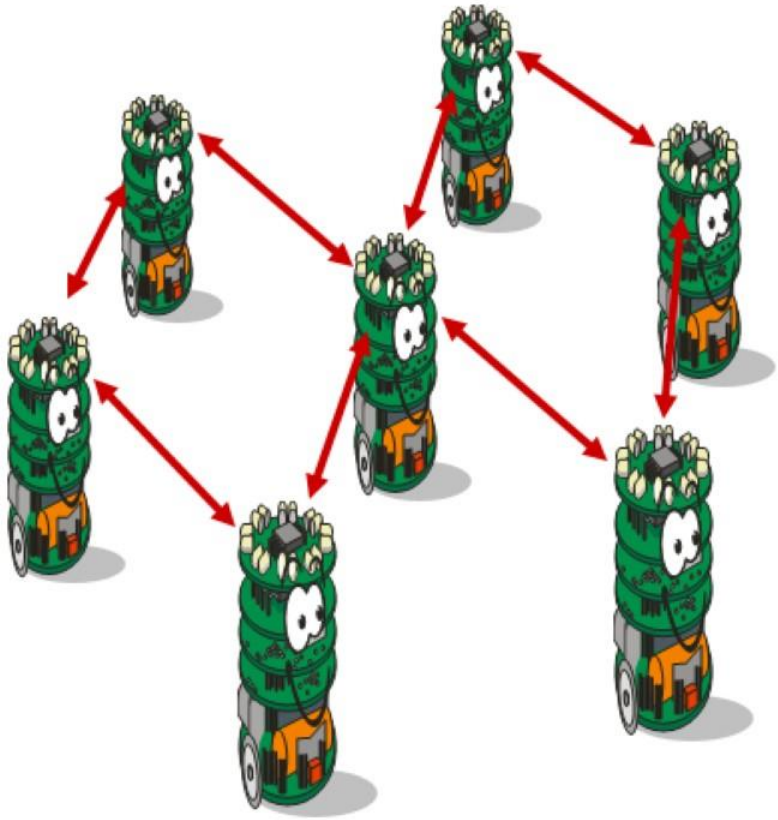
Chapter 5 Ad Hoc Networks

By Abebe Belay (PhD)

1. Introduction: Types of Networks

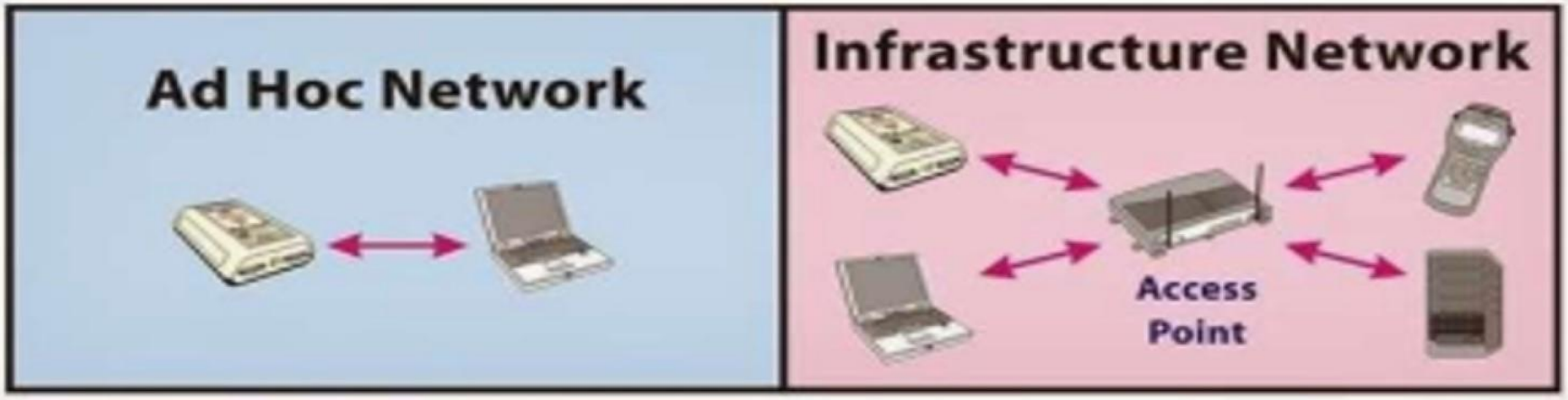
- **Cellular Networks**
  - Base stations distributed over the field
  - each base station covers a cell
  - used for mobile phones
  - WLAN can be seen as a special case
- **Sensor Networks**
  - Network of sensor devices with controller and radio transceivers
  - Base station with more resources
- **Mobile Ad Hoc Networks**
  - Self-configuring network of mobile nodes
  - Node serve as client and router
  - No infrastructure necessary
- Vehicular networks (ad hoc+++)
  - • Example: vehicle-2-vehicle game network
  - • Extra challenge: extreme mobility



Wireless Ad-hoc network

- An ad-hoc wireless network is a collection of wireless mobile nodes that self-configure to form a network without the aid of any established infrastructure.

- Multihop routing, whereby intermediate nodes relay packets towards their final destination, can improve the throughput and power efficiency of the network. Webster's lists two relevant definitions for ad-hoc: "formed or used for specific or immediate problems", and "fashioned from whatever is immediately available."



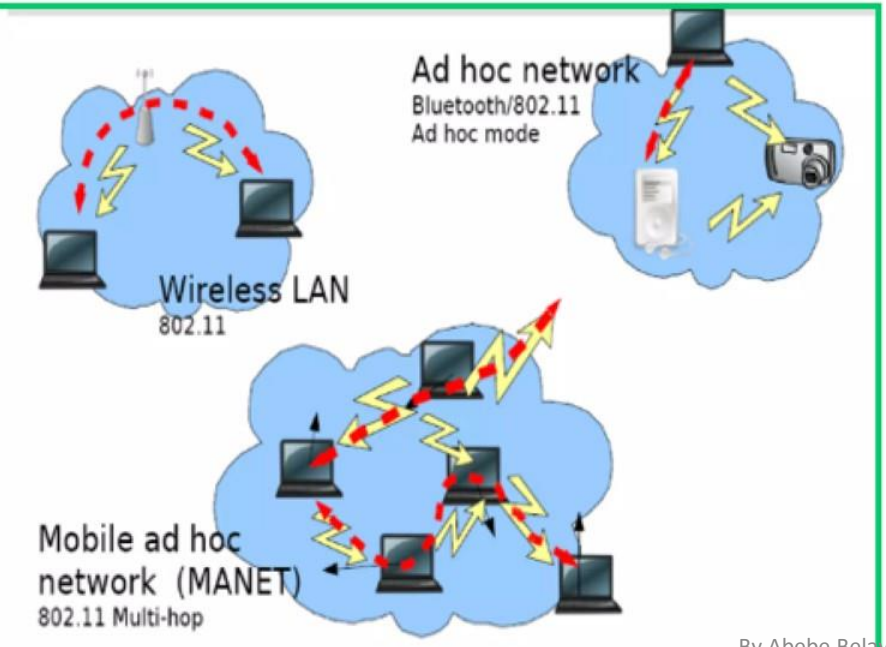
- Wireless sensor networks mainly use **broadcast** communication while ad hoc networks use **point-to-point** communication.
- Unlike ad hoc networks wireless sensor networks are **limited by sensors** limited power, energy and computational capability.
- Sensor nodes may **not have global ID** because of the large amount of overhead and large number of sensors.

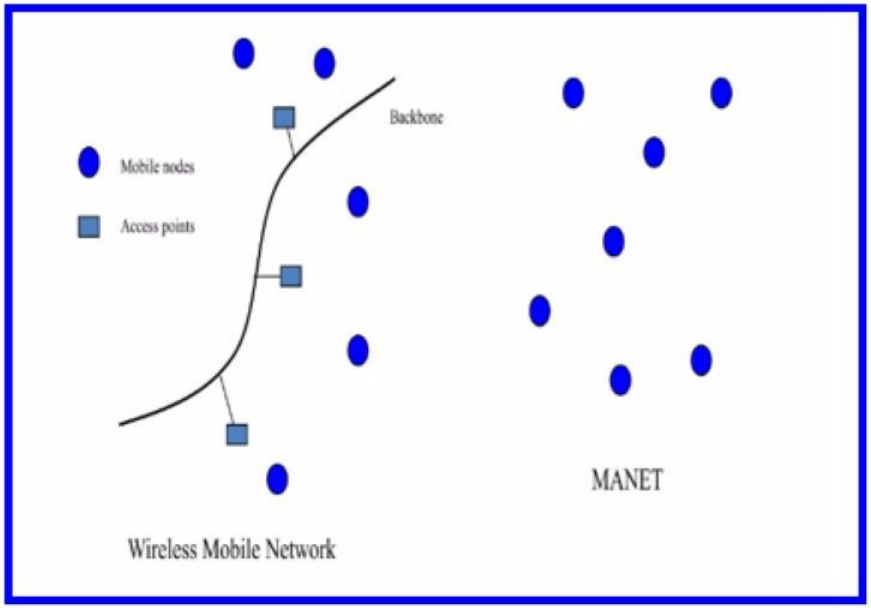
- A Mobile Ad hoc Network (MANET)
  - Formed as needed
  - Does not require support from any existing network infrastructure

- MANET: An autonomous system of mobile nodes or MSs (also serving as routers) connected by wireless links, the union of which forms a communications network modeled in the form of an arbitrary communication graph

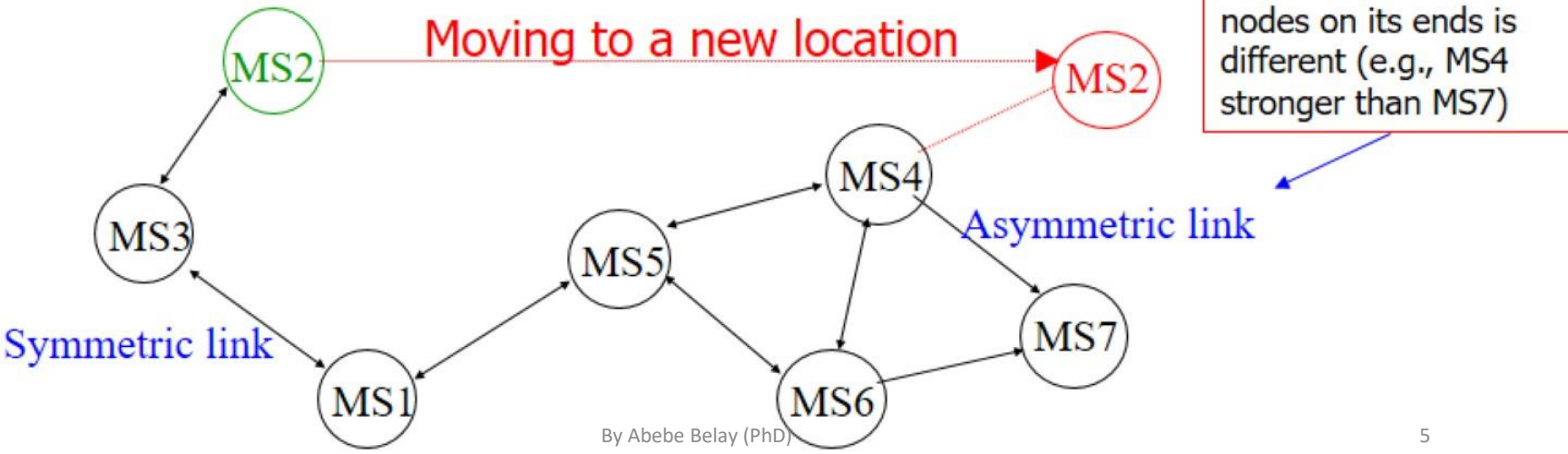
Motivation




Ad hoc network
Bluetooth/802.11
Ad hoc mode
Wireless LAN
802.11
Mobile ad hoc
network (MANET)
802.11 Multi-hop

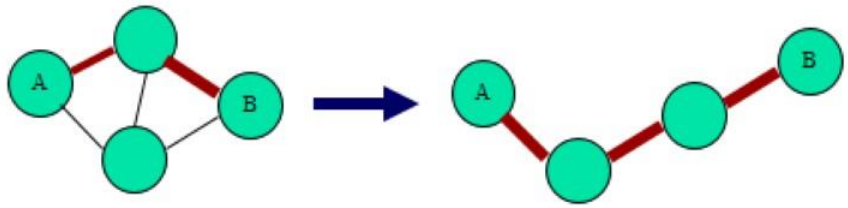

Backbone
Mobile nodes
Access points
MANET
Wireless Mobile Network

- Characteristics of MANETs:
  - Dynamically changing topology
    - Changing in an unpredictable manner
      - Since nodes are free to move
  - Limited power available to nodes (e.g., a battery)
  - Usually communicates only with neighboring nodes
    - Among other reasons, to save power
  - Peer-to-peer
    - No more or less "important" nodes
  - Information transmission via store-and-forward
    - Using multi-hop routing
    - MSs also serve as routers
  - lack of single points-of-failure.



Mobile Ad Hoc Networks (MANET)

- Topology change frequent
- No cellular infrastructure. Multi-hop wireless links.
- Data must be routed via intermediate nodes.

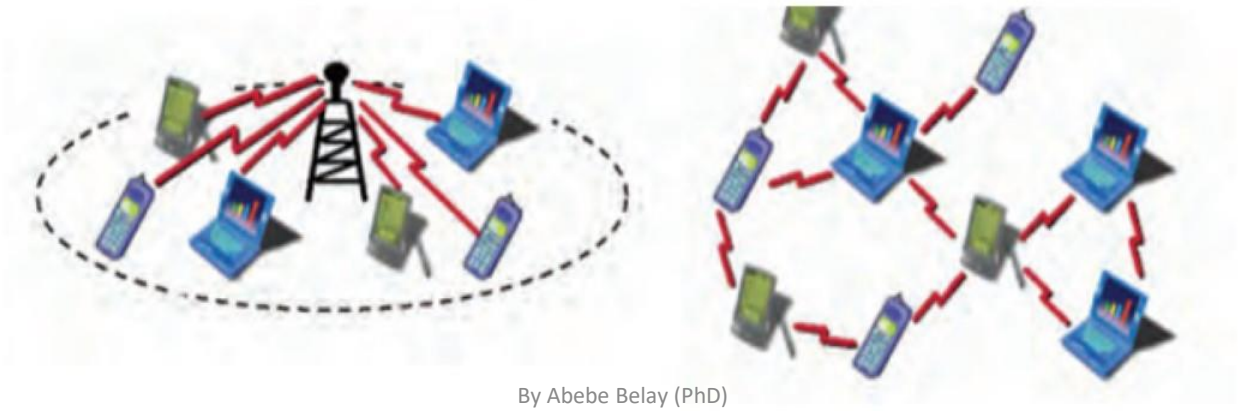


Vehicular Networks – Challenges?

- Extreme mobility
  - DSR won't work if the routes keep changing
- Scale
  - Possibly the largest ever ad-hoc networks
- Topology
  - Deployment/density not controlled by designer (e.g., highway vs city)
  - Gradual deployment (new cars equipped from the factory in the near future)

Infrastructure VsAd HocNetwork

Infrastructure networks	Ad-hoc wireless networks
Fixed infrastructure	No infrastructure
Single-hop wireless links	Multi-hop wireless links
High cost and time of deployment	Very quick and cost-effective
Reuse of frequency via channel reuse	Dynamic frequency sharing
Nowadays applications: civilian, commercial	Nowadays applications: military, rescue
High cost of network maintenance	Maintenance operations are built-in
Low complexity of mobile devices	Intelligent mobile devices are required
Widely deployed, evolves	Still under development in commercial sector



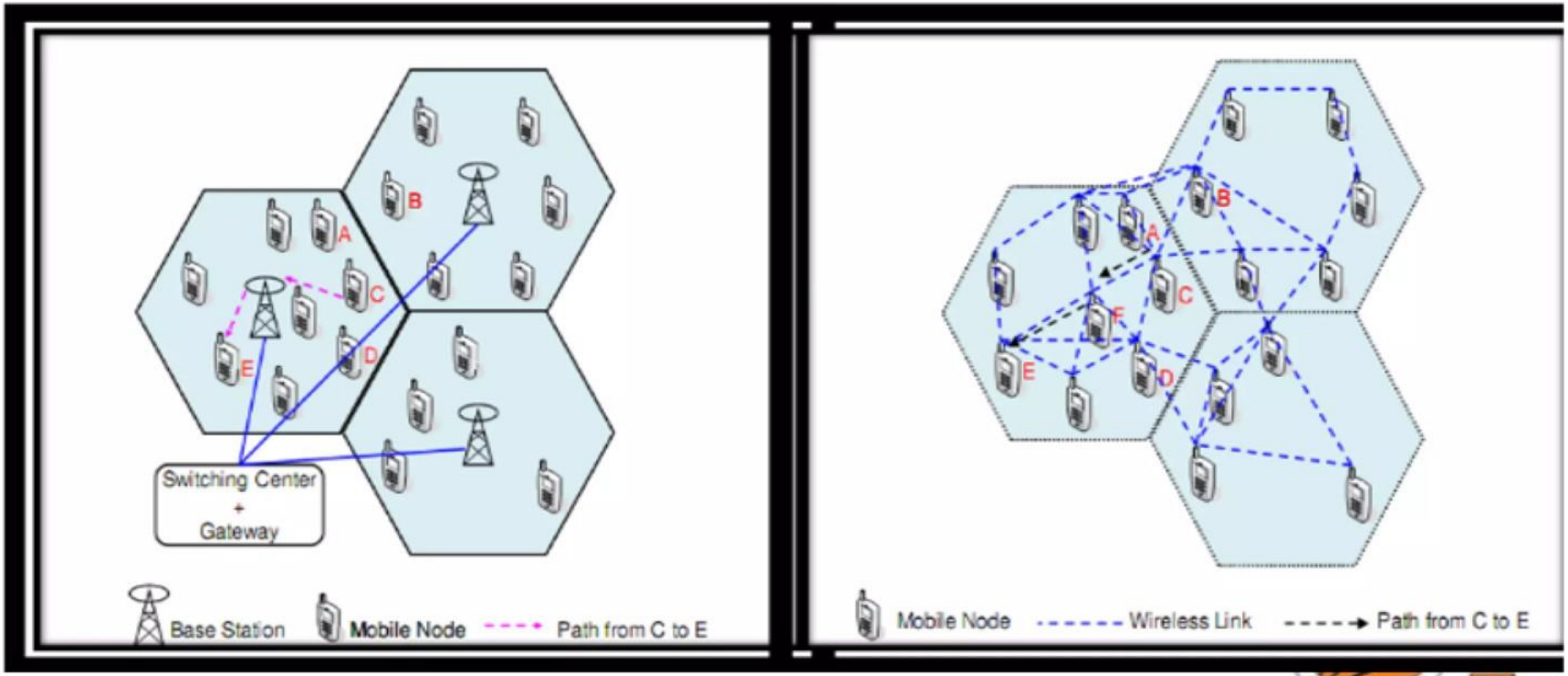
(a) Infrastructure-based wireless network (b) Ad hoc wireless network

Cellular Net vs. Ad Hoc Net

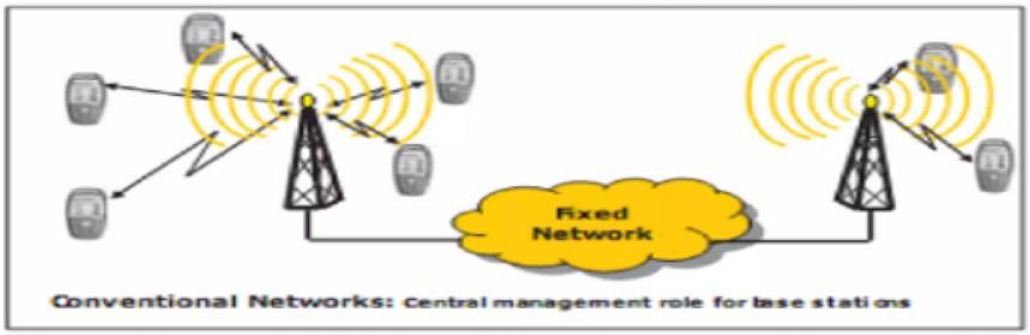
Easier to achieve time synchronization	Time synchronization is difficult and consumes bandwidth
Easier to employ bandwidth reservation	Bandwidth reservation requires complex medium access control protocols
Application domains include mainly civilian and commercial sector	Application domains include battlefields, emergency search and rescue operation, and collaborative computing
High cost of network maintenance (backup power source, staffing, etc.)	Self-organization and maintenance properties are built into the network
Mobile hosts are of relatively low complexity	Mobile hosts require more intelligence (should have a transceiver as well as routing/switching capacity)
Major goals of routing and call admission are to maximize the call acceptance ratio and minimize the call drop ratio	Man aim of routing is to find paths with minimum overhead and also quick reconfiguration of broken paths
Widely deployed and currently in the third generation	Several issues are to be addressed for successful commercial deployment even though widespread use exists in defense

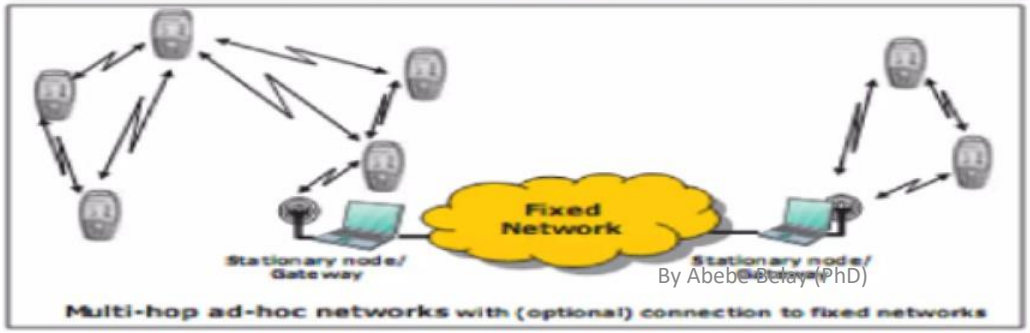
Chandra Prakash, CSE

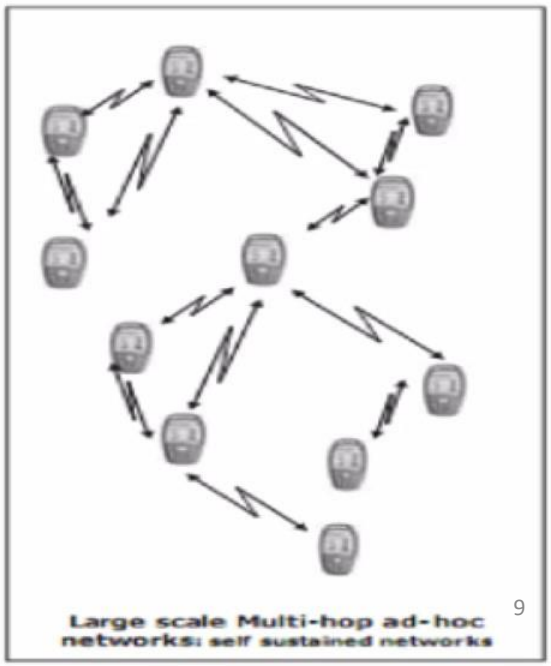
Cellular and ad hoc networks.



Comparison of wireless cellular and wireless ad-hoc network concepts







- Communication characteristics for MANETs:
  - Each node equipped with a wireless transmitter and a receiver with an appropriate antenna
  - Impossible to have all nodes within each other's radio range
  - When the nodes are close by (within each others radio range), they can communicate directly
    - If direct comm. => no routing needed (one hop)
  - Wireless connectivity modeled by a random multi-hop graph exists between the nodes.
  - As nodes move:
    - Connectivity changes
    - Topology information must be updated
      - E.g., MS2 changes attachment: from MS3 to MS4

Why Ad Hoc Networks ?

- Setting up of fixed access points and backbone infrastructure is not always viable
  - Infrastructure may not be present in a disaster area or war zone
  - Infrastructure may not be practical for short-range radios; Bluetooth (range ~ 10m)

- Ad hoc networks
  - Do not need backbone infrastructure support
  - Are easy to deploy
  - Useful when infrastructure is absent, destroyed or impractical

Characteristics of Ad Hoc Networks

- Dynamic topologies
  - Network topology may change dynamically as the nodes are free to move
- Bandwidth-constrained, variable capacity links
  - Wireless links have typically lower capacity than wired
  - Realized throughput of wireless communication is lower than the radio's maximum transmission rate
  - Link capacity is relatively low => congestion is common (collisions occurs frequently as application demand approaches link capacity)
- Energy-constrained operation
  - Nodes in ad hoc network may rely on batteries or other limited energy sources
    - Energy conservation may be a dominant design factor

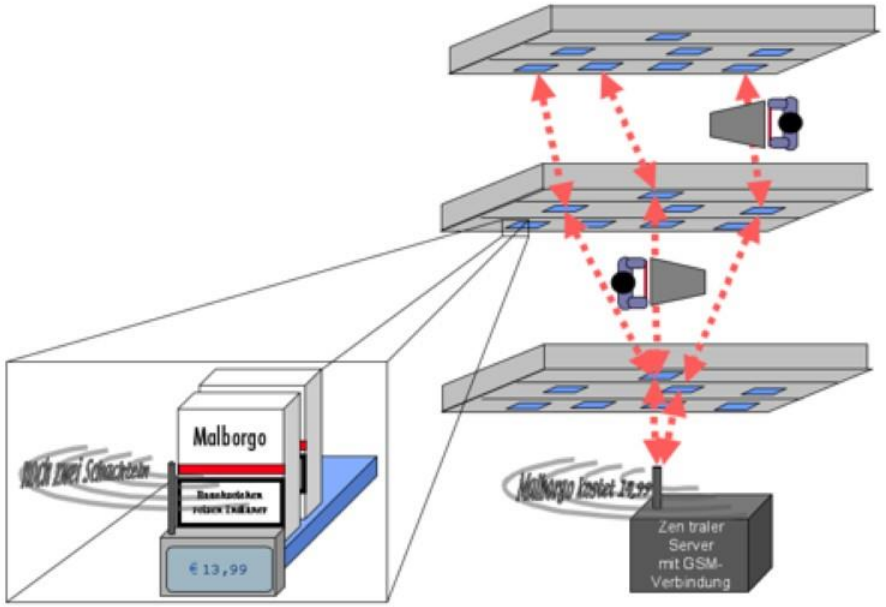
- Limited physical security
  - More prone to physical security threats than wired networks
    - Incl. stealing mobile ad hoc devices
  - Many attacks, incl. Eavesdropping, spoofing, and DoS attacks are easier
- Decentralized network control
  - Eliminates single points of failure (=> better reliability)
- Scalability problems
  - As networks get large

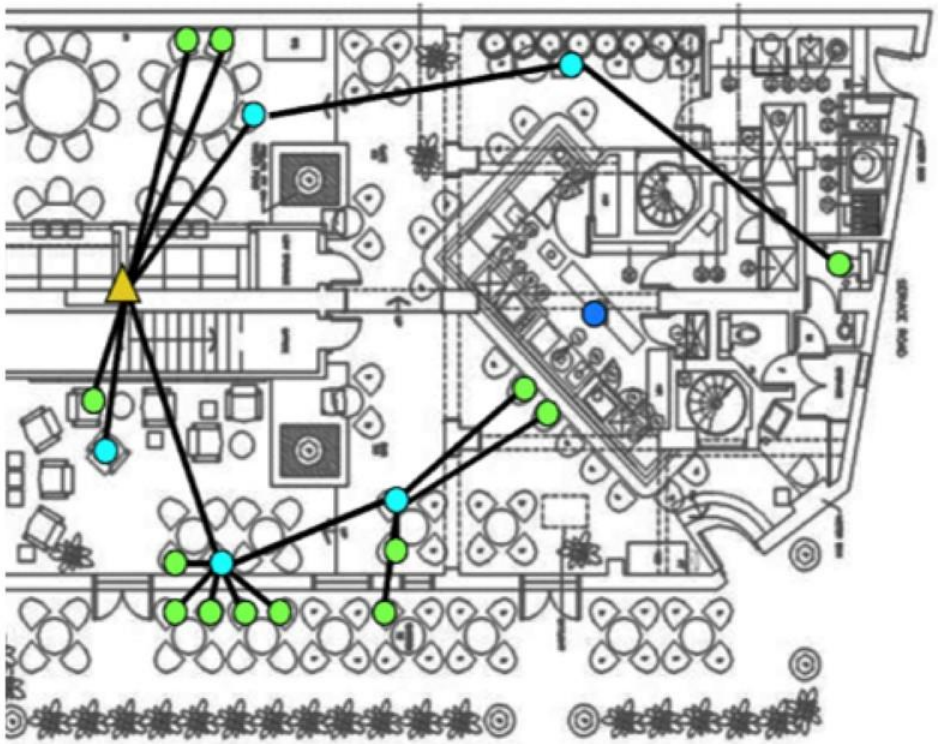
Some Applications

- "Wearable" computing
- Defense applications
- Crisis-management applications
  - Natural disasters, where the entire communication infrastructure is in disarray
- Telemedicine
  - E.g., assistance by a surgeon for an emergency
- Tele-geoprocessing applications
  - Queries dependent on location of the users
  - Integrating geographical info systems (GIS) & GPS
- Virtual navigation
  - Data from a remote database transmitted to navigation device in car or in hand
  - May contain graphical representation of streets, buildings, and the latest traffic information
    - May assist driver in selecting a route
- Education and Internet access
  - K-12, continued education, etc., for people in remote areas
  - E.g., email-by-bus in remote villages

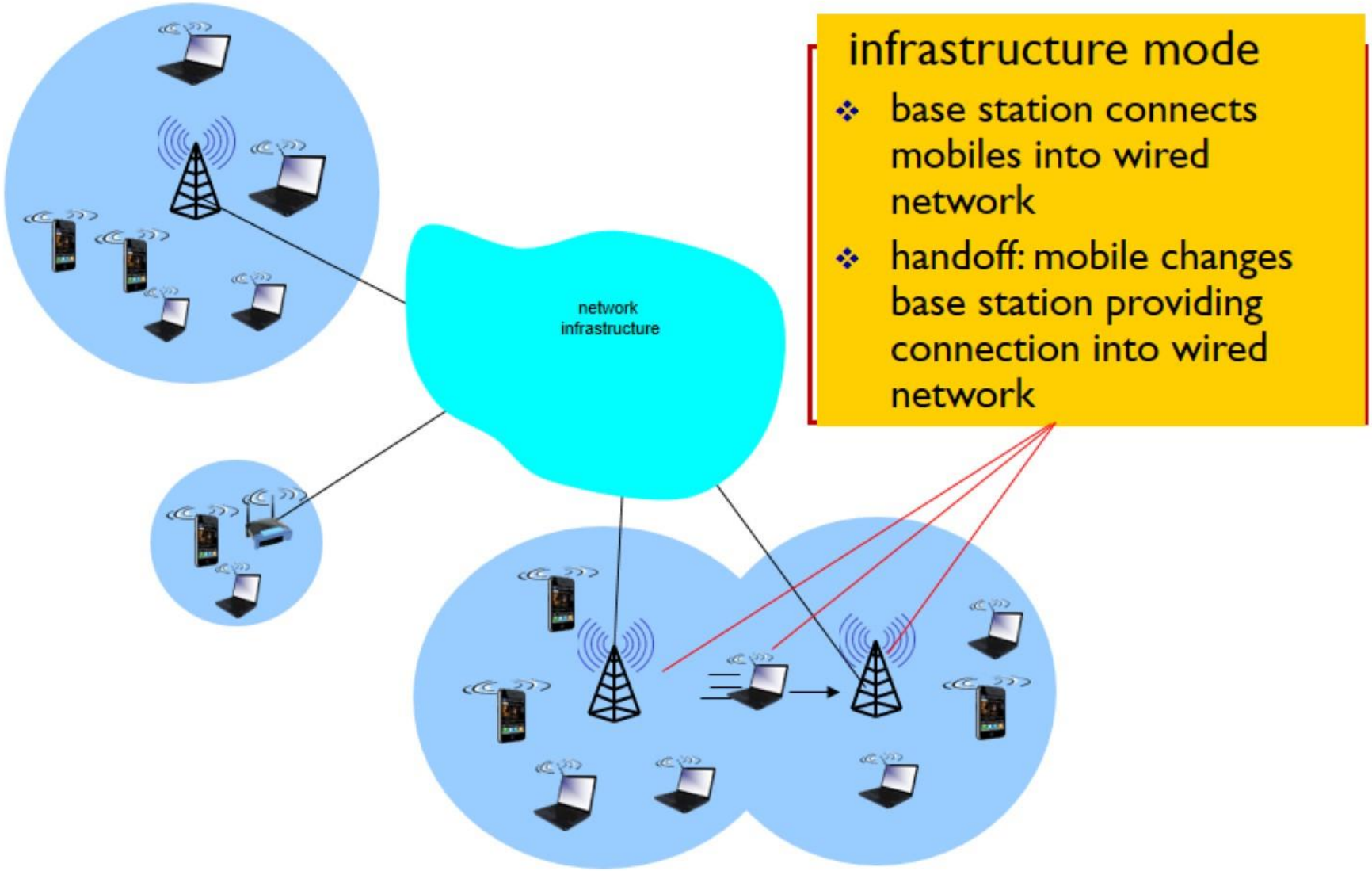
Applications .....

- Network Failure
- Military
- Deserted Areas
- Entertainment
  - Spontanous games
  - Dating-Tool
- Sensor networks
  - Environmental control
  - Intelligent Home
  - Supermarket
- Car technology
  - Inter-car communication
  - Car coordination
- WLAN hotspot extension





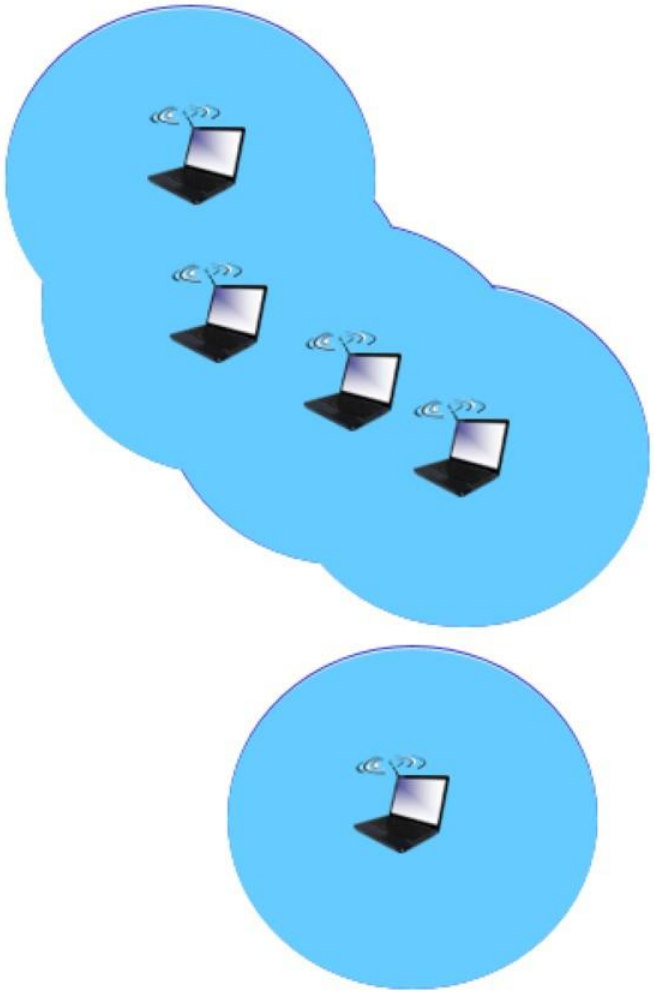
Elements of a wireless network



infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

Elements of a wireless network



ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Wireless network taxonomy

	single hop	multiple hops
Infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	■ host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
No infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	■ no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Routing in MANETS

- Many factors affecting routing in MANETs:
  - Models of topology
  - Selection of routers
  - Initiation of route requests
  - Specific underlying characteristics
    - E.g. application-based characteristics
- Major goals in selecting routing protocols:
  - Provide the maximum possible reliability - use alternative routes if an intermediate node fails
  - Choose a route with the least cost
    - E.g., minimal # of hops from source to destination
  - Give the nodes the best possible response time and throughput
  - Each node in MANETs expected to serve as a router
    - All execute the same routing protocol
      - Protocol calculates a route

Need for Routing in MANETS

1) Route computation must be distributed
   - Centralized routing in a dynamic network is usually too expensive
2) Routing computation should not involve the maintenance of global state
   - Would require mitting a lot of information in dynamic topology
3) As few nodes as possible involved in route computation and state propagation
   - But every node must have quick access to routes on demand
   - Ensure infrequent topology updates for MANET portions that have no traffic
4) Each node must be only concerned about the routes to its destinations
5) Stale routes must be avoided or detected & eliminated
6) Broadcasts should be avoided
   - Broadcasts can be highly unreliable in MANETs
7) If topology stabilizes, the routes must converge to the optimal routes
8) It is desirable to have a backup route
   - Used when the primary route becomes stale

Limitation of Ad-hoc network

- **Throughput Drops** with More Hops Nodes that are in the transmission range of each other are able to send the data packets directly. However, when the node needs to send data to a non-neighbouring node, the data packets will have to be sent through a sequence of multiple hops, with the intermediate nodes acting as routers. This indicates an increase in the number of hops taken. Throughput will decrease rapidly when the number of hops is increased. This can be explained using the four-hop network illustrated in Figure .



When link 1-2 is active, link 2-3 cannot be active because a node cannot be transmitting and receiving at the same time. Link 3-4 is also inactive because communication by node 3 may interfere with node 2 (Holland and Vaidya, 2002). Thus, with more hops, there are in turn more idle nodes, which reduces the throughput

- **Throughput Drops with Increasing Mobility** Highly mobile nodes will result in more overheads due to frequent topology changes. This is because of the increase in the number of routing packet transmissions due to the need to determine new routes after route failures. When the routing table is used, each node keeps a list of all available destinations as well as the number of hops required to reach each destination. Changes in the topology will be reflected in the routing table. Any routing table changes are relayed to all the other nodes. This imposes a larger overhead on the overall network. When the overhead is large, a lower percentage of the packet goes towards the transmission of data, resulting in a lower throughput.

- **Delay** Delay represents the average time duration which a packet takes from the time it leaves a source to the time it arrives at its destination. As seen above, there is a need to keep the nodes busy with the transmission and receiving of packets in order to increase the throughput of the network. This, in turn will mean that the queue of each node is always not empty, leading to a longer delay

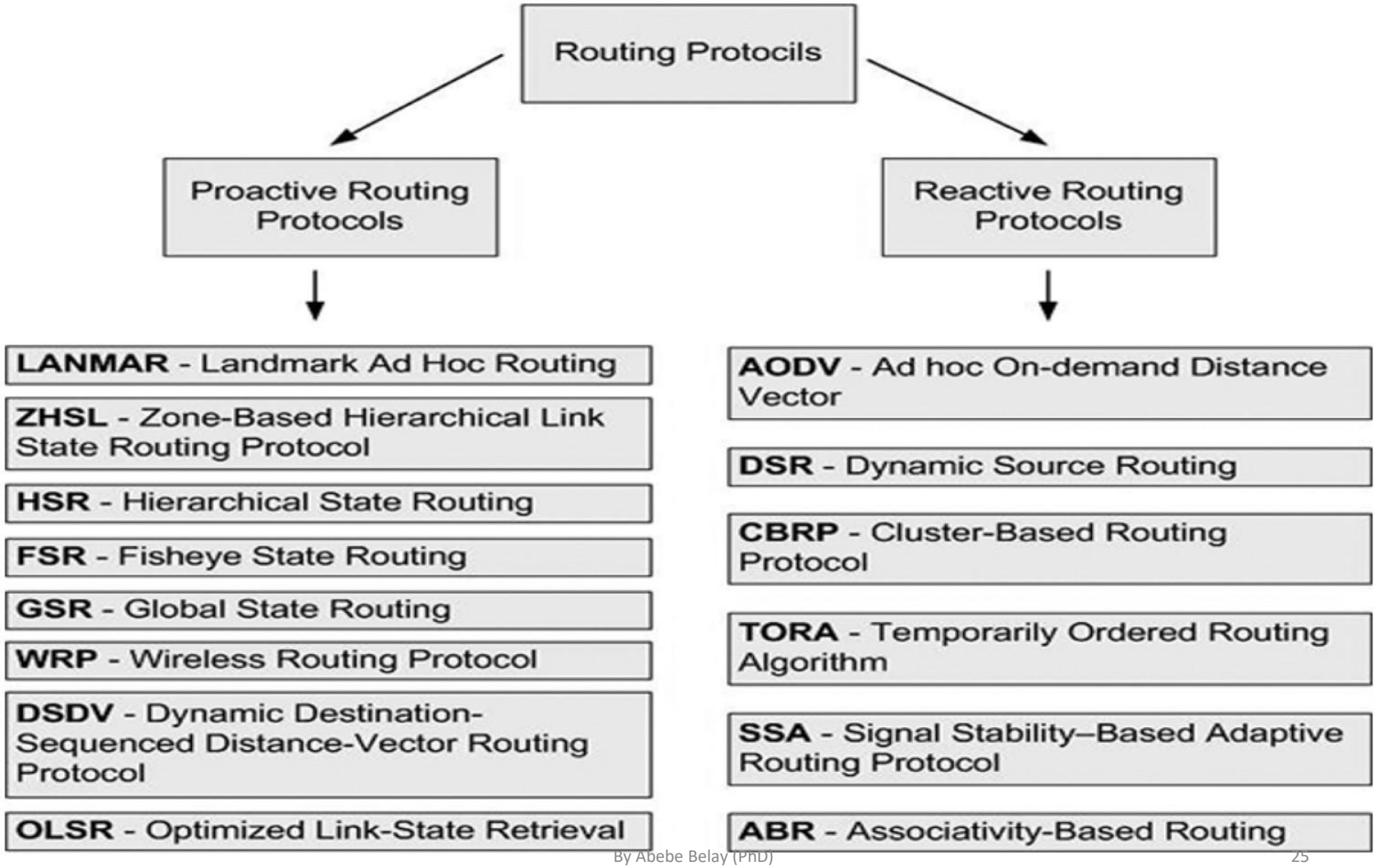
Pros and Cons of MANET

- **Pros:**
  - Separation from central network administration.
  - Each node can play both the roles ie. of router and host showing autonomous nature.
  - Self-configuring and self-healing nodes do not require human intervention.
  - Highly scalable and suits the expansion of more network hub.
- **Cons:**
  - Resources are limited due to various constraints like noise, interference conditions, etc.
  - Lack of authorization facilities.
  - More prone to attacks due to limited physical security.
  - High latency i.e. There is a huge delay in the transfer of data between two sleeping nodes.

2. Routing-based MANET Classification

- Types of routing protocols:
  1) Proactive protocols
     - Keep routes ready at all times
     - have lower latency due to maintenance of routes at all times
     - can result in much higher overhead due to frequent route updates
     - Example: distance vector routing protocols .
  2) Reactive (= on-demand) protocols
     - Determine a route only when there is a packet to send.
     - Examples: flooding routing algorithms, ad hoc on-demand distance vector (AODV), temporarily ordered routing algorithm (TORA).
     - higher latency since the routes have to be discovered when the source node initiates a route request
     - lower overhead since routes are maintained only on-demand basis
  3) Hybrid protocols

- Pure proactive use too much bandwidth for control - updating routing information
  - Too keep it current all the time
  - But topology changes are so quick that most routes never used – a waste!
- Pure reactive too slow for real-time applications



2.1. Table-driven Routing Protocols

- "Table-driven" : Each node maintains table(s) with routing information for every other nodes in the network
- Table-driven: When the topology changes, updates are propagated throughout the network.
- Examples of table-driven routing protocols are:
  - Destination Sequenced Distance Vector routing (DSDV)
  - Wireless Routing Protocol (WRP)
- Destination-Sequenced Distance-Vector Routing (DSDV)
  - Each mobile node maintains a routing table
    - In terms of number of hops to each destination
  - Routing table updates are periodically transmitted
  - Each entry in the table is marked by a sequence number
    - Helps to distinguish stale routes from new ones, and thereby avoiding loops
  - To minimize the routing updates, variable sized update packets are used
    - Depending on the number of topological changes

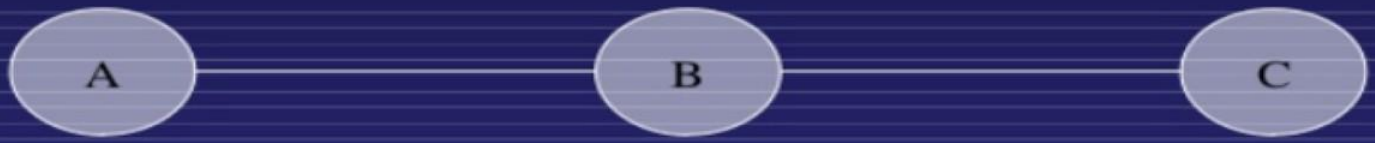
Advantages of DSDV

- It is quite suitable for creating ad-hoc networks with small number of nodes
- Solve the Routing Loop problem
- Count to infinity problem is reduced
- DSDV maintains only the best path instead of maintaining multiple paths to every destination

Disadvantages of DSDV

- DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle
- Whenever the topology of the network changes, a new sequence number is necessary
- DSDV is not suitable for highly dynamic networks

- Each Node Maintains Tables for:
  - Next Hop on Path
  - Distance (in hops) to destination
  - Sequence Number (keep current route)
- Nodes Exchange Updates With Neighbors
- If the two nodes have the same sequence number then route with the best metric is used

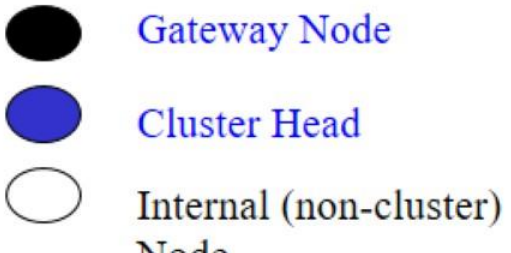


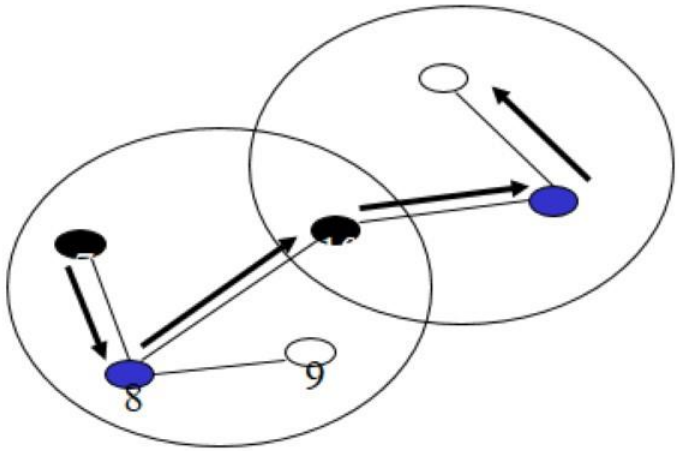
Routing table of Node A in this network is

Destination	Next Hop	Number of Hops	Sequence Number	Install Time
A	A	0	A 46	001000
B	B	1	B 36	001200
C	B	2	C 28	001500

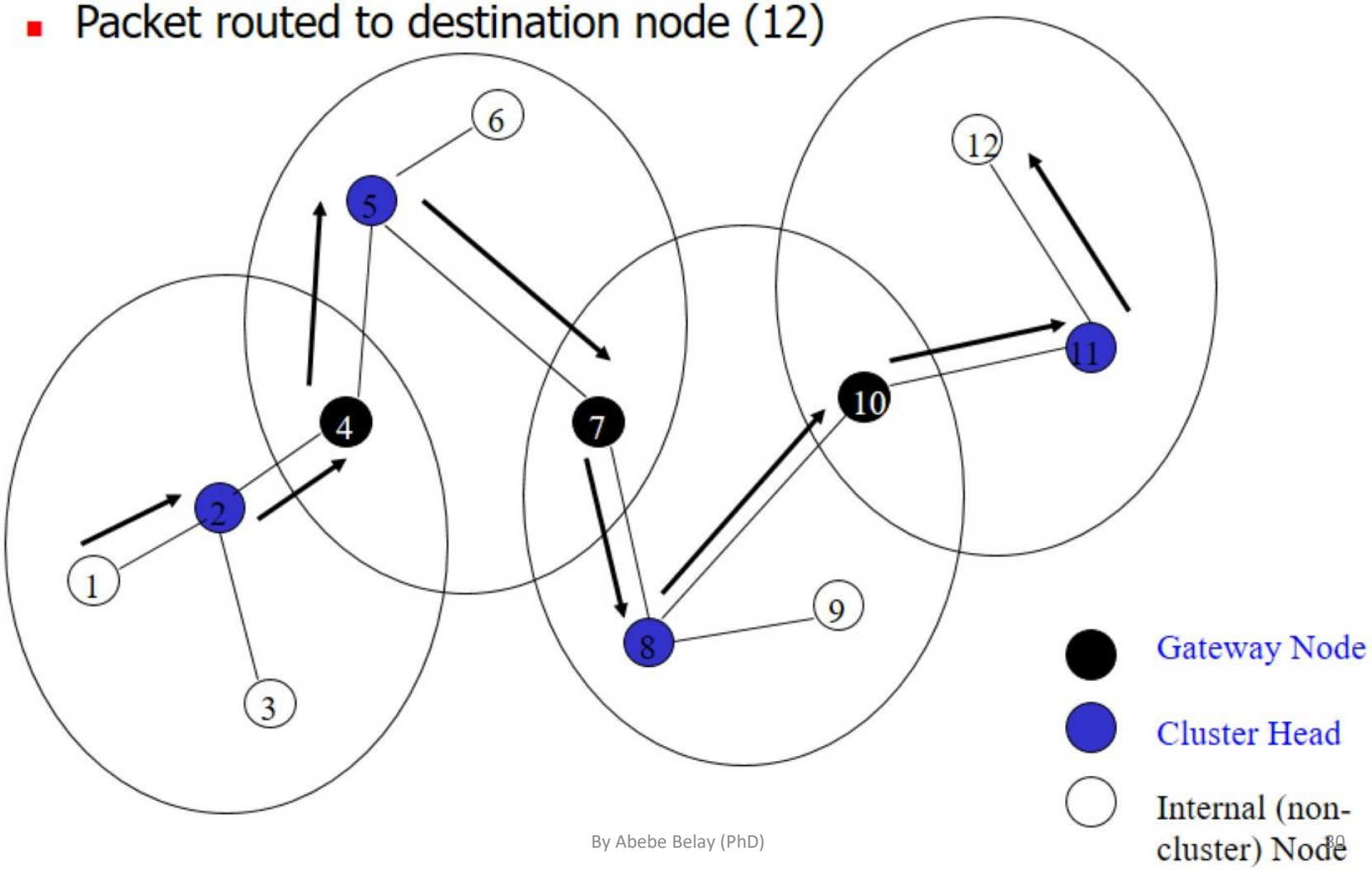
Cluster-head Gateway Switch Routing (CGSR)

- Cluster-head gateway switch routing (CGSR) –
  a clustered multi-hop routing, heuristic
- MANET divided into clusters
  - For each cluster, a cluster-head (CH) elected
    - By a distributed CH selection algorithm
      - It modifies DSDV by using a hierarchical CH to route traffic
  - Gateway nodes are bridges connecting cluster heads
- Frequent changes of CHs affect the performance

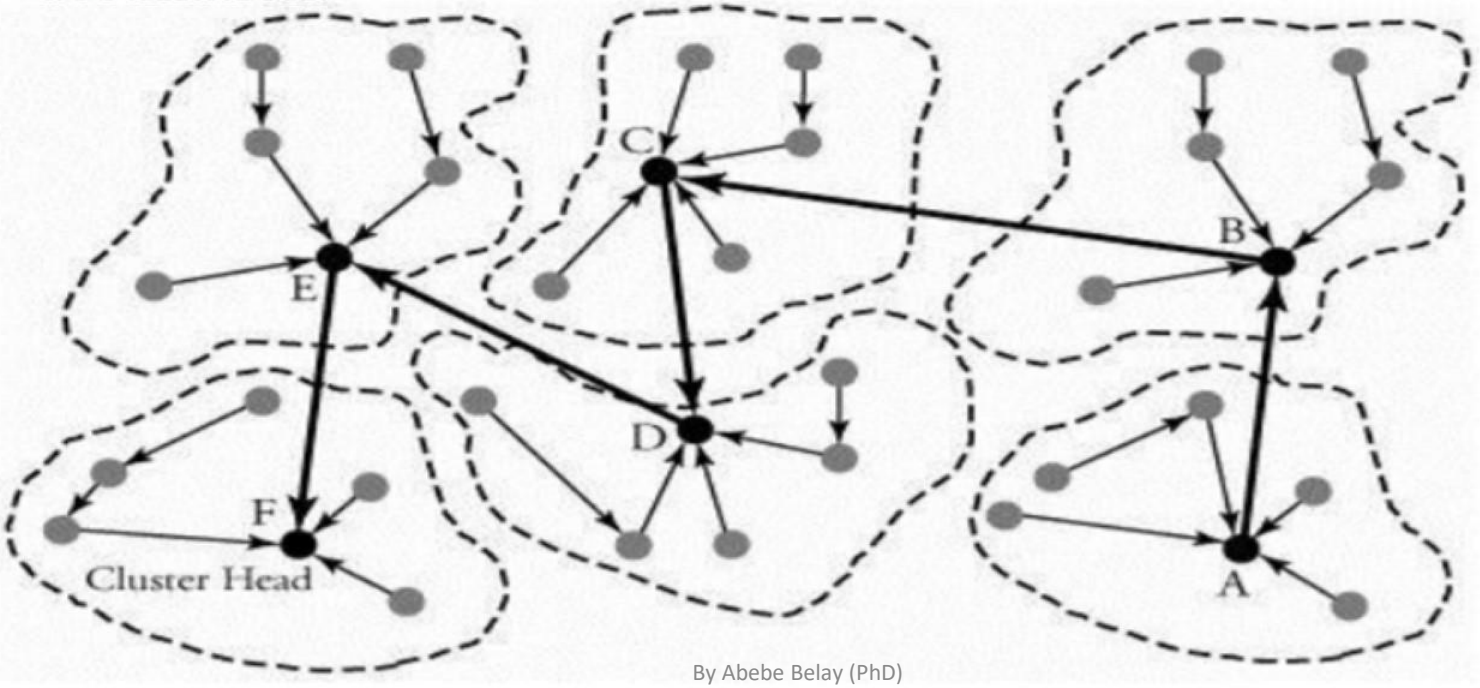




- CGSR scenario - routing from ***Node 1 to Node 12***:
  - Packet sent by Node 1 is first routed to its CH (2)
  - The packet is routed from CH (2) to gateway (4) connecting to CH of another cluster (5)
  - Packet routed from gateway (4) to the next CH (5)
  - …
  - Packet routed from gateway (10) to CH of destination cluster (11)
  - Packet routed to destination node (12)



- A node in cluster A is transmitting a packet to a node in cluster F. Nodes within each cluster route their packets to their own associated clusters.
- The transmitting node then sends its packet to the next hop, according to the routing table entry associated with that cluster head. The cluster head transmits the packet to another cluster head until the cluster head of the destination node is reached.
- The routing is made through a series of available cluster heads from A to F. Packets are then transmitted to the destination.



Advantages & Disadvantages of (CGSR)

Advantages:

- Hierarchical scheme enables partial coordination
- Better bandwidth utilization

Disadvantages:

- Too frequent cluster head selection can be an overhead and cluster nodes and Gateway can be a bottleneck
- Increase the path length
- Gateway conflicts

The Wireless Routing Protocol (WRP)

- Each node maintains 4 tables:
  - Distance table
  - Routing table
  - Link cost table
  - Message Retransmission List table (MRL)

    MRL contains the sequence number of the update message, a retransmission counter and a list of updates sent in the update message

Advantages of WRP

- A problem of the Bellman-Ford protocol is the count-to-infinity problem. This is a problem that is solved by WRP

Disadvantages of WRP

- Four tables requires a large amount of memory
- Periodic hello message consumes power and bandwidth

- Nodes inform each other of link changes using update messages
- Nodes send update messages after processing updates from their neighbors or after detecting a change in the link
  - If a node is not sending messages, it must send a HELLO message within a specified time to ensure connectivity
  - If the node receives a HELLO message from a new node, that node is added to the table
- It avoids the "count to infinity" problem

Summary of Table Driven Routing

Table Driven Routing Protocols

- Destination Sequenced Distance – Vector Routing Protocol (DSDV)
- The Wireless Routing Protocol (WRP)
- Global State Routing (GSR)
- Fisheye State Routing (FSR)
- Hierarchical State Routing (HSR)
- Zone-based Hierarchical Link State Routing Protocol (ZHLS)
- Clusterhead Gateway Switch Routing Protocol (CGSR)

2.2. Source-Initiated On-Demand Routing

- This family of protocols includes:

1) Ad hoc On-Demand Distance Vector (AODV)
2) Dynamic Source Routing (DSR)
3) Temporary Ordered Routing Algorithm (TORA)
4) Associativity Based Routing (ABR)
5) Signal Stability Routing (SSR)

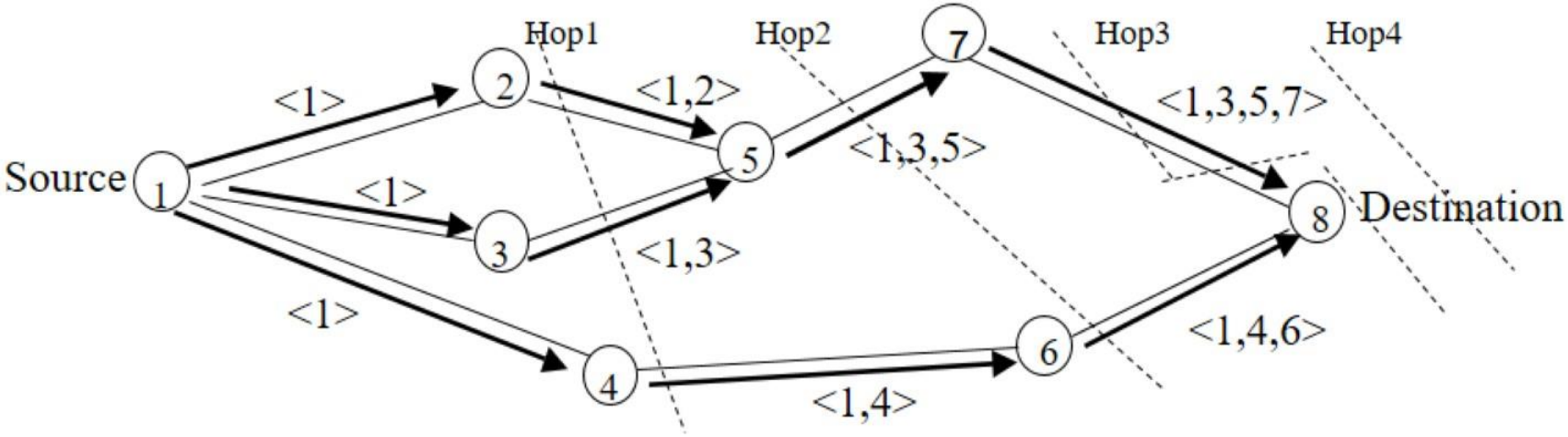
Dynamic Source Routing (DSR)

- The protocol consists of two major phases: Route Discovery, Route Maintenance

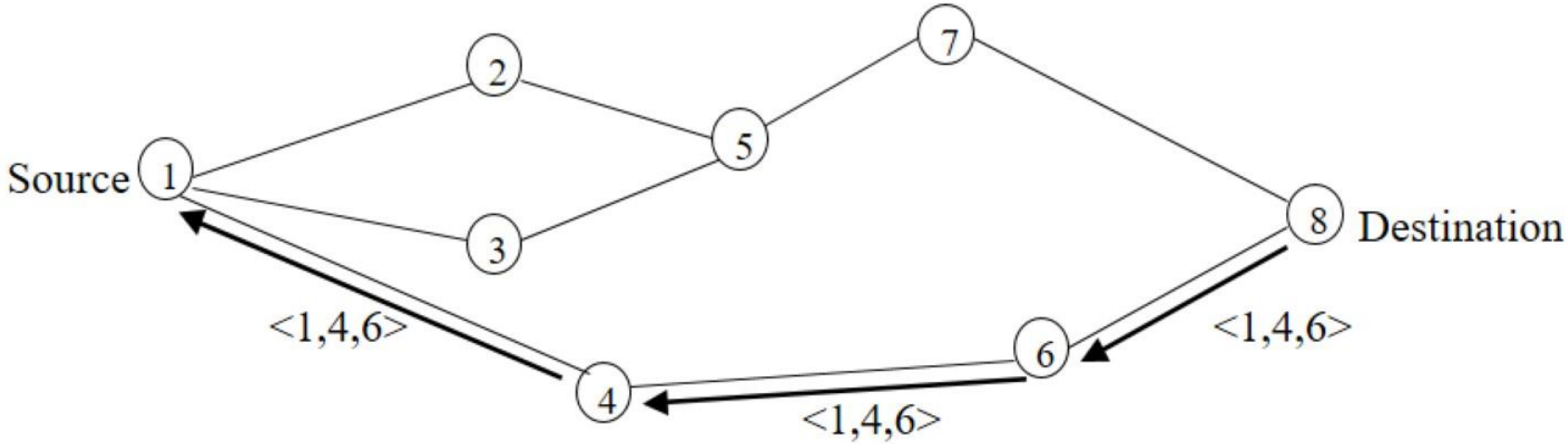
- When a mobile node has a packet to send to some destination, it first consults its route cache to check whether it has a route to that destination
  - If it is an un-expired route, it will use this route
  - If the node does not have a route, it initiates route discovery by broadcasting a Route Request packet
- This Route Request contains the address of the destination, along with the source address

- Each node receiving the packet checks to see whether it has a route to the destination.
  - If it does not, it adds its own address to the route record of the packet and forwards it.
- A route reply is generated when the request reaches either the destination itself or an intermediate node that contains in its route cache an un-expired route to that destination.
  - If the node generating the route reply is the destination, it places the route record contained in the route request into the route reply.

Creation of Route Record in DSR

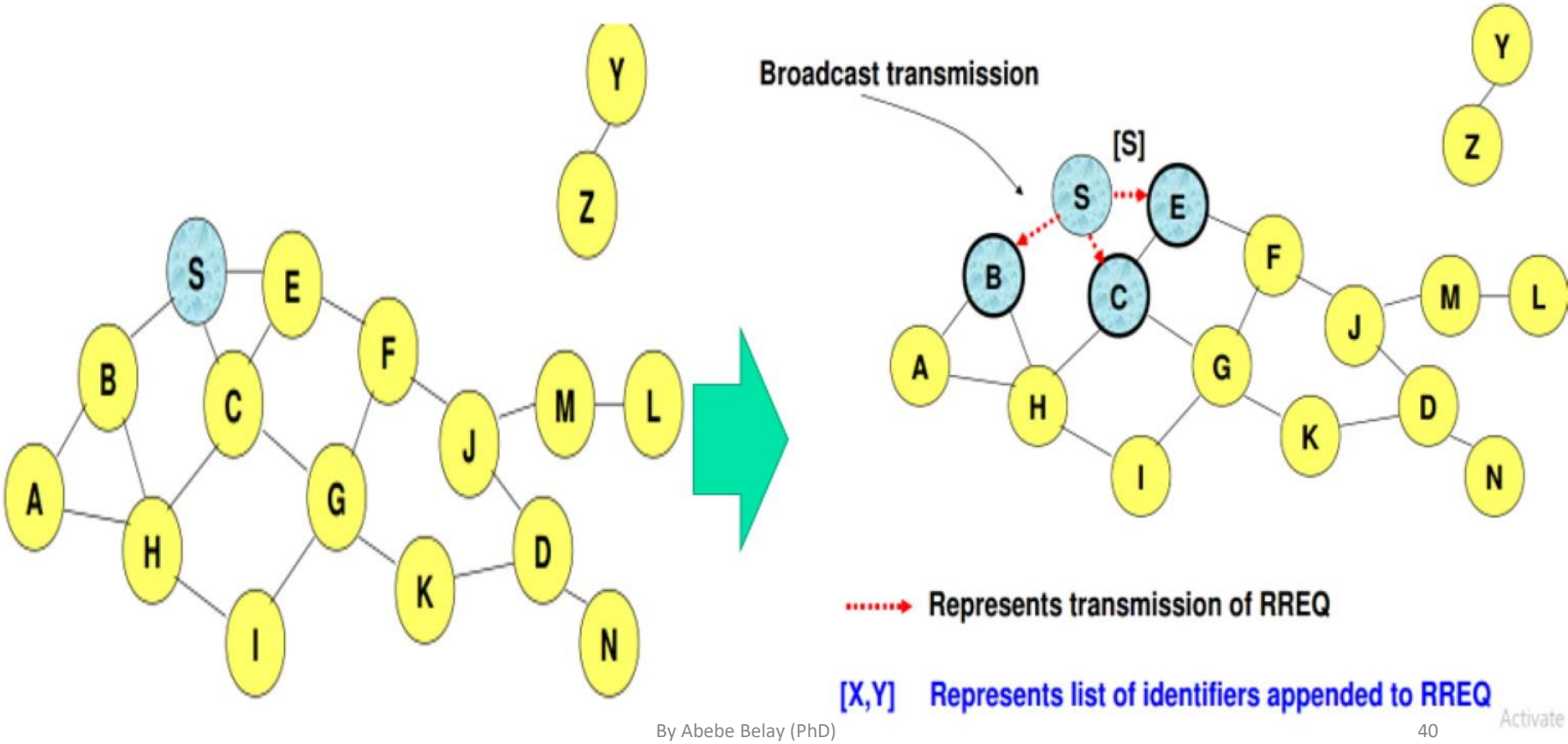


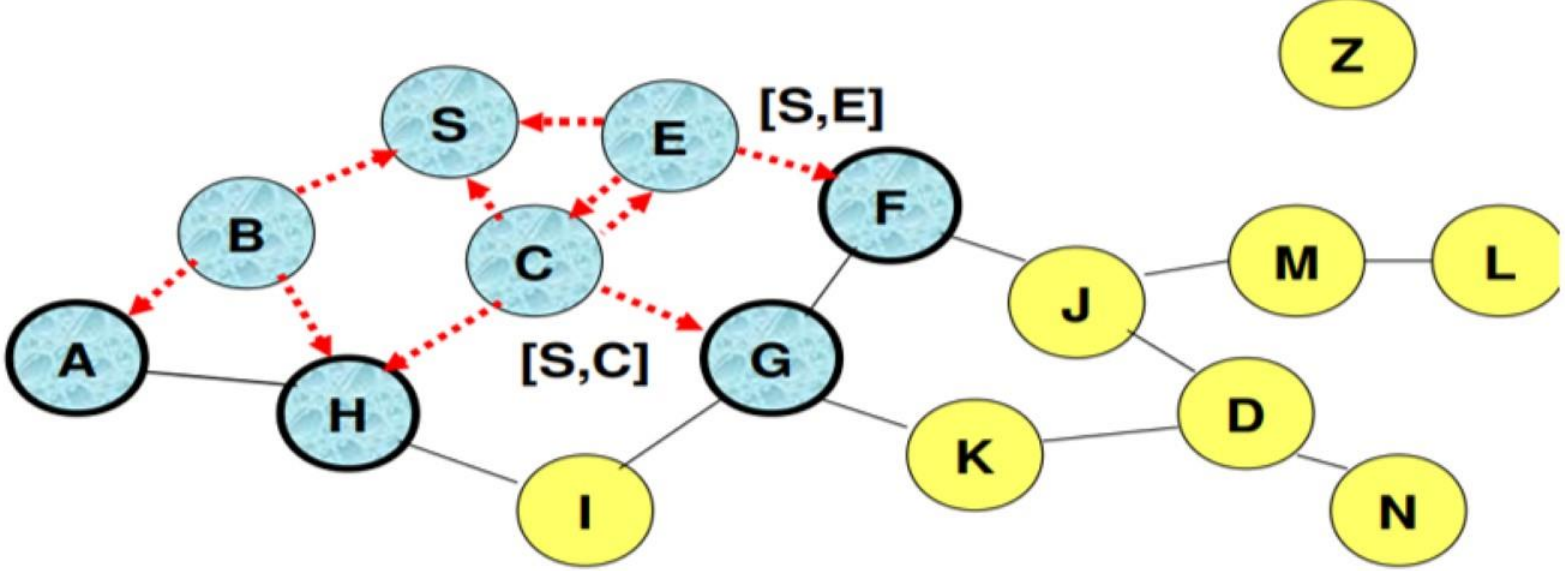
(a) Building Record Route During Route Discovery



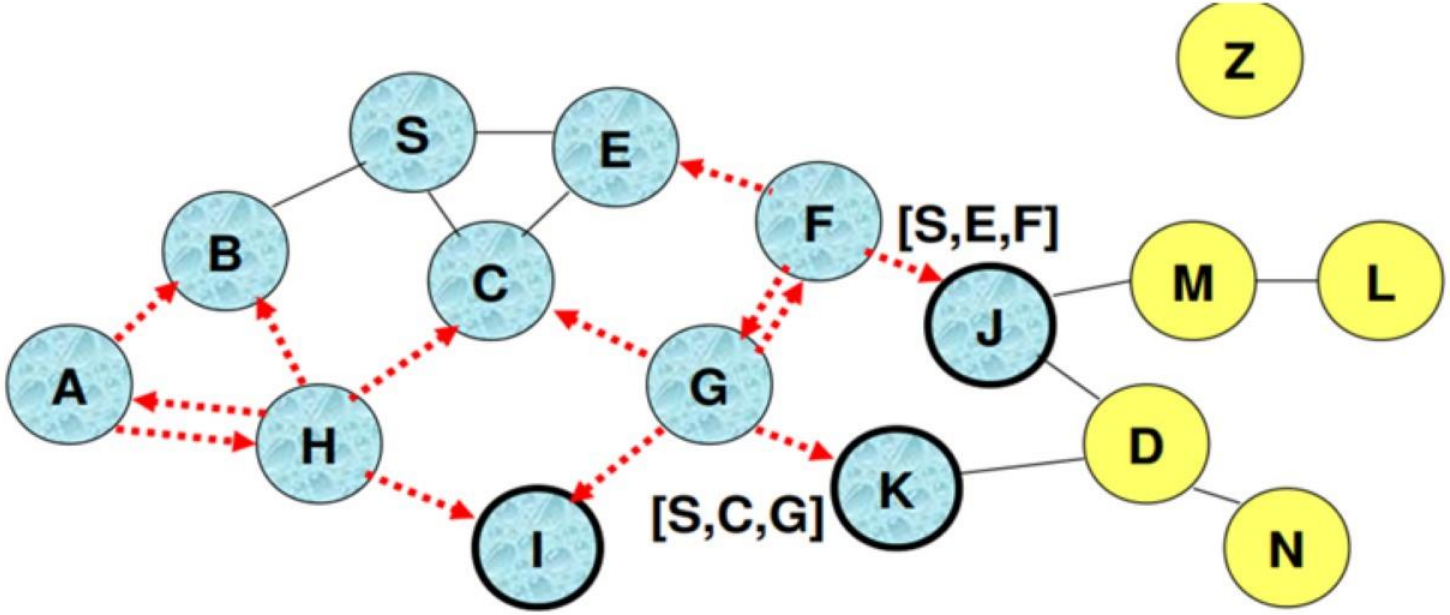
(b) Propagation of Route Reply with the Route Record

- EXAMPLE:
  - When node S wants to send a packet to node D, b ut does not know a route to D, node S initiates a r oute discovery
  - Source node S floods Route Request (RREQ)
  - Each node appends own identifier when forwardin g RREQ

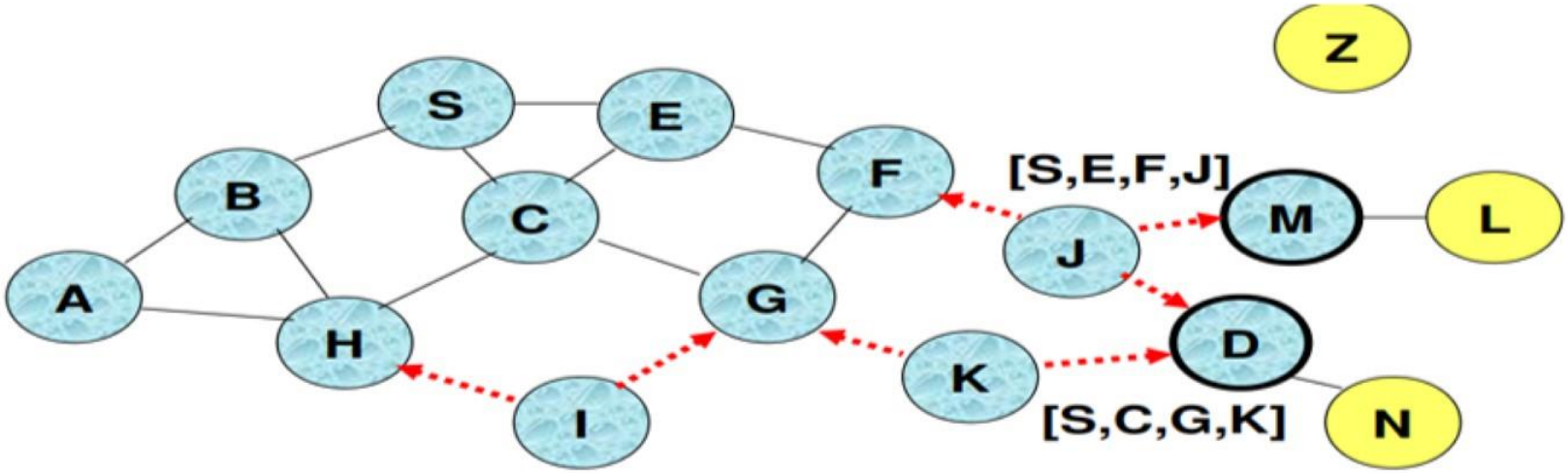




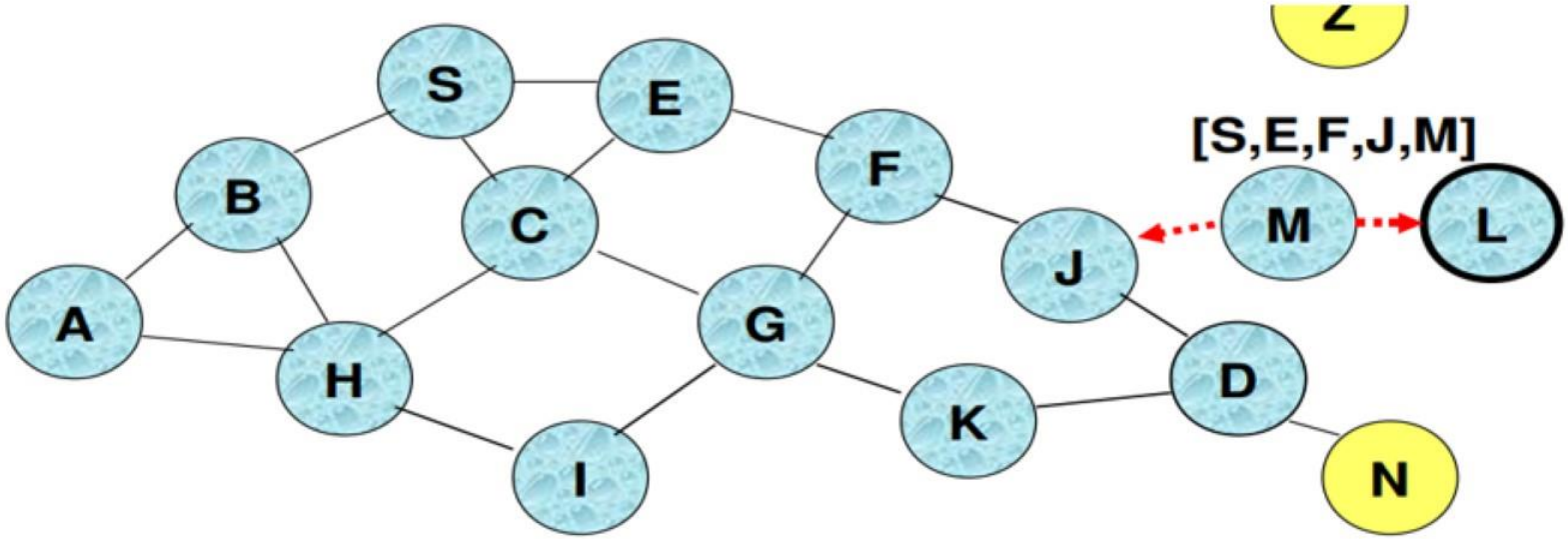
- Node H receives packet RREQ from two neighbors: potential for collision



- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

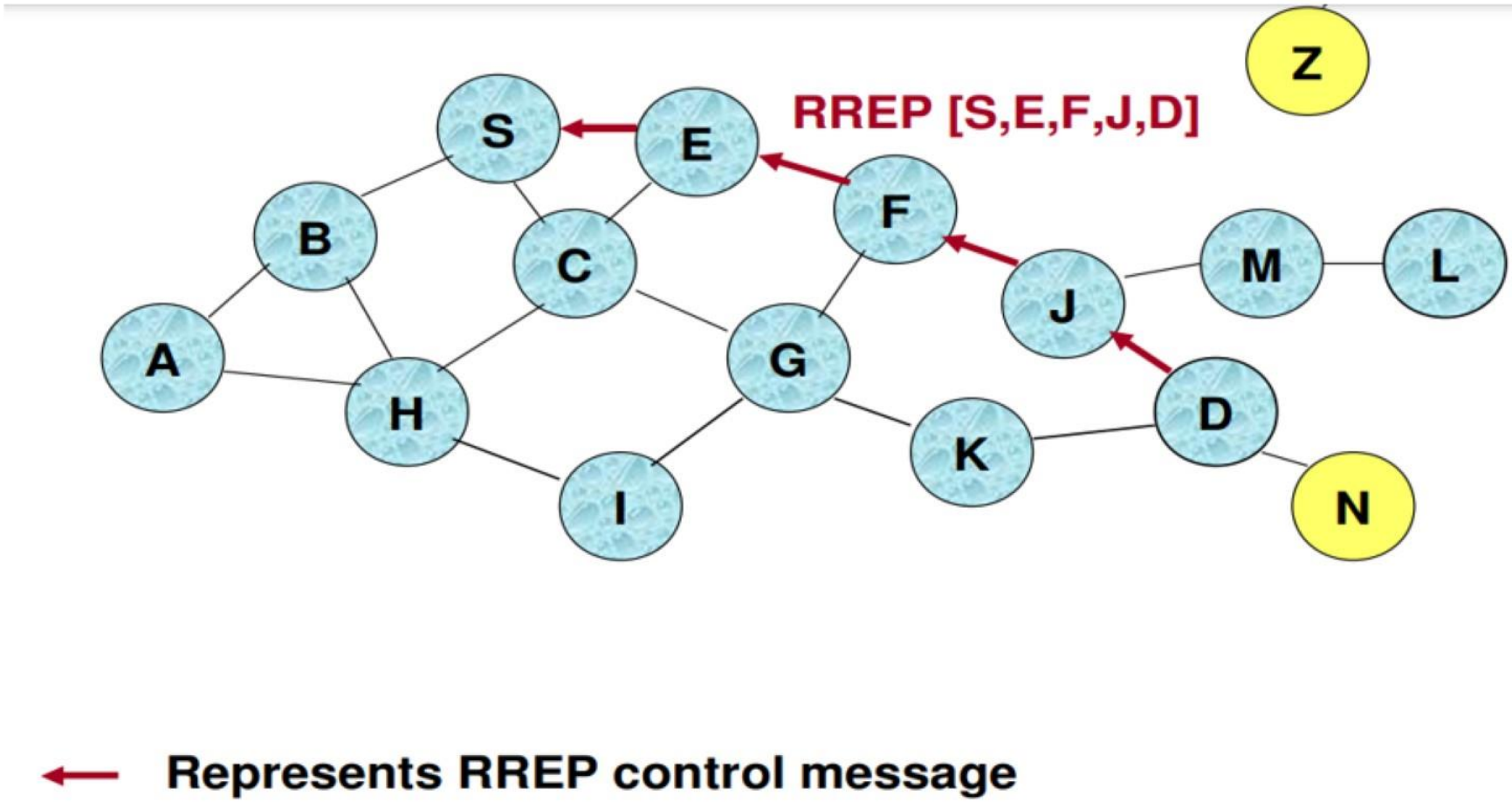


- Nodes J and K both broadcast RREQ to node D
- Since nodes J and K are hidden from each other, their transmissions may collide



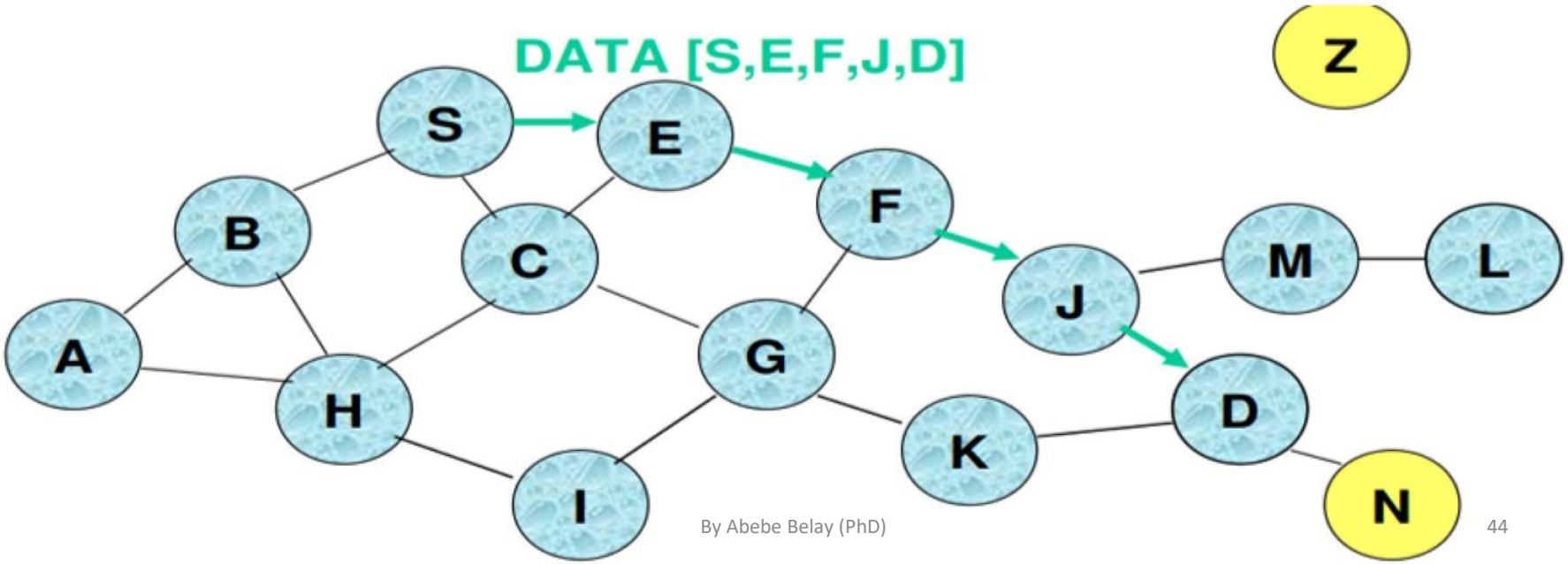
- Node D does not forward RREQ, because node D is the intended target of the route discovery

- Destination D on receiving the first RREQ, sends a Ro ute Reply (RREP)
- RREP is sent on a route obtained by reversing the rout e appended to received RREQ
- RREP includes the route from S to D on which RREQ was received by node D



Dynamic Source Routing (DSR)

- Node S on receiving RREP, caches the route included in the RREP
- When node S sends a data packet to D, the entire route is included in the packet header
  - hence the name source routing
- Intermediate nodes use the source route included in a packet to determine to whom a packet should be forwarded



DSR Optimization: Route Caching

- Each node caches a new route it learns by *any means*
- When node S finds route [S,E,F,J,D] to node D, node S also learns route [S,E,F] to node F
- When node K receives Route Request [S,C,G] destined for node, node K learns route [K,G,C,S] to node S
- When node F forwards Route Reply RREP [S,E,F,J,D], node F learns route [F,J,D] to node D
- When node E forwards Data [S,E,F,J,D] it learns route [E,F,J,D] to node D
- A node may also learn a route when it overhears Data
- Problem: Stale caches may increase overheads

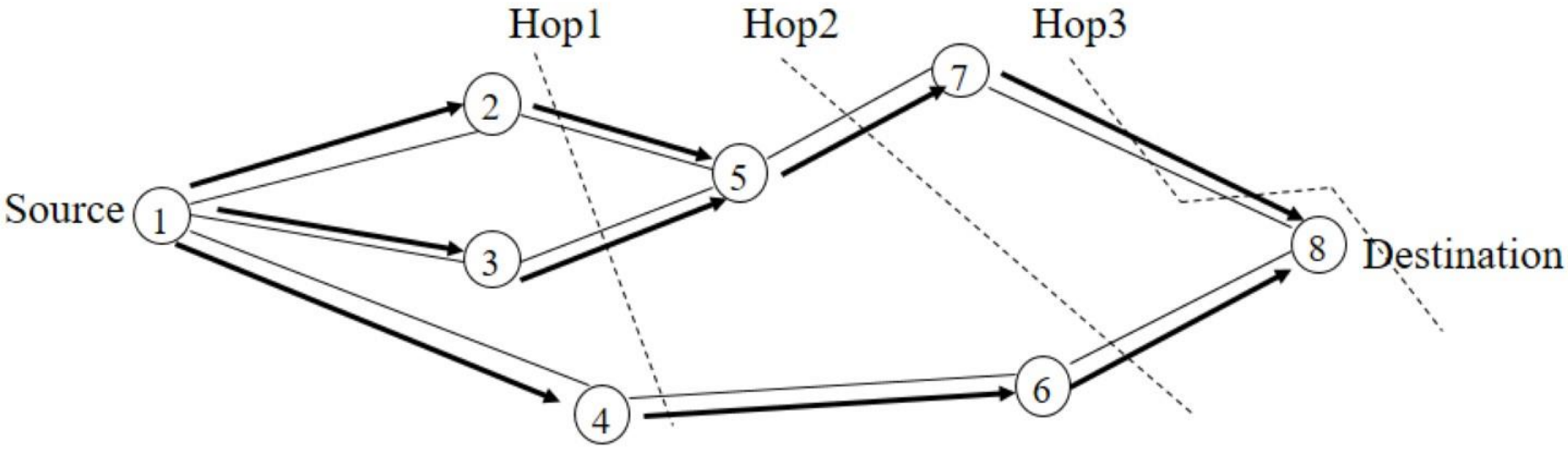
- **Advantages:**
  - Routes maintained only between nodes who ne ed to communicate-
    reduces overhead of route maintenance
  - Route caching can further reduce route discove ry overhead
  - A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches

- Disadvantages
  - Packet header size grows with route length due to so urce routing
  - Flood of route requests may potentially reach all no des in the network
  - Potential collisions between route requests propagat ed by neighboring nodes –
    insertion of random delays before forwarding RREQ
  - Increased contention if too many route replies come back due to nodes replying using their local cache –
    Route Reply Storm problem
  - Stale caches will lead to increased overhead

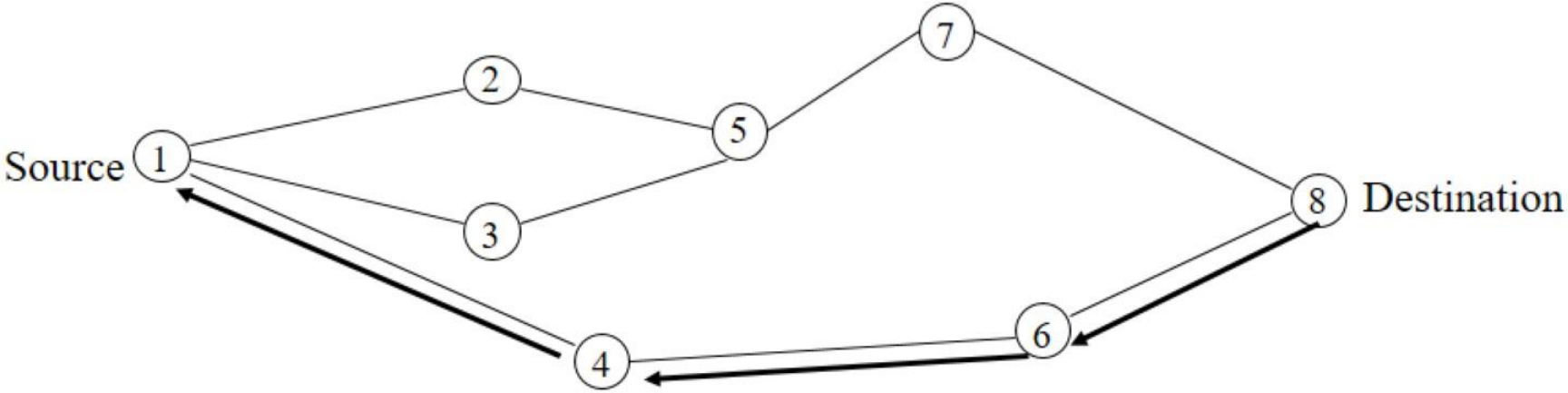
Ad hoc On-Demand Distance Vector Routing

- AODV is an improvement over DSDV, which minimizes the number of required broadcasts by creating routes on demand.
- Nodes that are not in a selected path do not maintain routing information or participate in routing table exchanges.
- A source node initiates a path discovery process to locate the other intermediate nodes (and the destination), by broadcasting a Route Request (RREQ) packet to its neighbors.
- AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to cont ain routes
- AODV retains the desirable feature of DSR that routes are maintained only between nodes which need to communicat e

Route Discovery in AODV Protocol



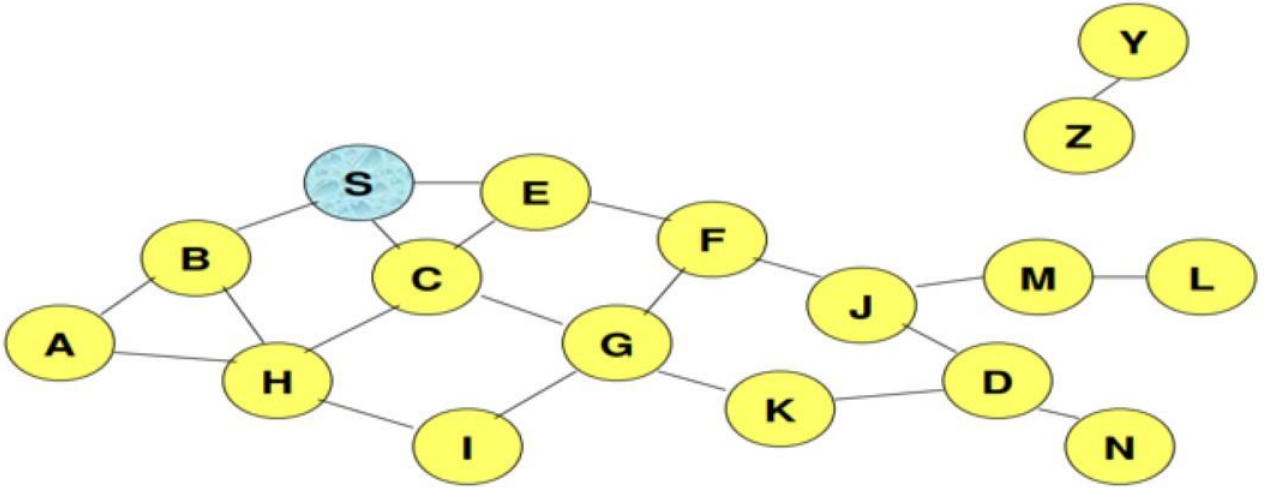
(a) Propagation of Route Request (RREQ) Packet



(b) Path Taken by the Route Reply (RREP) Packet

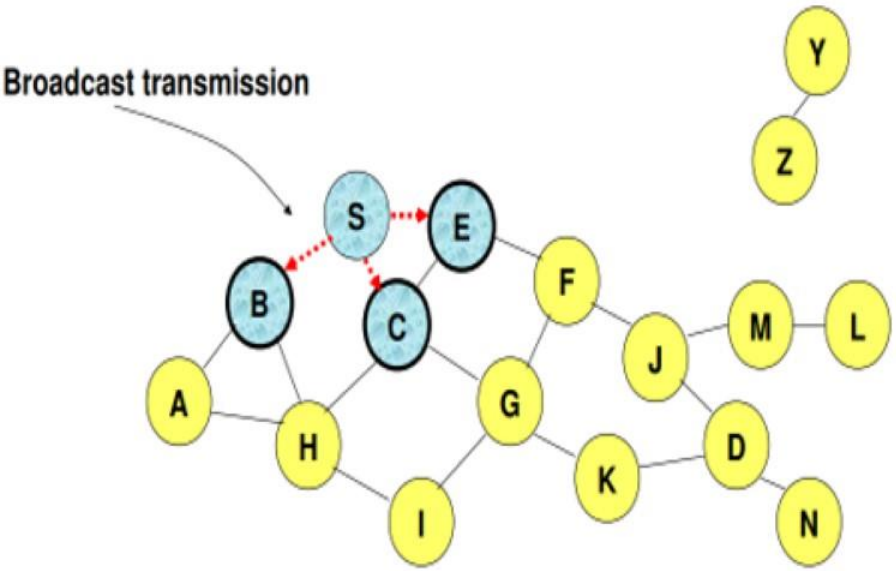
Step:

- Route Requests (RREQ) are forwarded in a manner similar t o DSR
- When a node re-broadcasts a Route Request, it sets up a reverse path pointi ng towards the source – AODV assumes symmetric (bi-directional) links
- When the intended destination receives a Route Request, it replies by sending a Route Reply (RREP)
- Route Reply travels along the reverse path set-up when Route Request is forwarded



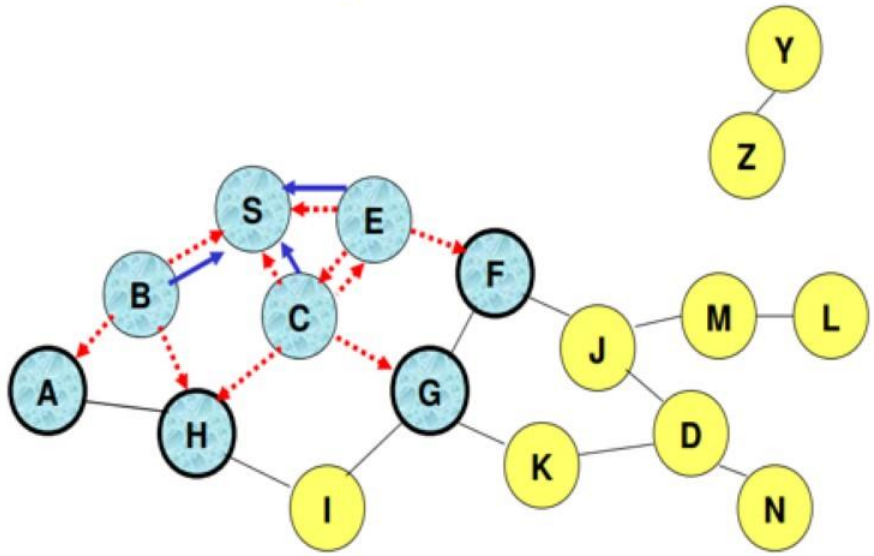
Represents a node that has received RREQ for D from S

Route Requests in AODV



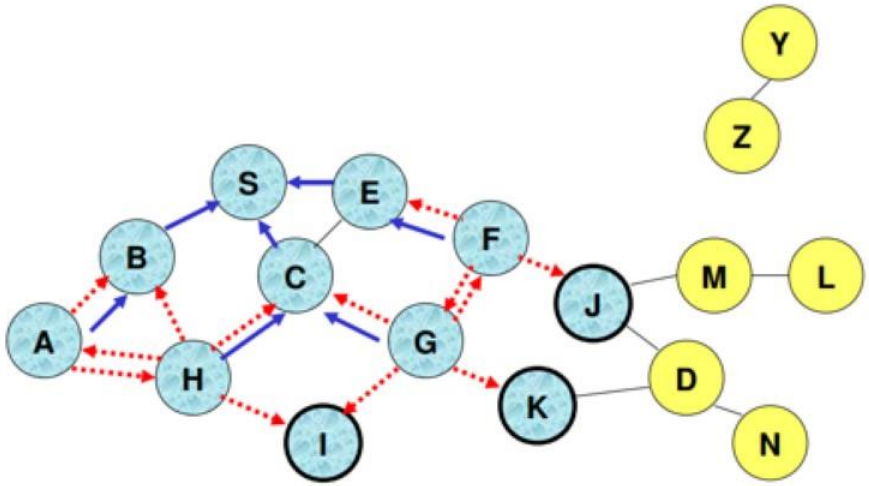
Represents transmission of RREQ

Route Requests in AODV



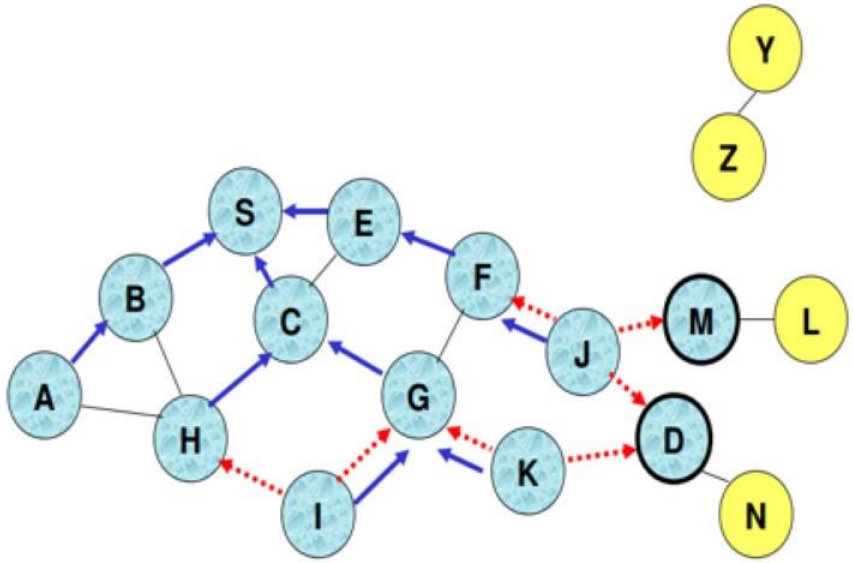
Represents links on Reverse Path

Reverse Path Setup in AODV

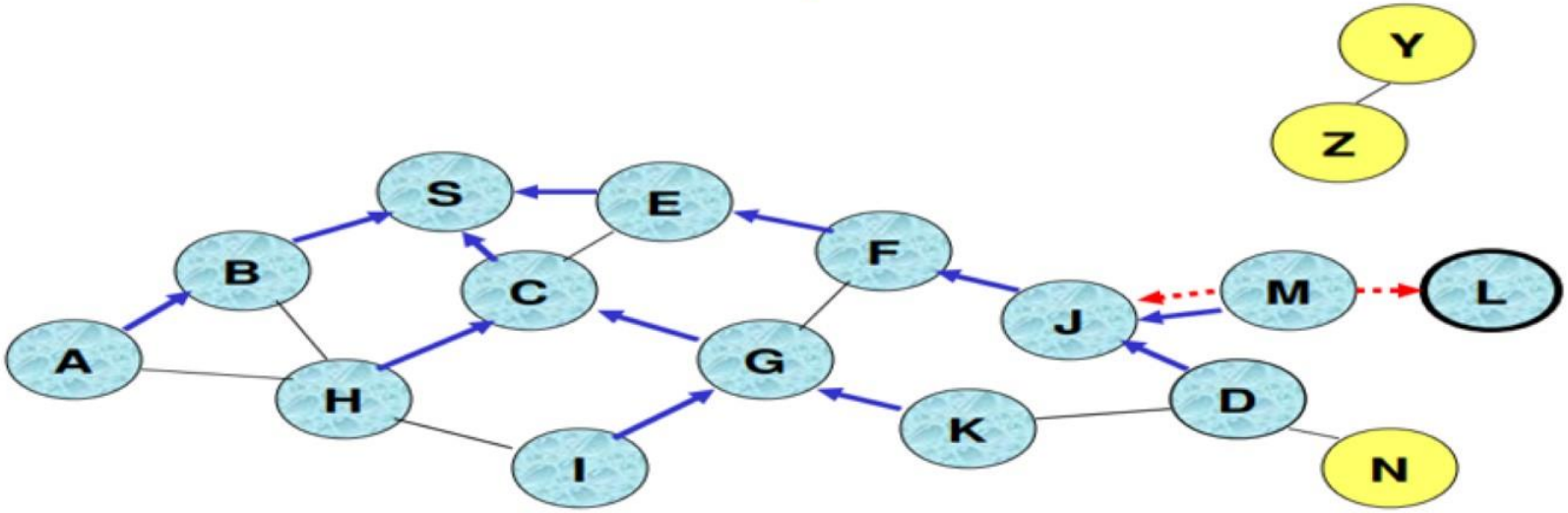


- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

Reverse Path Setup in AODV

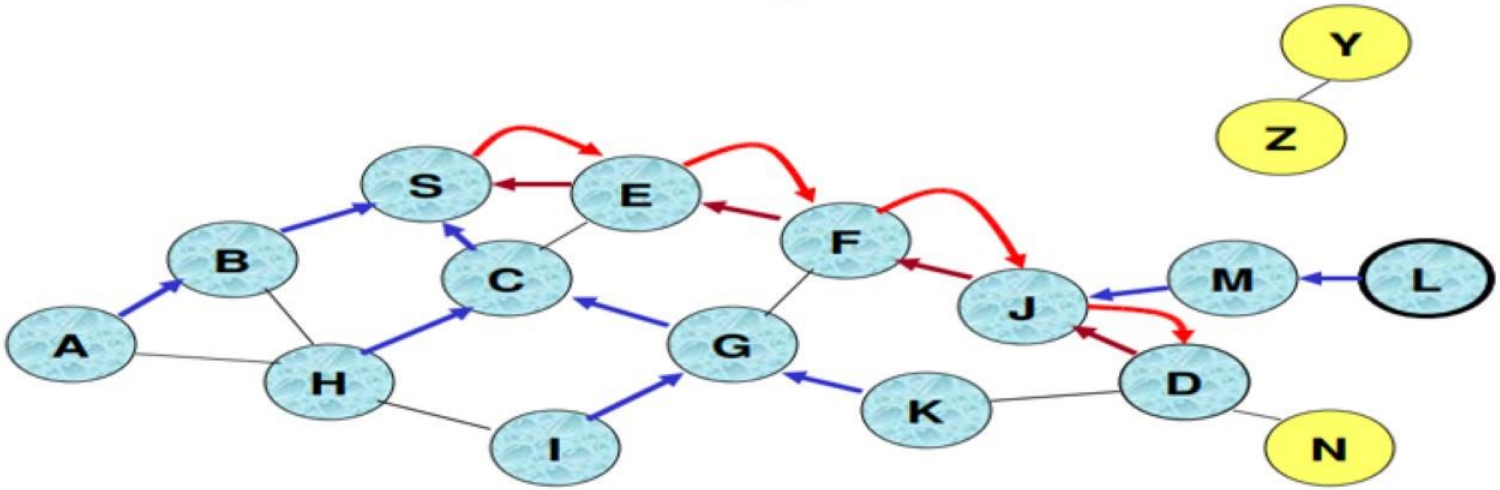


Reverse Path Setup in AODV



- Node D does not forward RREQ, because node D is the intended target of the RREQ

Forward Path Setup in AODV



Forward links are setup when RREP travels along the reverse path

Represents a link on the forward path

Route Request and Route Reply

- Route Request (RREQ) includes the last known sequence number for the destination
- An intermediate node may also send a Route Reply (RREP) provided that it knows a more recent path than the one previously known to sender
- Intermediate nodes that forward the RREP, also record the next hop to destination
- A routing table entry maintaining a reverse path is purged after a timeout interval
- A routing table entry maintaining a forward path is purged if *not used* for a *active_route_timeout* interval

Link Failure

- A neighbor of node X is considered active for a routing table entry if the neighbor sent a packet within *active_route_timeout* interval which was forwarded using that entry
- Neighboring nodes periodically exchange hello message
- When the next hop link in a routing table entry breaks, all active neighbors are informed
- Link failures are propagated by means of Route Error (RERR) messages, which also update destination sequence numbers

Route Error

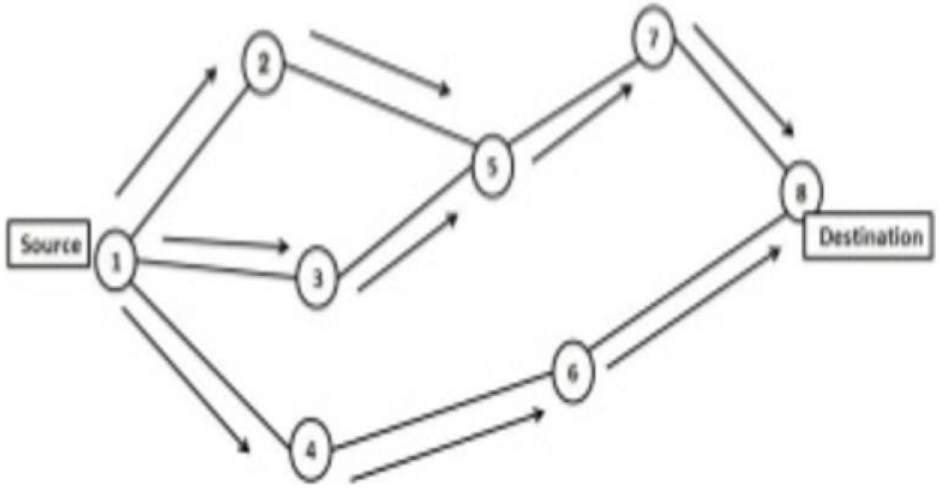
- When node X is unable to forward packet P (from node S to node D) on link (X,Y), it generates a RERR message
- Node X increments the destination sequence number for D cached at node X
- The incremented sequence number *N* is included in the RERR
- When node S receives the RERR, it initiates a new route discovery for D using destination sequence number at least as large as *N*
- When node D receives the route request with destination sequence number N, node D will set its sequence number to N, unless it is already larger than N

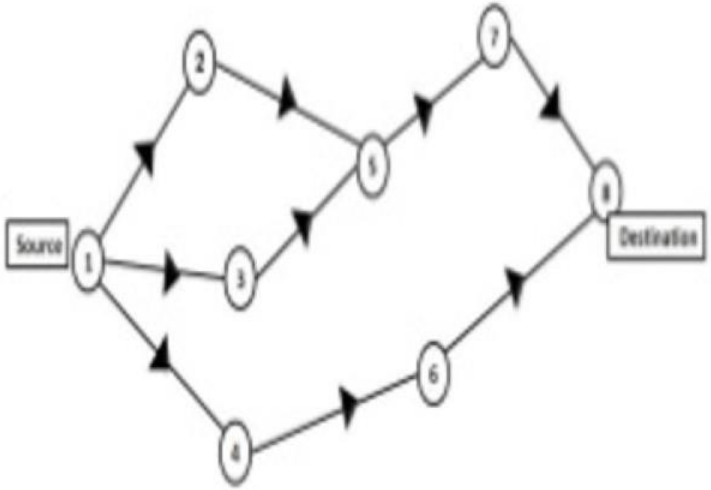
Temporarily Ordered Routing Algorithm (TORA)

- TORA is a highly adaptive loop-free distributed routing algorithm based on the concept of link reversal.
- TORA decouples the generation of potentially far-reaching control messages from the rate of topological changes.
- The height metric is used to model the routing state of the network.
- The protocol performs three basic functions: route creation, route maintenance, route erasure.
- During the route creation and maintenance phases nodes use a height metric to establish a Directed Acyclic Graph (DAG) rooted at the destination.
- Thereafter links are assigned a direction based on the relative heights.

TORA Routing Protocol

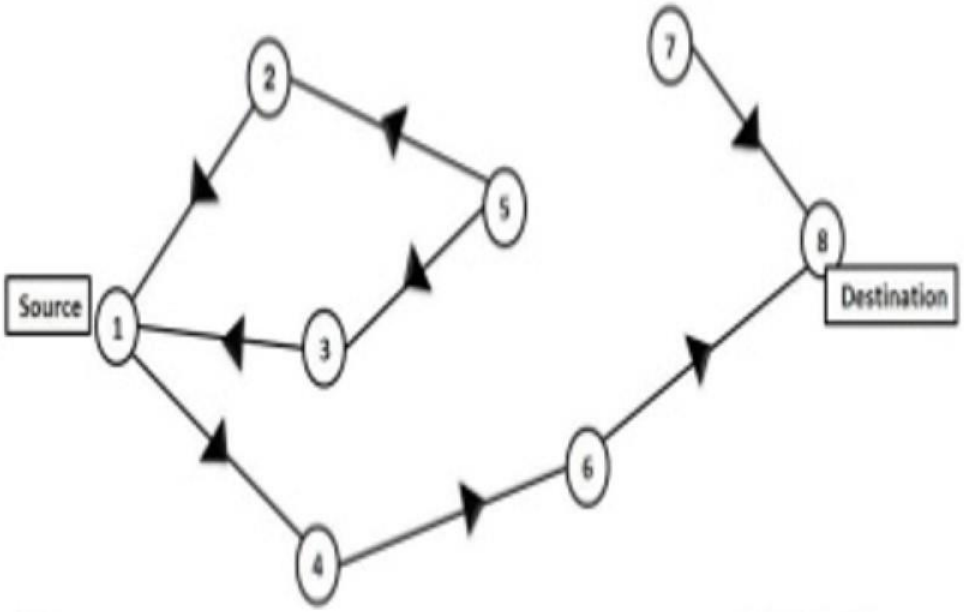
Temporary Ordered Routing Algorithm (TORA)

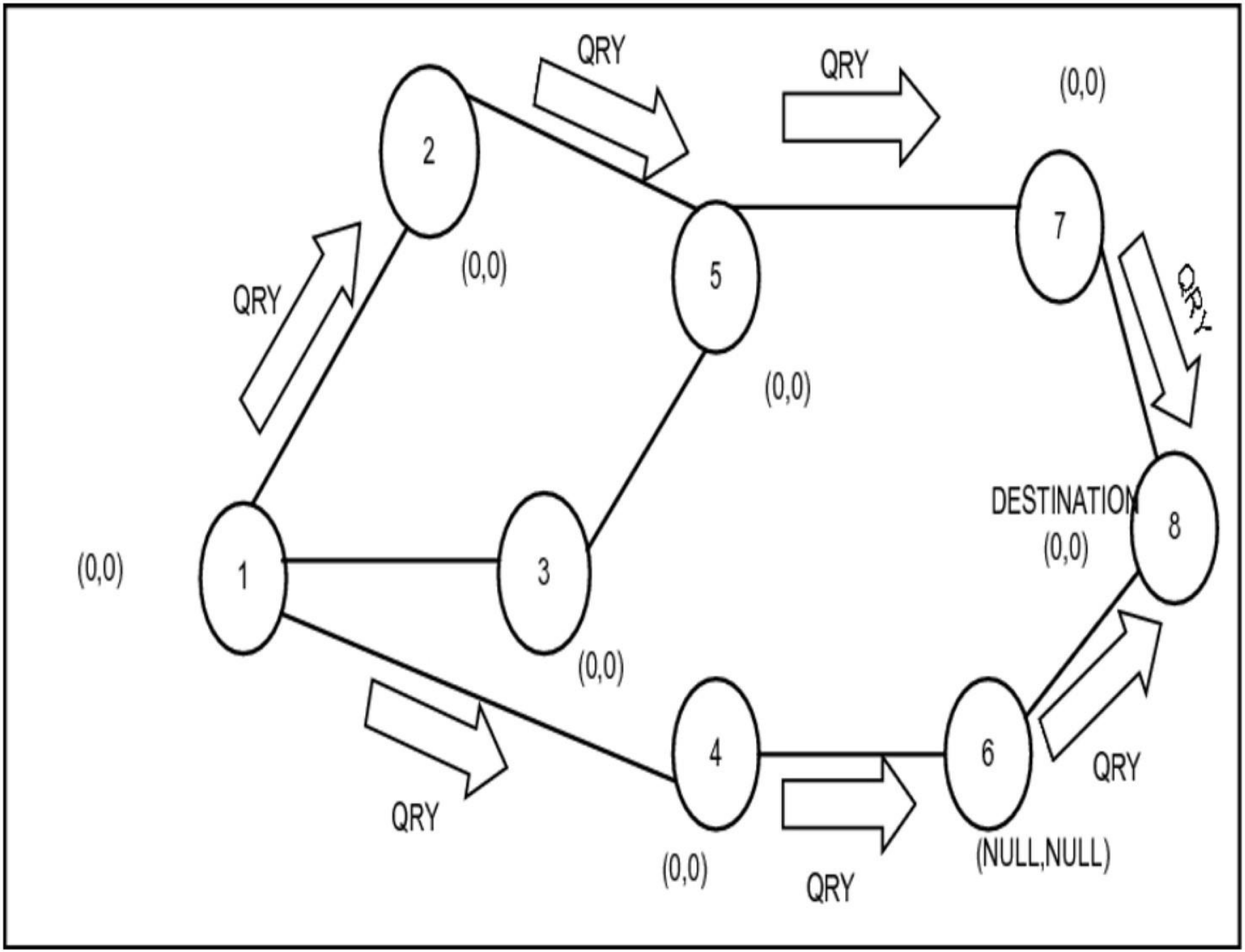




Height of each node updated a result of message

Re-establishing route on failure link 5-7.
The new reference level is node5




QRY
QRY
(0,0)
2
QRY
(0,0)
5
7
QRY
(0,0)
DESTINATION
(0,0)
8
(0,0)
1
3
(0,0)
4
6
QRY
QRY
(0,0)
QRY
(NULL,NULL)

TORA

- **Three major tasks**
  - **Route creation:** QRY and UPD packets
  - **Route maintenance**
  - **Route erasure**: Clear packet (CLR) is broadcasted
- Using Unique node ID and unique reference ID

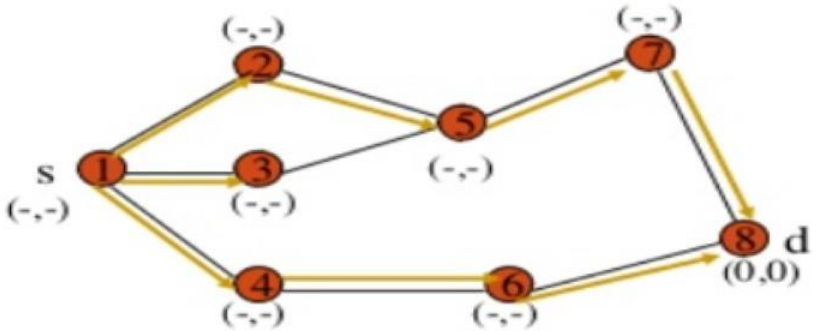
- **Route Creation**: demand driven "*query/reply*"
  - Performed only when a node requires a path to a destination but does not have nay directed link.
  - A query packet (QRY) is flooded through network
  - An update packet (UPD) propagates back if routes exist

- **Route Maintenance**: "*link-reversal*" algorithm
  - React only when necessary
  - Reaction to link failure is localized in scope

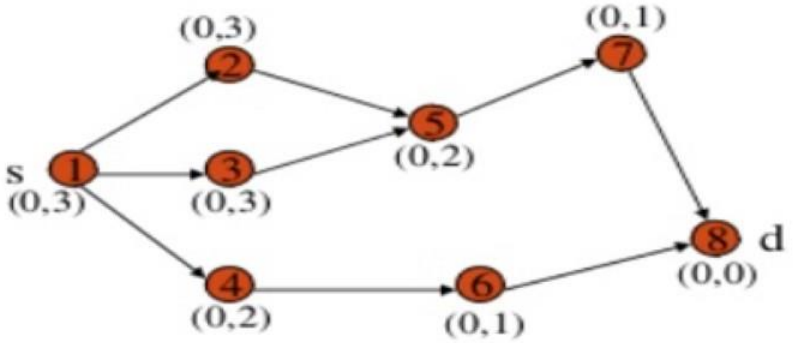
- **Route Erasure**:
  - A clear packet (CLR) is flooded through network to erase invalid routes

TORA

- Route creation of TORA



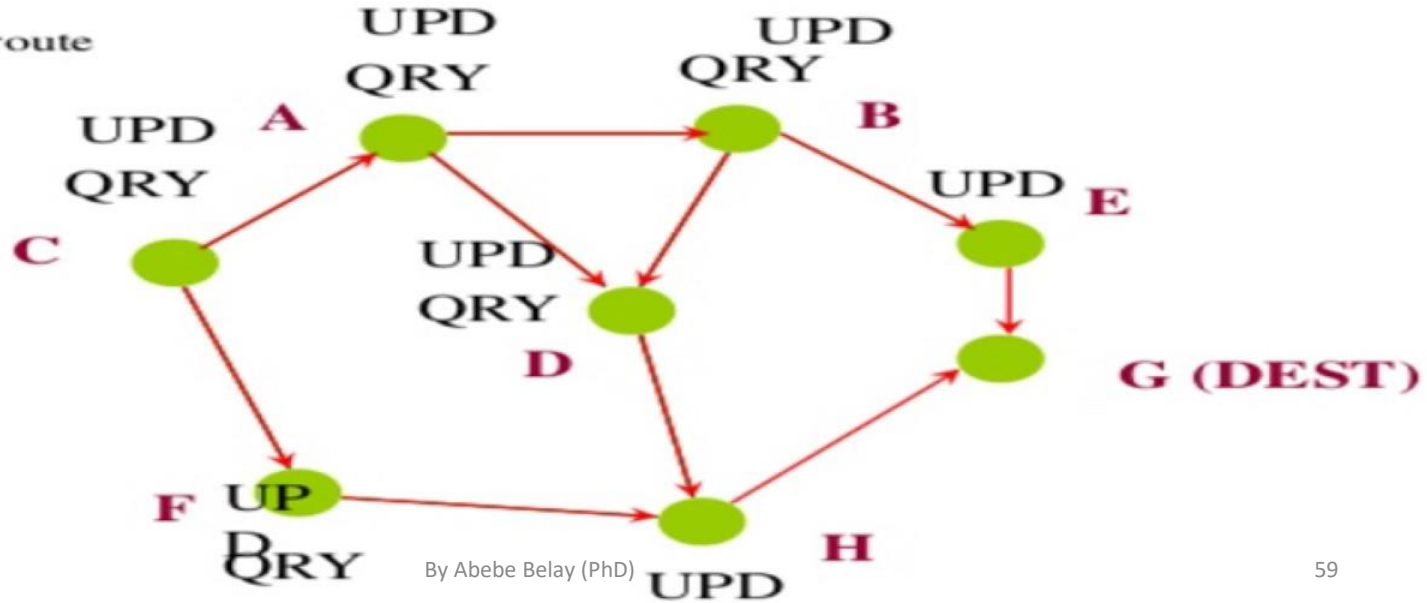
Propogation of QRY
(reference level, height)

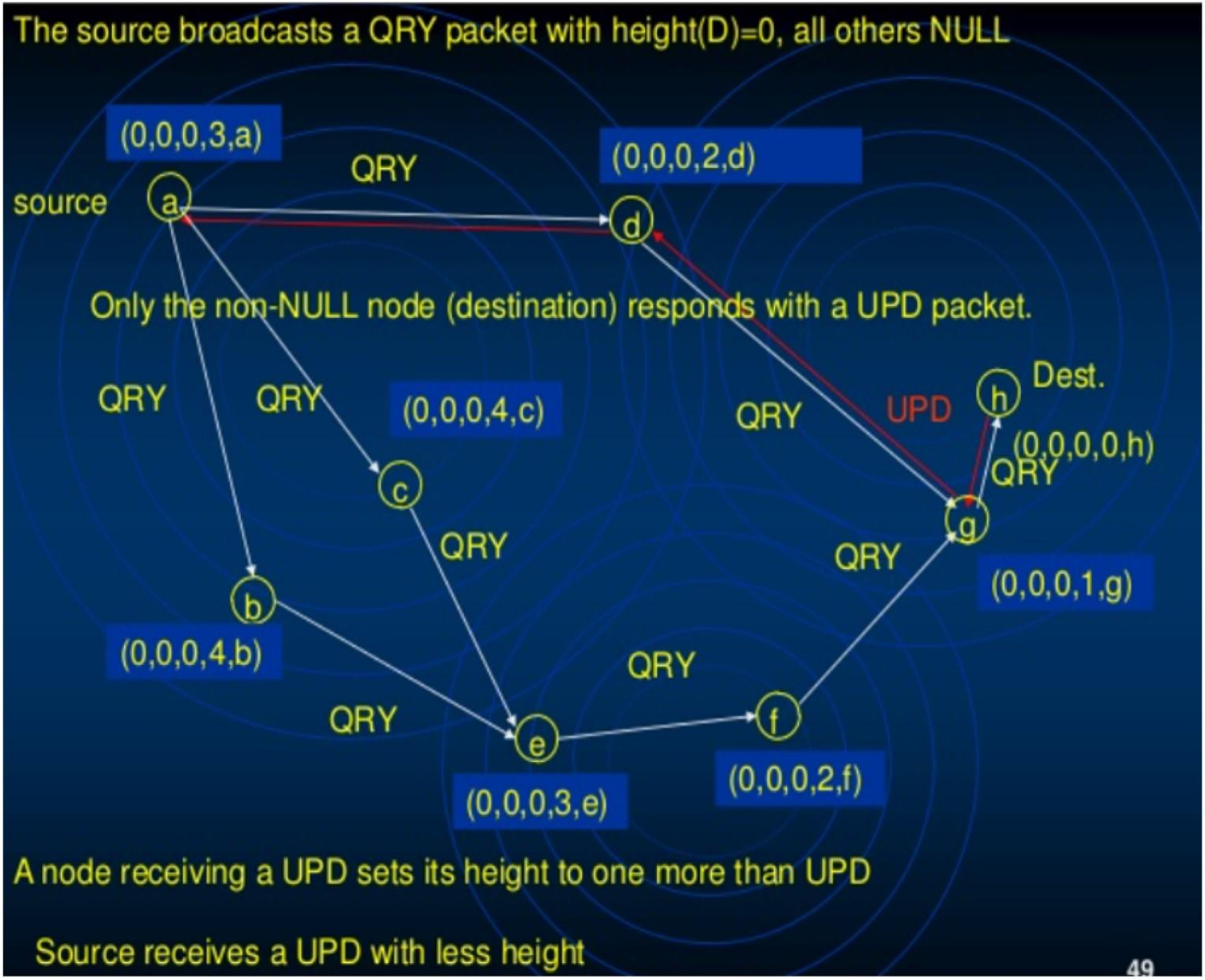


Height of each node
updated by UPD

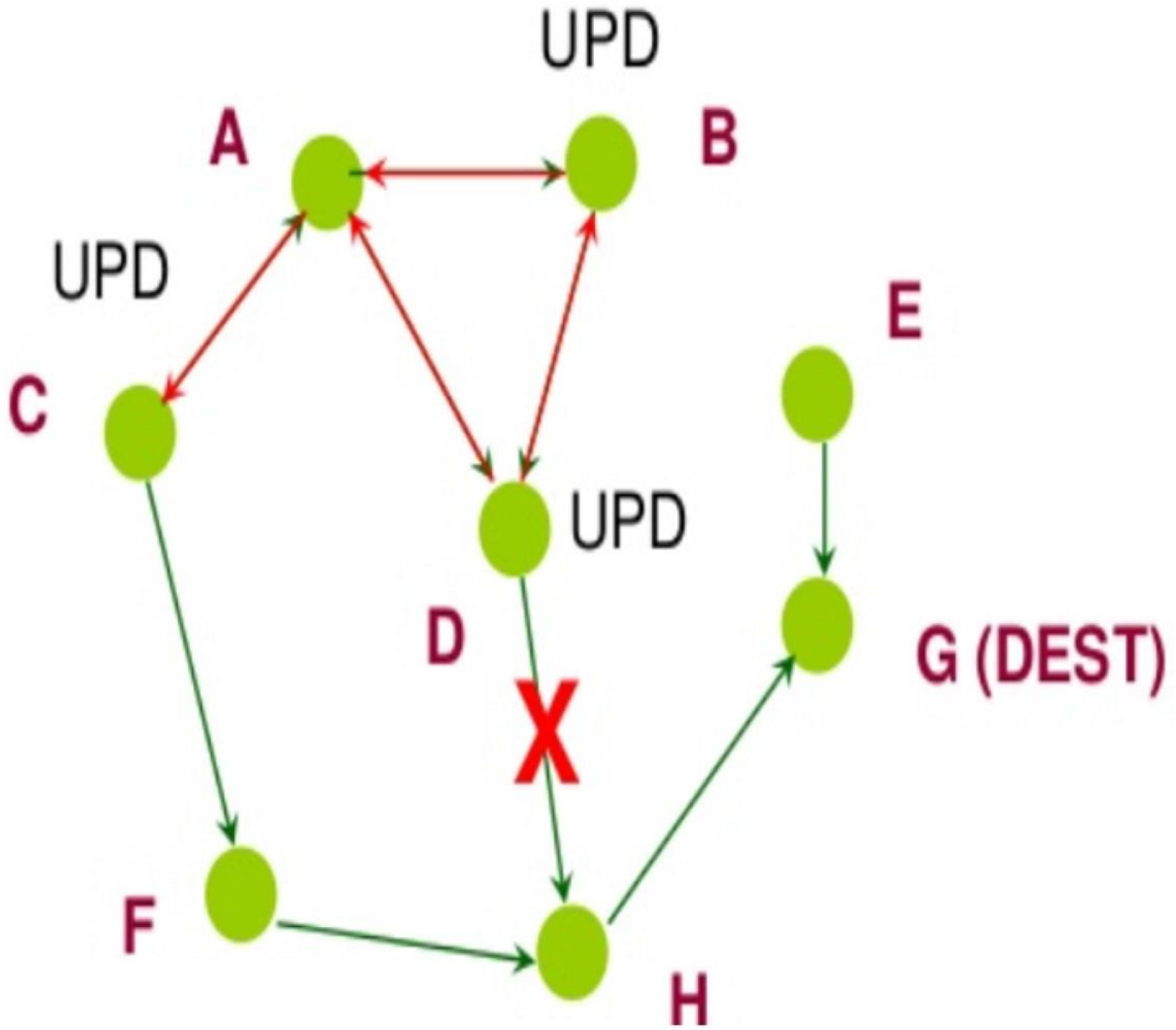
TORA

- Creation of route



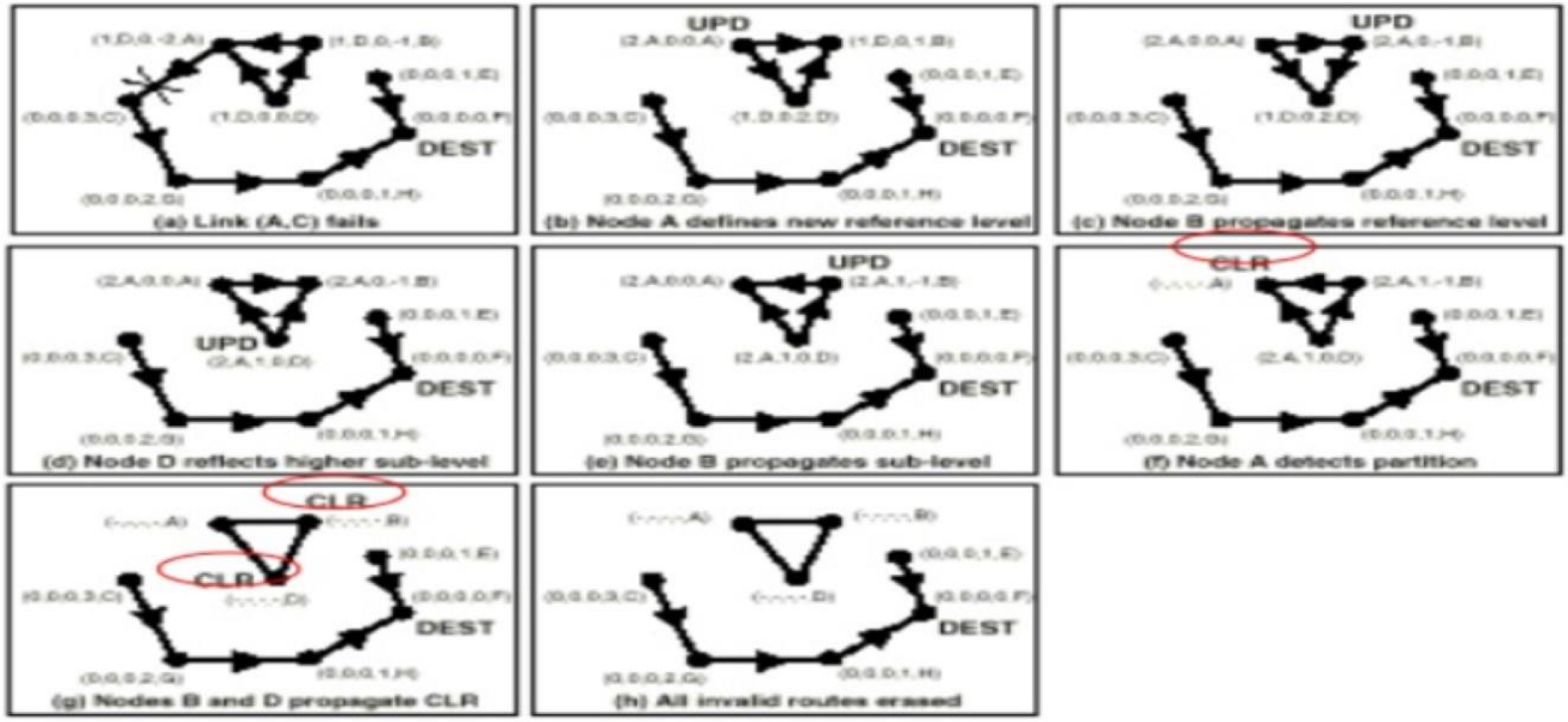

The source broadcasts a QRY packet with height(D)=0, all others NULL
(0,0,0,3,a)
QRY
(0,0,0,2,d)
source
a
d
Only the non-NULL node (destination) responds with a UPD packet.
QRY
QRY
(0,0,0,4,c)
QRY
UPD
h
Dest.
(0,0,0,0,h)
QRY
c
g
QRY
QRY
(0,0,0,1,g)
b
(0,0,0,4,b)
QRY
QRY
f
e
(0,0,0,2,f)
(0,0,0,3,e)
A node receiving a UPD sets its height to one more than UPD
Source receives a UPD with less height
49

- Route maintenance



50

TORA



TORA: Summary

Advantages

- **Less control overload**: by limiting the control packets for route reconfiguration to a small region

Disadvantage

- The local reconfiguration of paths results in non-optimal routes
- Concurrent deduction of partitions and subsequent deletion of routes could result in temporary oscillations and transient loops.

Associativity Based Routing (ABR)

- The three phases of ABR are: route discovery, route reconstruction, route deletion
- In ABR a route is selected based on the degree of stability associated with mobile node.
- Association stability is defined by connection stability of one node with respect to another node over time and space.
- Each node generates a beacon to signify its existence
- When received by neighboring nodes, the beacon causes their associativity tables to be updated
- The route discovery is accomplished by a Broadcast Query- Reply (BQ-REPLY) cycle
- When a discovered route is no longer desired, the source node initiates a Route Delete broadcast so that all the nodes along the route update their routing tables.

- First routing protocol that advocates the selection of stable links and routes for ad hoc wireless networks.
- **Goal: Best route is selected based on stability and shortest path of wireless link .**
- Associativity is related to the spatial, temporal, and connection stability of a mobile host (MH).
- **The stability is measured using associativity ticks(initially set to zero)**
- Each node broadcasts beacons, the nodes increment associativity ticks when they receive beacons and sets zero if beacon is not received. **High Associativity means high stability.**
- A node's association with its neighbors changes as it is migrating, and its transition period can be identified by associativity ticks or counts.

- **The protocol contains 3 phases:**
  - **Route discovery**: BQ-REPLY cycle
  - **Route reconstruction (RRC):**
  - **Route deletion (RD):** Source-initiated

Advantages

- Stable routes have a higher preference compared to shorter routes.
- Fewer path breaks
- Reduce the extent of flooding due to reconfiguration of paths in the network.

Disadvantage

- Chosen Path maybe longer than the shortest path between the source and destination because of the preference given to stable paths.
- Local query (LQ) broadcast may result in high delays during route repairs .

Signal-Stability-Based Routing (SSR)

- SSR selects a route based on the signal strength between nodes and a node's location stability
- This route selection criteria has the effect of choosing routes that have a better link connectivity

  - **Advance form of ABR**
  - **New metric:** *signal strength* between nodes and a node's location stability
  - Selects routes based on signal strength between nodes Prefers stronger connectivity.

  - **Tables**
    - Signal Strength Table (SST)–
      - *Periodic beacons from the link layer of the neighbouring nodes:*
      - fields [host, signal strength, last, clicks, set]
      - *Signal strength recorded by SST-- Weak or Strong*
    - Routing Table (RT)
      - field [destination, next host].

  - **Two protocols**
    - **Dynamic Routing Protocol (DRP):** manages SST & RT
    - **Static Routing Protocol (SRP):** forwards packets based on RT

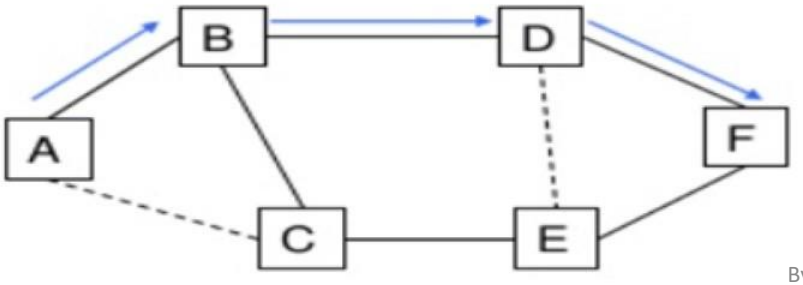
Signal Stability Routing (SSR)

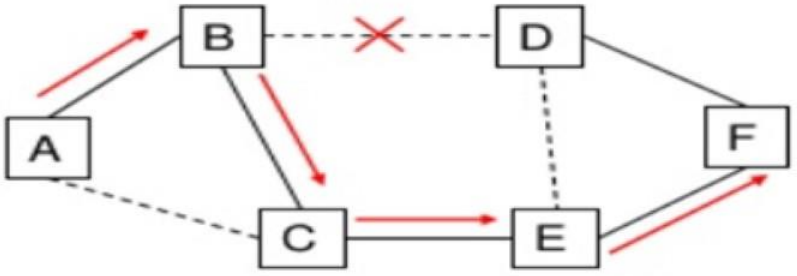
SSR consists of 2 cooperative protocols:

- **Dynamic Routing (DRP)**
  - Maintain **signal stability table**(SST) with and routing table(RT)
  - After updating all appropriate table entries, the DRP passes a received packet to the SRP
- **Static Routing (SRP) :**
  - Passing the packet up the stack if it is the intended receiver
  - If no entry is found in the RT for the destination, **initiate a route-search** process to find a route
  - Else forwarding the packet
  - Send a route reply message back to initiator

- **All transmission are received and processed by DRP**
- **After processing and updating the table DRP passes the packets to SRP**

- **Route discovery and route maintenance**
  - By default, only route request packets from strong channels are forwarded
  - initiate a new route-search process; erase the old route
- If there is no route-reply message received, the route changes to accept weak channel.





SSR: Summary

Advantages

- To select strong connection leads to fewer route reconstruction
- More stable route as compared to shortest path route selection protocols such as AODV and DSR.

Disadvantage

- Long delay since intermediate nodes can't answer the path (unlike AODV, DSR)

LocationAided Routing (LAR)

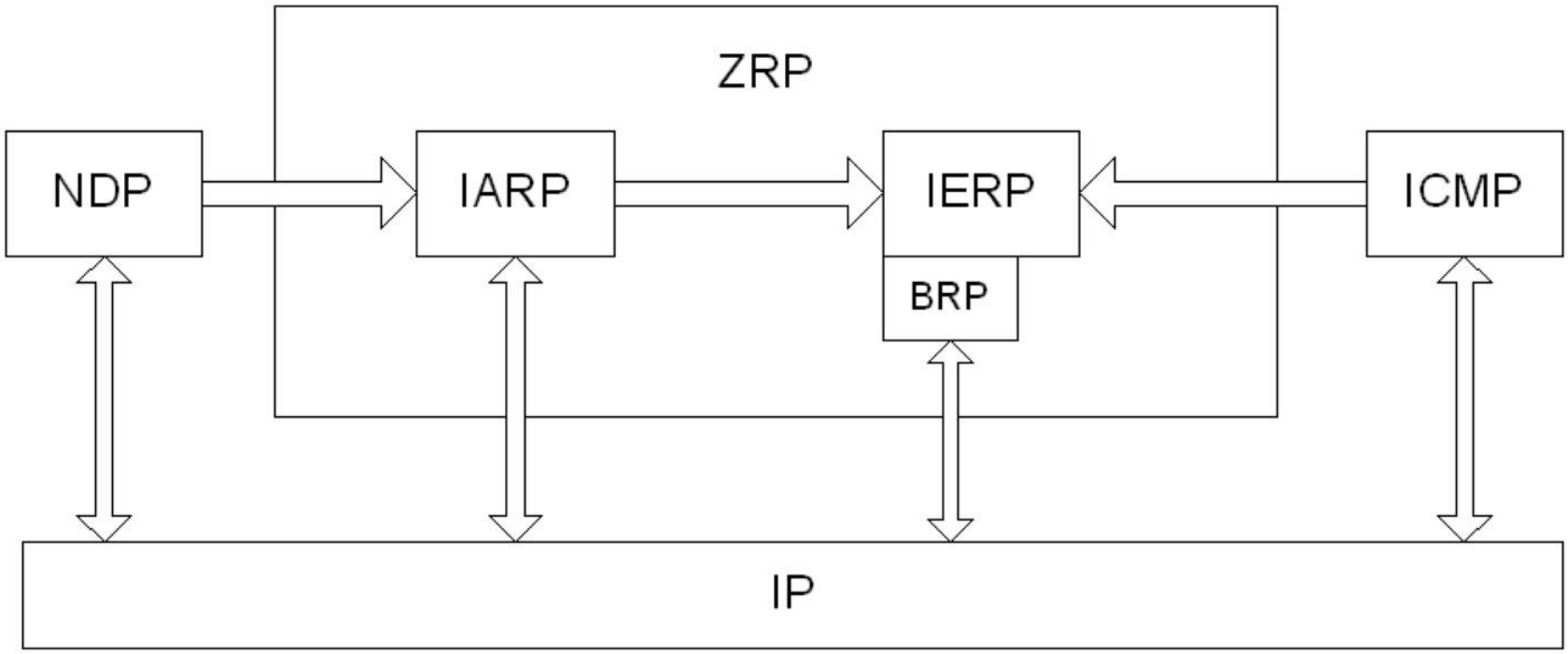
- Exploits location information to limit scope of route request flood
  - Location information may be obtained using GPS
- Expected Zone is determined as a region that is expected to hold the current location of th e destination
  - Expected region determined based on potentially old location information, and knowledge of the d estination's speed
- Route requests limited to a Request Zone that contains the Expected Zone and location of the sender node

- Define a Request Zone
- LAR is same as flooding, except that only nodes in request zone forward route request
- Smallest rectangle including S and expected zone for D



- Advantages
  - reduces the scope of route request flood
  - reduces overhead of route discovery
- Disadvantages
  - Nodes need to know their physical locations
  - Does not take into account possible existence of o bstructions for radio transmissions

Hybrid routing protocols



A ⟹ B Information passed from protocol A to B

A ⟺ B Exchange of packets between protocol A and B

Hybrid routing protocols – cont. 1

1) Zone Routing Protocol (ZRP): A node proactively maintains routes to destinations within a local neighborhood
   - The construction of a routing zone requires a node to first know who its neighbor, which is implemented through a MAC layer Neighbor Discovery Protocol

2) Fisheye State Routing (FSR): There are multi-level fisheye scopes to reduce routing update overhead in large networks
   - It helps to make a routing protocol scalable by gathering data on the topology, which may be needed soon.

3) Landmark Routing (LANMAR): Uses a landmark to keep track of a logical subnet
   - The LANMAR routing table includes only those nodes within the scope and the landmark nodes themselves

Hybrid routing protocols – cont. 2

4) Location-Aided Routing (LAR): Exploits location information to limit the scope of routing
   - LAR limits the search based on the expected location of the destination node and thereby restricts and controls the flood of Route Request packets

5) Distance Routing Effect Algorithm for Mobility (DREAM) : Based on the distance effect and a node's mobility rate
   - Each node can optimize the frequency at which it sends updates to the networks and correspondingly reduce the bandwidth and energy used

6) Relative Distance Micro-discovery Ad Hoc Routing (RDMAR): Based on the calculated relative distance between two terminals
   - The query flood is localized to a limited region centered at the source node

Hybrid routing protocols – cont. 3

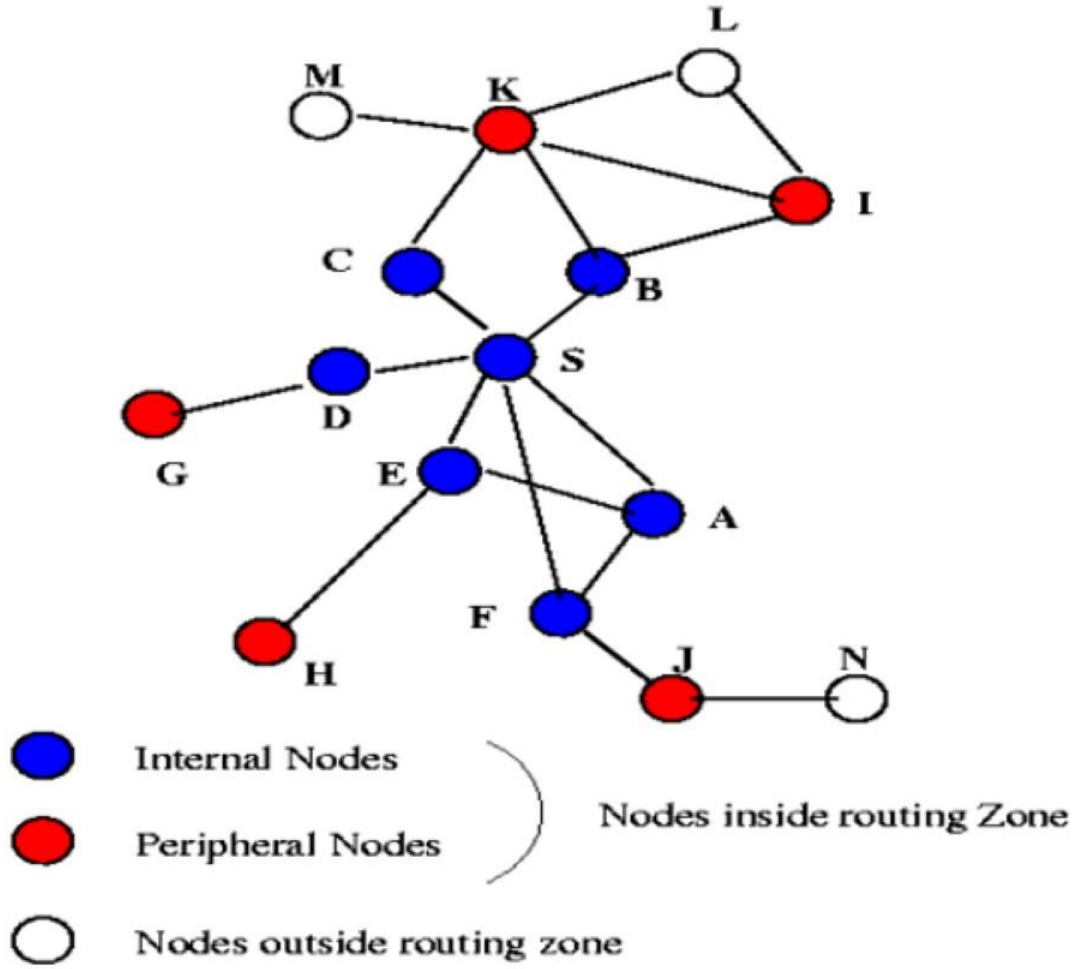
7) Power Aware Routing: Power-aware metrics are used for determining routes

- It reduces the cost, ensures that the mean time to node failure is increased, without any further delay in packet delivery.

Example

- Zone Routing Protocol (ZRP)
  - ZRP combines proactive and reactive approaches
  - All nodes within hop distance at most *d* from a node X are said to be in the routing zone of node X
  - All nodes at hop distance exactly *d* are said to be peripheral nodes of node X's routing zone
  - Intra-zone routing: Proactively maintain routes to all nodes within the source node's own zone.
  - Inter-zone routing: Use an on-demand protocol (similar to DSR or AODV) to determine routes to outside zone.

Zone Routing Protocol (ZRP)



Radius of routing zone = 2

Summary of Some Characteristics of Selected Protocols

Pro-tocol	Route Acquisi-tion	Flood for Route Discovery	Delay for Route Discover y	Multipath Capability	Effect of Route Failure
DSDV	Compute d a priori	No	No	No	Updates the routing tables of all nodes
WRP	Compute d a priori	No	No	No	Ultimately, updates the routing tables of all nodes by exchanging MRL between neighbors
DSR	On-demand, only when needed	Yes. Aggressive use of caching may reduce flood	Yes	Not explicitly. The technique of salvaging may quickly restore a route	Route error propagated up to the source to erase invalid path

Summary of Some Characteristics of Selected Protocols – cont.

Pro-tocol	Route Acquisi-tion	Flood for Route Discovery	Delay for Route Discovery	Multipath Capability	Effect of Route Failure
AODV	On-demand, only when needed	Yes. Controlled use of cache to reduce flood	Yes	No, although recent research indicate viability	Route error propagated up to the source to erase invalid path
TORA	On-demand, only when needed	Basically one for initial route discovery	Yes. Once the DAG is constructed, multiple paths are found	Yes	Error is recovered locally
LAR	On-demand, only when needed	Reduced by using location information	Yes	No	Route error propagated up to the source
ZRP	Hybrid	Only outside a source's zone	Only if the destination is outside the source's zone	No	Hybrid of updating nodes' tables within a zone and propagating route error to the source

Practical areas MANET

1.Vehicular Ad hoc Network (VANETs) –
Enable effective communication with another vehicle or with the roadside equipments. Intelligent vehicular ad hoc networks(InVANETs) deals with another vehicle or with roadside equipments.

2.Smart Phone Ad hoc Network (SPANC) –
To create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. Here peers can join or leave the network without destroying it.

3.Internet based Mobile Ad hoc Network (iMANETs) –
It supports internet protocols such as TCP/UDP and IP. To link mobile nodes and establish routes distributed and automatically.

4.Hub-Spoke MANET:
Multiple sub MANET's may be connected in hub-spoke VPN to create a geographically distributed MANET. Normal Ad-hoc routing algorithm does not apply directly.

5.Military or Tactical MANETs –
This is used by the military units. Emphasis on data rate, real-time demand, fast re-routing during mobility, security, radio range, etc.

6.Flying Ad hoc Network (FANETs) –
This is composed of unmanned aerial vehicles (commonly known as drones). Provides links to remote areas and mobility.

2.3. Transport in MANET

- **User Datagram Protocol (UDP)**
- Studies comparing different routing protocols for MANET typically measure UDP performance
- Several performance metrics are used
  - – routing overhead per data packet
  - – packet delivery delay
  - – throughput/loss
- Many variables affect performance
  - – Traffic characteristics
  - – Mobility characteristics
  - – Node capabilities
- Difficult to identify a single scheme that will perf orm well in all environments

- **Transmission Control Protocol (TCP)**
- Reliable ordered delivery
  - Reliability achieved by means of retransmissions if neces sary
- Endtoend semantics
  - Receiver sends cumulative acknowledgements for in-sequence packets
  - Receiver sends duplicate acknowledgements for out of-sequence packets
- Implements congestion avoidance and control using slidingwindow
  - Window size is minimum of
    - receiver's advertised window- determined by available buffer space at the receiver
    - congestion window - determined by the sender, based on feedback from the networ k
  - Congestion window size bounds the amount of data that can be sent per roundtrip time

Detection of packet loss in TCP

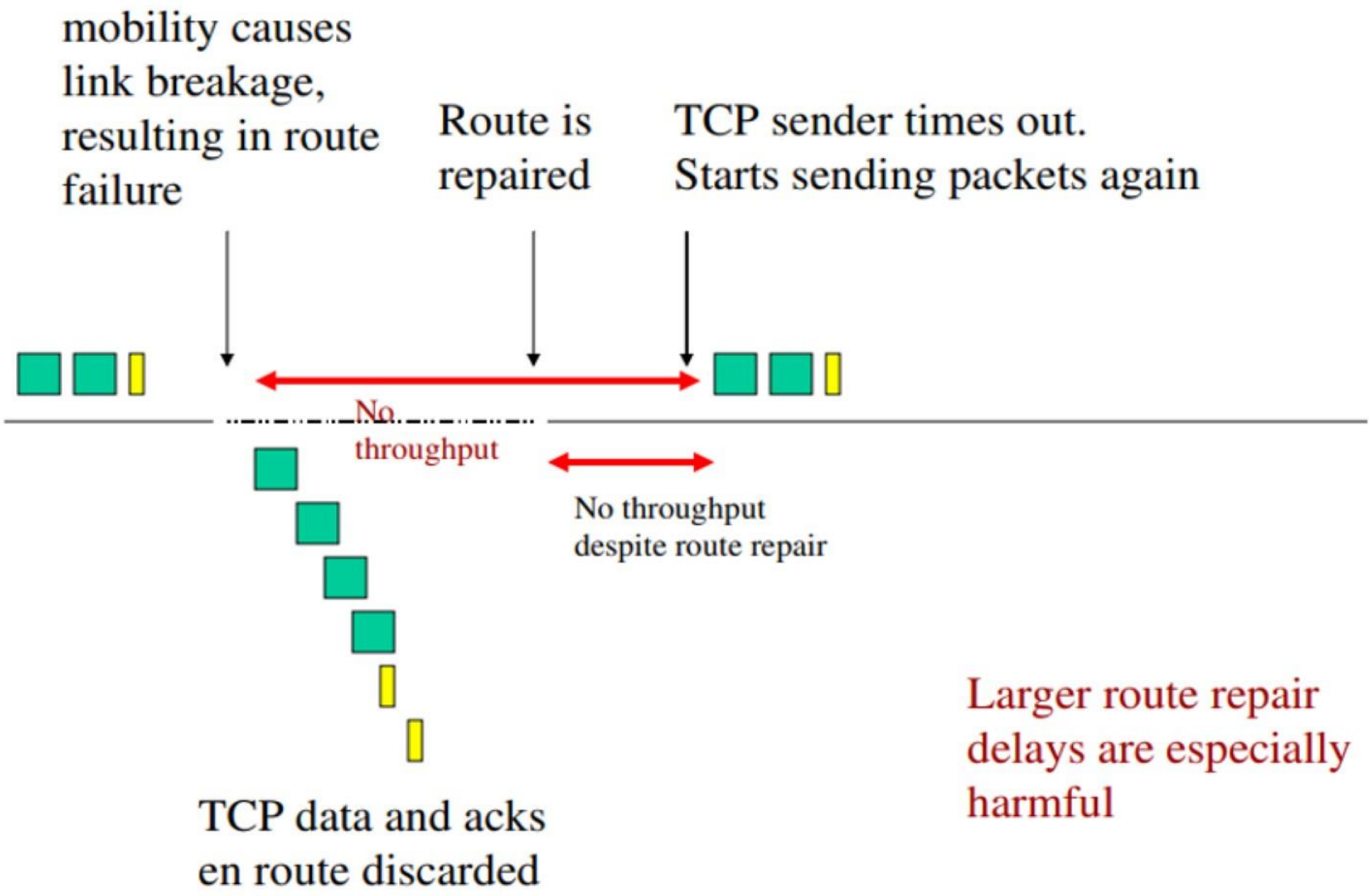
- Retransmission timeout (RTO)
  - sender sets retransmission timer for only one pac ket
  - if Ack not received before timer expiry, the packet is assumed lost
  - RTO dynamically calculated, doubles on each time out
- Duplicate acks
  - sender assumes packet loss if it receives three co nsecutive duplicate acknowledgements (dupacks)
- On detecting a packet loss, TCP sender assu mes that network congestion has occurred a nd drastically reduces the congestion window

- Several factors affect TCP performance in MA NET:
  - Wireless transmission errors
    - may cause fast retransmit, which results in
      - retransmission of lost packet
      - reduction in congestion window
    - reducing congestion window in response to errors is un necessary
  - Multihop routes on shared wireless medium
    - Longer connections are at a disadvantage compared to shorter connections, because they have to contend f or wireless access at each hop
  - Route failures due to mobility

- Impact of Multihop Wireless Paths
  - Packet transmission can occur on at most one hop among three consecutive hops – Increasing the number of hops from 1 to 2, 3 results in increased delay, and decreased throughput
  - Increasing number of hops beyond 3 allows simultaneous transmissions on more than one link, however, degradation continues due to contention between TCP Data and Acks traveling in opposite directions
  - When number of hops is large enough (>6), throughput stabilizes

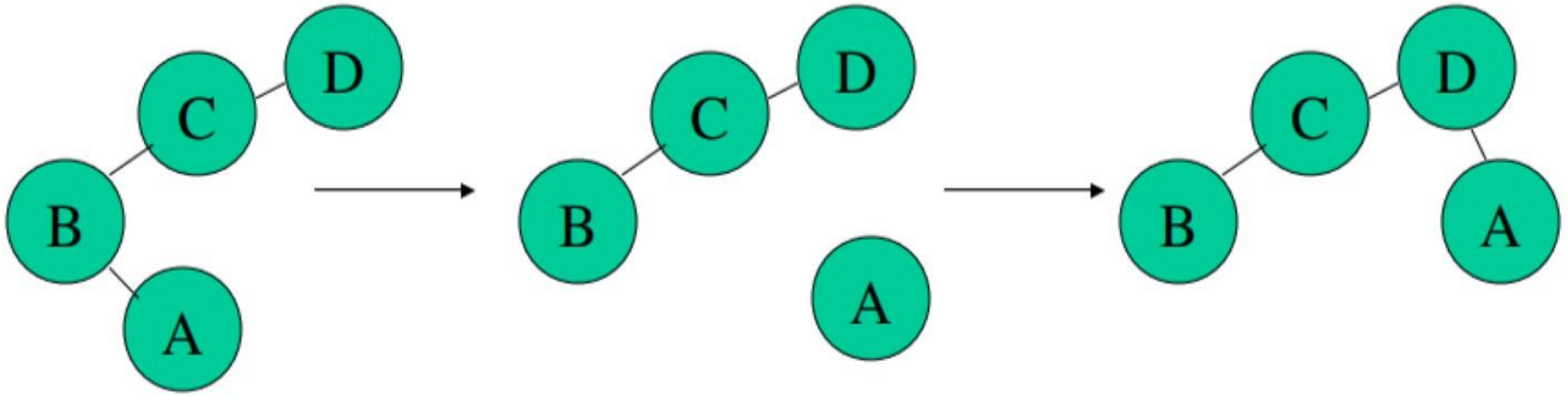
Impact of Node Mobility

TCP throughput degrades with increase in mobility but not always



Larger route repair delays are especially harmful

Improved Throughput with Increased Mobility



- Low speed: (Route from A to D is broken for ~1.5 seconds)
  - When TCP sender times after 1 second, route still broken.
  - TCP times out after another 2 seconds, and only then resumes

- High speed: (Route from A to D is broken for ~0.75 seconds)
  - When TCP sender times out after 1 second, route is repaired

- TCP timeout interval somewhat (not entirely) independent of speed
- Network state at higher speed may sometimes be more favorable than lower speed

Impact of Route Caching

TCP performance typically degrades when caches are used for route repair

- When a route is broken, route discovery returns a cached route from local cache or from a nearby node
- After a time-out, TCP sender transmits a packet on the new route. However, typically the cached route has also broken after it was cached



- Another route discovery, and TCP time-out interval
- Process repeats until a good route is found

- Caching can result in faster route repair
  - Faster does not necessarily mean correct
  - If incorrect repairs occur often enough, caching performs poorly

- If cache accuracy is not high enough, gains in routing overhead may be offset by loss of TCP performance due to multiple time-outs

- Need mechanisms for determining when cached routes are stale

Assignments:

1. **Develop a python program to simulate the following algorithm (10%) :**
   - Distance vector routing algorithm--Yitayew
   - Flooding routing algorithms--Meseret
   - Ad hoc on-demand distance vector (AODV)--Gashaye
   - Temporarily ordered routing algorithm (TORA)---Bereket