data Forwarding Phase: The malicious nodes participate cooperatively in routing discovery & maintenance phase, but in data forwarding phase, they do not forward data pkts consistently acc^n to RT. They simply drop data pkts quitely, modify data content, replay or flood data pkts.

→ Attacks on Particular Routing Protocols: In DSR, the attacker may modify the source route listed in RREQ or RREP pkts. In AODV, attacker may advertise a route with smaller distance metric than actual distance, or advertise a routing update with a large seq. no. & invalidate all routing updates from other nodes.

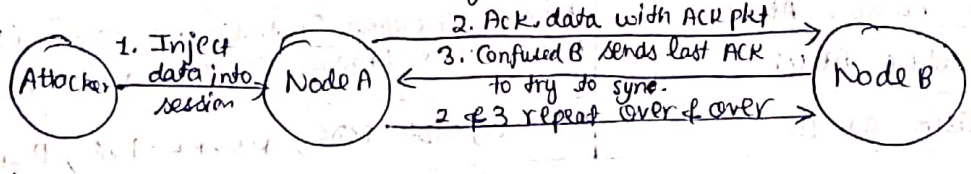
3.2 Transport Layer Attack

→ SYN flooding attack: It is a DOS attack. The attacker creates a large no. of half-opened TCP connections with a victim node but never completes handshake to fully open the connection



TCP-3-way Handshake

→ Session Hijacking: Attacker spoofs victim's IP address, determines correct seq. no. that is expected by target & then performs DOS attack on victim



TCP ACK Storm

3.3 Appl^n Layer Attack

→ Repudiation: Denial or attempted denial by node in communication of having participated in all or part of communication.

→ Malicious Code Attacks: Malicious codes, such as virus, worms, spywares, & Trojan Horses, can attack both operating systems & user appl^ns.

3.4 Multi-Layer Attacks

→ Denial of Service (DOS)

→ Impersonation Attacks

→ Man-in-the-middle attacks

* Key Management

— To make sure secure communication possible, it is necessary to have access to proper keying material. This is objective of key management process.

— Symmetric Key Management

→ Same key to encrypt & decrypt msg

→ Two concerns in a large-scale sensor n/w:

Connectivity # Resilience

– Random Key Distribution

→ Consists 3 phases : ① key pre-distribution, ② shared-key discovery & ③ ③ path-key establishment

→ In pre-distribution phase, a large key-pool of K keys & their corresponding identities are generated. For each sensor within sensor n/w, k keys are randomly drawn from key pool. These k keys form a key ring for a sensor node.

→ During key discovery phase, each sensor node finds out which neighbours share a common key with itself by exchanging discovery msgs. If two neighbour nodes share common key, then secure link blw two nodes.

→ In path-key establishment phase, ~~each~~ a path-key is negotiated for each pair of neighbouring sensor nodes who don't share a common key but can be connected by two or more multi-hop secure links at the end of shared-key discovery phase.

– Combinational Design on Key Distribution

→ The combinatorial design supports q^2+q+1 nodes in the n/w. The size of key pool is q^2+q+1 & each node has $q+1$ keys.

→ Every pair of nodes has exactly one key in common, & every key is owned by exactly $q+1$ nodes. Thus, probability of key sharing among a pair of sensor nodes is 1. When a sensor node is captured by an adversary, the probability that a link is compromized is $1/q$.

→ Disad: parameter q is a prime no. hence not all n/w sizes are supported.

→ Performance issues in Symmetric key algo.:

Speed # Scalability # Management

– Public Key Management

→ Uses pair of keys (private & public keys)

→ Partially Distributed Authority

The objective of threshold cryptography is to protect info by distributing it among a set of n entities. In addition, there is a threshold t associated with the TC schemes. In case of an (n,t) TC scheme (t out of n parties), fewer than t parties will not be able to execute operation cryptographic operation successfully.

→ Fully Distributed Authority

A new node that does not have a certificate will have to contact at least $t+1$ servers which can issue a certificate after establishing identity of node. Any $t+1$ nodes can also renew a certificate

→ Self-Issued Certificates

Each user decides their own public-private key pair. Other users issue a certificate to each other based on other factors such as

personal acquaintances. Each user then maintains in their personal ~~directory~~ repository the list of valid certificates.

* Secure Routing In Adhoc Wireless N/ws

(1) Security-Aware Adhoc Routing Protocol (SAR)

→ Comprehensive framework. For appl^n's that require security, it is preferable to route pkts through trusted nodes rather than route the pkts through shortest ~~first~~ path, that may include untrusted nodes.

→ Additional security properties (comes with a cost) can be incorporated in routing protocols depending on needs of appl^n using n/w:
timeliness # ordering # authentication # authorization
integrity # confidentiality # non repudiation

(2) Secure Efficient Adhoc Distance Vector Routing Protocol (SEAD)

→ Design based on Destination Sequenced Distance Vector (DSDV) routing.

→ It provides authentication on metric's lower bounds & sender's identities by using one-way hash chain.

→ Using a hash value corresponding to the seq. no. & metric in a ~~ret~~ routing update entry allows the authentication of the update & prevents any node from advertising a route to some destination, forging a greater seq. no. or a smaller metric. To authenticate the update, a node can ~~be~~ use any given earlier authentic hash value from same hash chain to authenticate the current update with seq. no. i & metric j.

(3) Authenticated Routing for Adhoc N/ws (ARAN)

→ There is a trusted certificate server, T, which creates & distributes a certificate for each node before the node joins the n/w. All the nodes have access to the true public key of T which they can use to verify the authenticity of the certificate.

→ Node A certificate, $cert_A = [IP_A, Pu\,K_A, t, e]\, Pr\, K_T$
(time of certificate, expire time; IP_A: IP of A; $Pu\,K_A$: Public key of A; $Pr\,K_T$: signed by T's private key)

→ when a node (say A) wishes to find a path to node X, it broadcasts a msg called route discovery pkt (RDP) (contains certificate of node A & current time t).

→ When another node (say B) receives msg it first verifies its authenticity & then verify proper signature. It also check if certificate has not expired. ~~Not~~ Node B then set up a route.

→ If node B is ~~not~~ dest has not seen the msg before & is not dest, it signs its own private key, attaches its own certificate & rebroadcast RDP msg to its neighbours. When next node (say C) receives msg, it follow same process as B's although it remove node B's certificate & sign first & replace this with its own.

→ Eventually node X receives that msg & responds with Reply (REP) msg which contains X certificate.

④ Security-Aware AODV Protocol (SAODV)

↳ Secure extension of AODV protocol

→ main objective to ensure integrity, authentication & non-repudiation of msg. used in AODV

→ ~~Too~~ Uses two mechanisms to secure routing msgs:
  (i) digital signatures to authenticate non-mutable fields of msg
  (ii) hash chains to secure hop count field of msg

→ SAODV uses following additional fields in a routing pkt header:
  (i) hash func^n field (ii) max hop count field (iii) top hash field (iv) hash field

→ Each time a node sends a RREQ or RREP msg, it generates a random no. & sets the value of ~~$ max hop count field same as time to live (TTL) field in IP header. The node then sets hash field with random no. & also sets identifier field of hash func^n. Finally, nodes completes top hash by hashing the random no. max hop count times.

→ The protocol enables receiver node to verify hop count of each msg by applying hash func^n (max hop count − hop count) times to the value in hash field. If the computed value & top hash field value match, hop count is verified.

* Comparison of Secure Routing Protocols for Adhoc NWs

Performance Parameter	ARAN	ARIADNE	SAODV	SAR	SBAD	SLSP	SRP
Type	Reactive	Reactive	Reactive	Reactive	Proactive	Proactive	Reactive
MANET Protocol	AODV/DSR	DSR	AODV	AODV	DSOV	ZHLS	DSR/ZRP
Encryption	Asym	Sym	Asym	Sym/Asym	Sym	Asym	Sym
Synchronization	No	Yes	No	No	Yes	No	No
Trust Authority	CA	KDC	CA	CA/KDL	CA	CA/KDC	CA
Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Confidentiality	Yes	No	No	Yes	No	No	No
Integrity	Yes	Yes	Yes	Yes	No	No	Yes
Non-Repudiation	Yes	No	Yes	Yes	No	Yes	No
Anti-Spoofing	Yes	Yes	Yes	Yes	No	Yes	Yes
DOS Attacks	No	Yes	No	No	Yes	Yes	Yes