Routing protocols in Adhoc networks

SUBMITTED BY:
13MIT0062

MANET

- Mobile adhoc networks

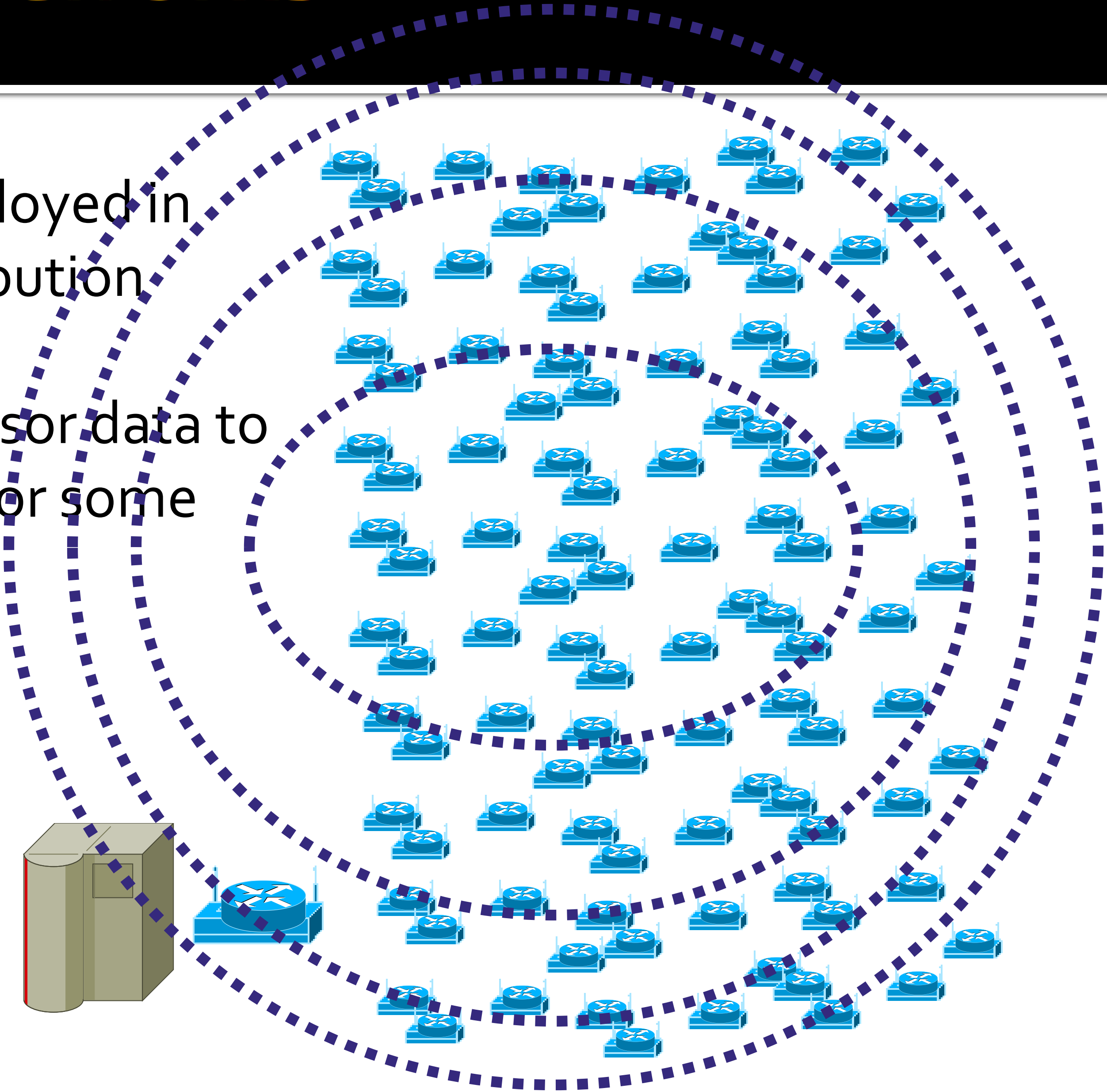
- Mobile Ad hoc NET work (MANET) is a self configuring network of mobile routers (and associated hosts)
- connected by wireless links – the union of which forms an arbitrary topology

Examples of such networks

- Sensor networks
- Military applications

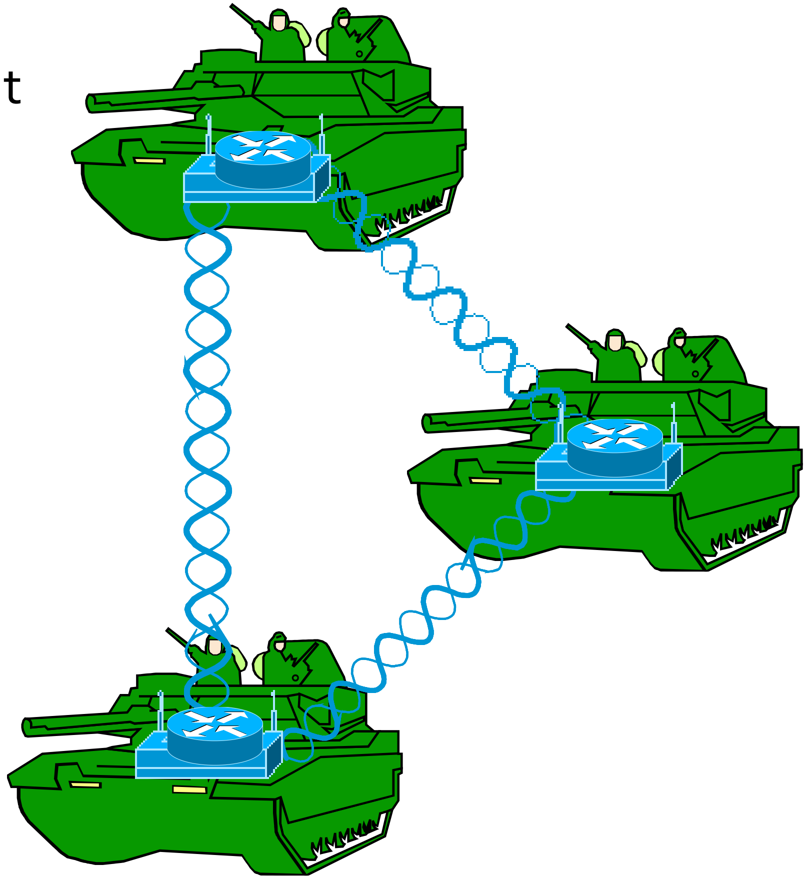
Sensor networks

- Networks deployed in random distribution
- Low power
- Delivering sensor data to a central site for some purpose



Military applications

- Combat regiment in the field
  - Perhaps 4000-8000 objects in constant unpredictable motion…
- Intercommunication of forces
  - Proximity, function, plan of battle
- Special issues
  - Low probability of detection
  - Random association and topology



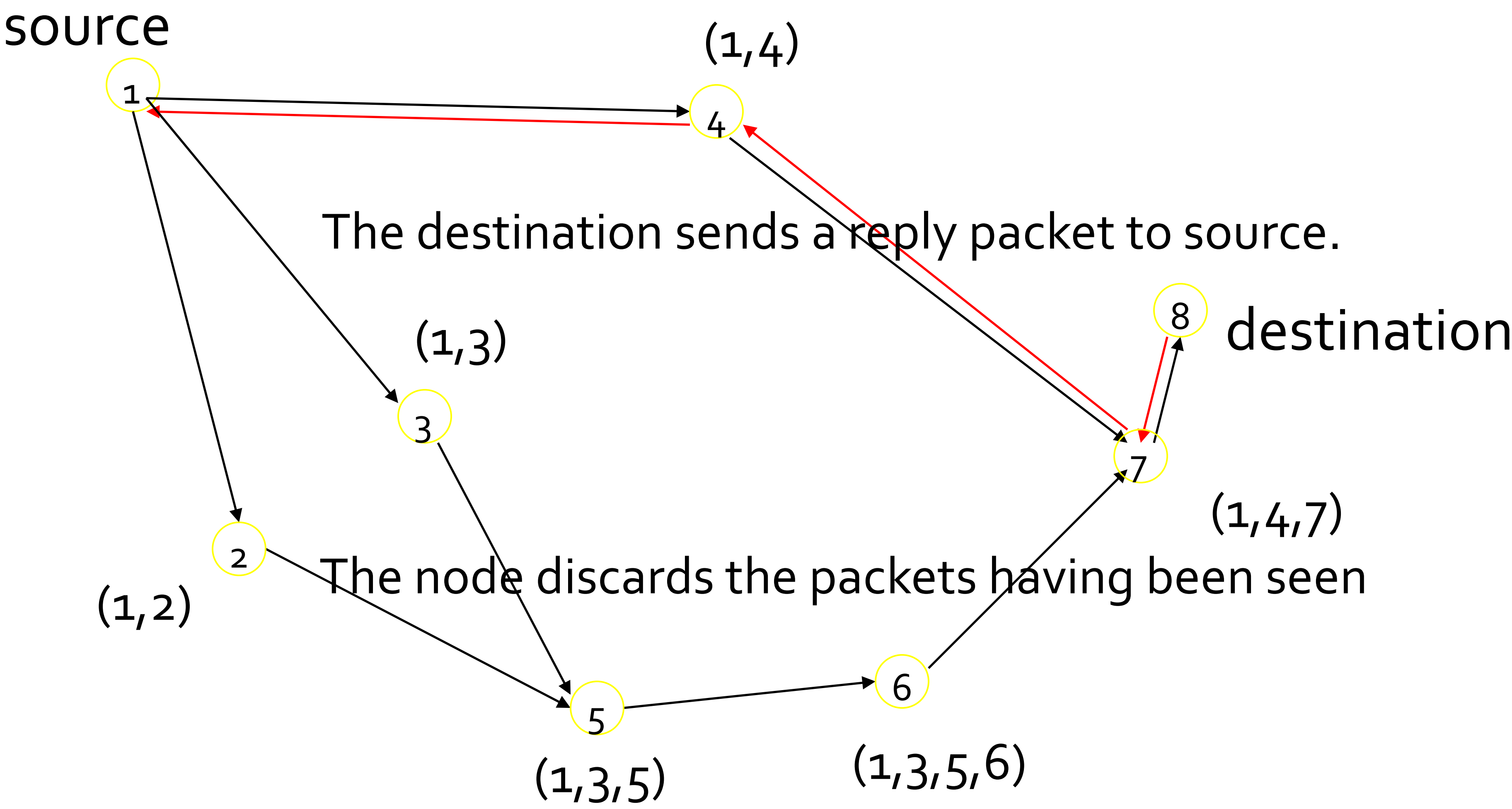
Dynamic source routing

- DSR is designed for MANETs
- DSR doesn’t need any network infrastructures
  - Loop free routing
  - No routing information in the intermediate nodes
- Nodes may easily cache this routing information for future use

DSR protocol activities

- Route discovery
  - Undertaken when source needs a route to a destination
- Route maintenance
  - Used when link breaks, rendering specified path unusable

source broadcasts a packet containing address of source and destination



The destination sends a reply packet to source.

The node discards the packets having been seen

The route looks up its route caches to look for a route to destination
If not find, appends its address into the packet

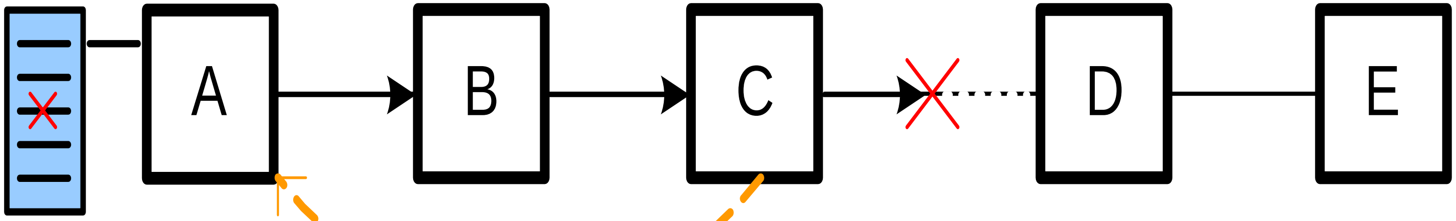
How to send a reply packet

- If the destination has a route to the source in its route cache, use it
- Else if symmetric links are supported, use the reverse of route record
- Else if symmetric links are not supported, the destination initiates route discovery to source

Route Maintenance

- Whenever a node transmits a data packet, a route reply, or a route error, it must verify that the next hop correctly receives the packet.
- If not, the node must send a route error to the node responsible for generating this route header
  - Intermediate nodes “eavesdrop”, adjust cached routes
- Source deletes route; tries another if one cached, or The source restart the route discovery

Route Maintenance……



Route error message: C-D is broken

http://ashrafsau.blogspot.in/

Disadvantages

- Packet header size grows with route length due to source routing.
- Flood route request may potentially reach all nodes in the network.
- Route reply storm problem.

AODV Overview

- AODV is a packet routing protocol designed for use in mobile ad hoc networks (MANET)
- Intended for networks that may contain thousands of nodes
- *Source, destination* and *next hop* are addressed using *IP addressing*
- Each node maintains a *routing table* that contains information about reaching destination nodes.

Main Features of the AODV Protocol

- The Ad hoc On-Demand Distance Vector protocol is both an on-demand and a table-driven protocol.

- The packet size in AODV is uniform unlike DSR. Unlike DSDV, there is no need for system-wide broadcasts due to local changes.

- AODV supports multicasting and unicasting within a uniform framework.

Main Features of the AODV Protocol (II)

- Each route has a lifetime after which the route expires if it is not used.

- A route is maintained only when it is used and hence old and expired routes are never used.

- Unlike DSR, AODV maintains only one route between a source-destination pair.

Routing Table Fields

- Destination IP address
- Destination Sequence Number
- Valid Destination Sequence Number Flag
- Other state and routing flags
- Network Interface
- Hop Count (needed to reach destination)
- Next Hop
- Lifetime (route expiration or deletion time)

Lifetime of a Route-Table Entry

- A lifetime is associated with the entry in the route table.

- This is an important feature of AODV. If a route entry is not used within the specified lifetime, it is deleted.

- A route is maintained only when it is used. A route that is unused for a long time is assumed to be stale.

Overview

- Routing table size is minimized by only including next hop information, not the entire route to a destination node.
- Sequence numbers for both destination and source are used.
- Managing the sequence number is the key to efficient routing and route maintenance

Overview

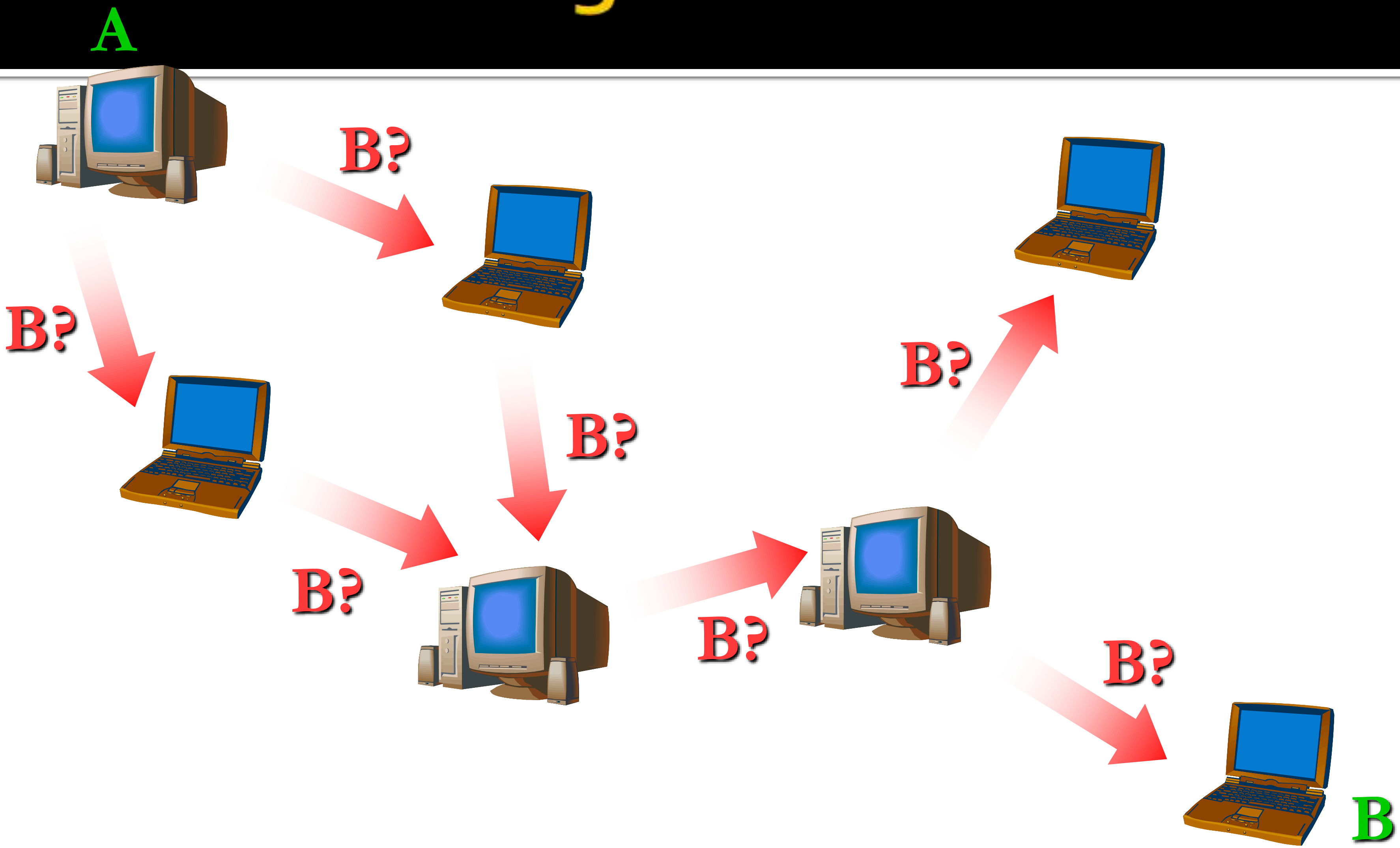
- The basic message set consists of:
    - RREQ – Route request
    - RREP – Route reply
    - RERR – Route error
    - HELLO – For link status monitoring

Messages

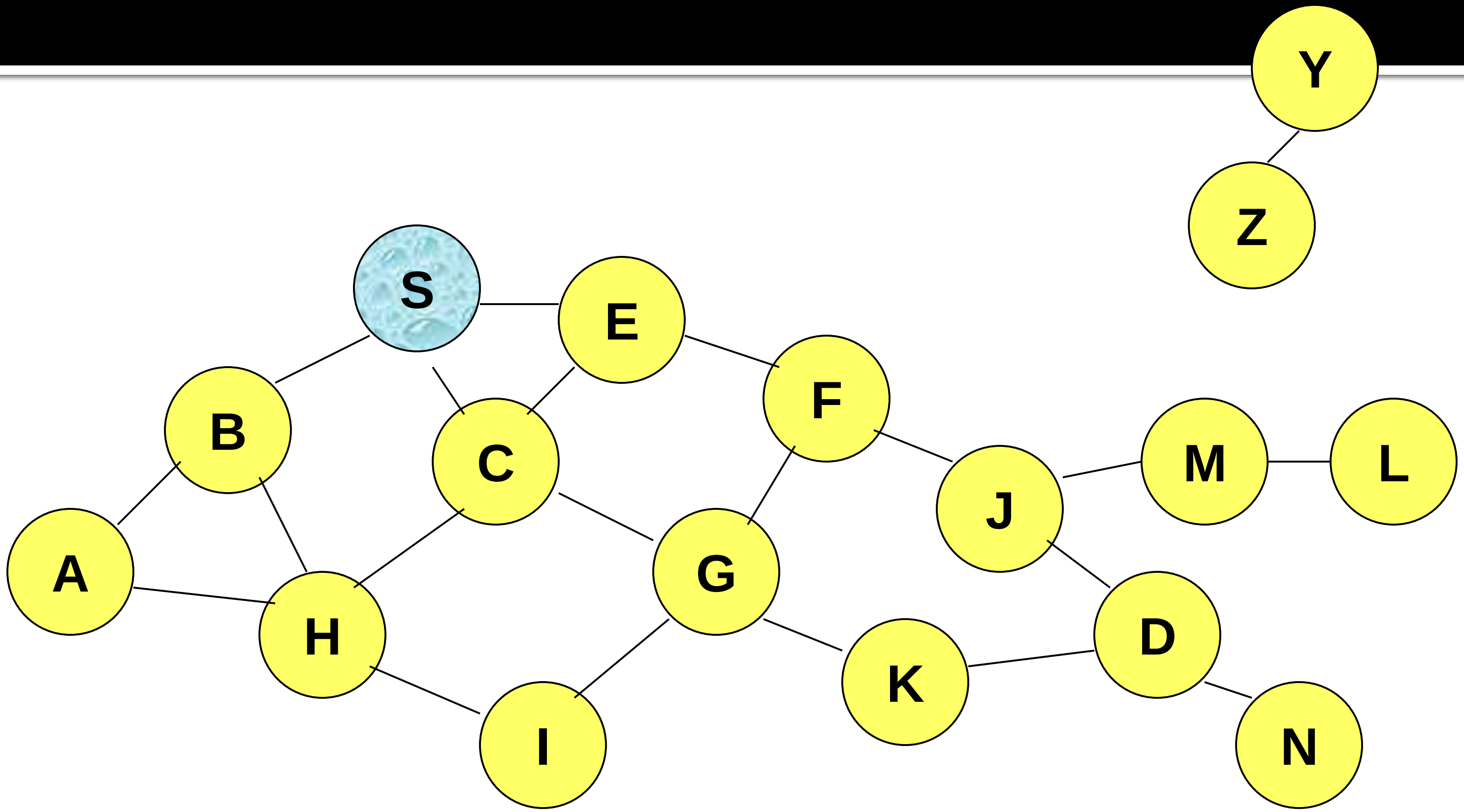
- Route Request: “I need a route”
- Route Response: “Route advertisement”
- Route Error: “Withdraw route”

- Periodic route response to neighbors acts as “hello”, installing and refreshing route

RREQ Message



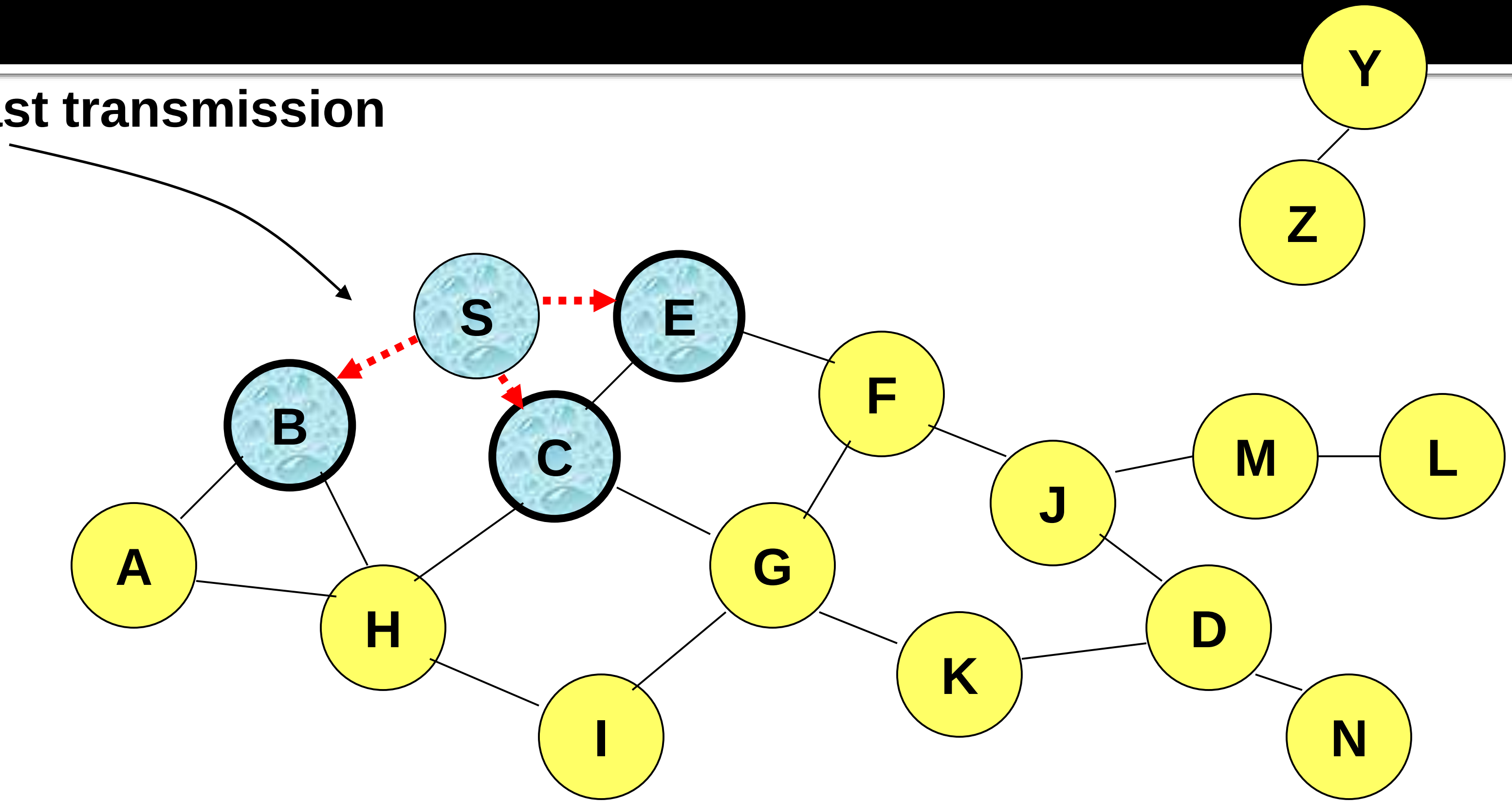
Route Requests in AODV



● Represents a node that has received RREQ for D from S

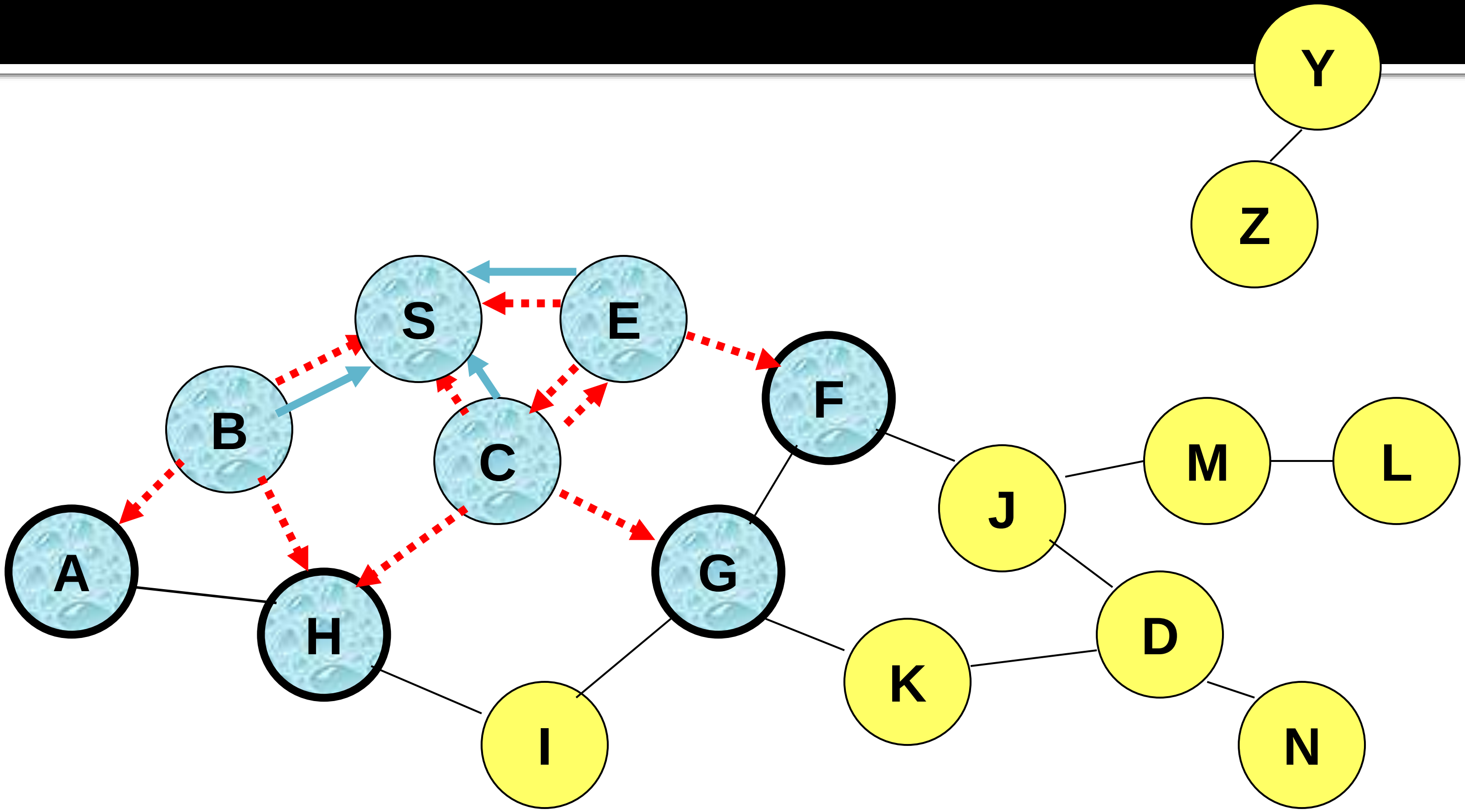
Route Requests in AODV

Broadcast transmission



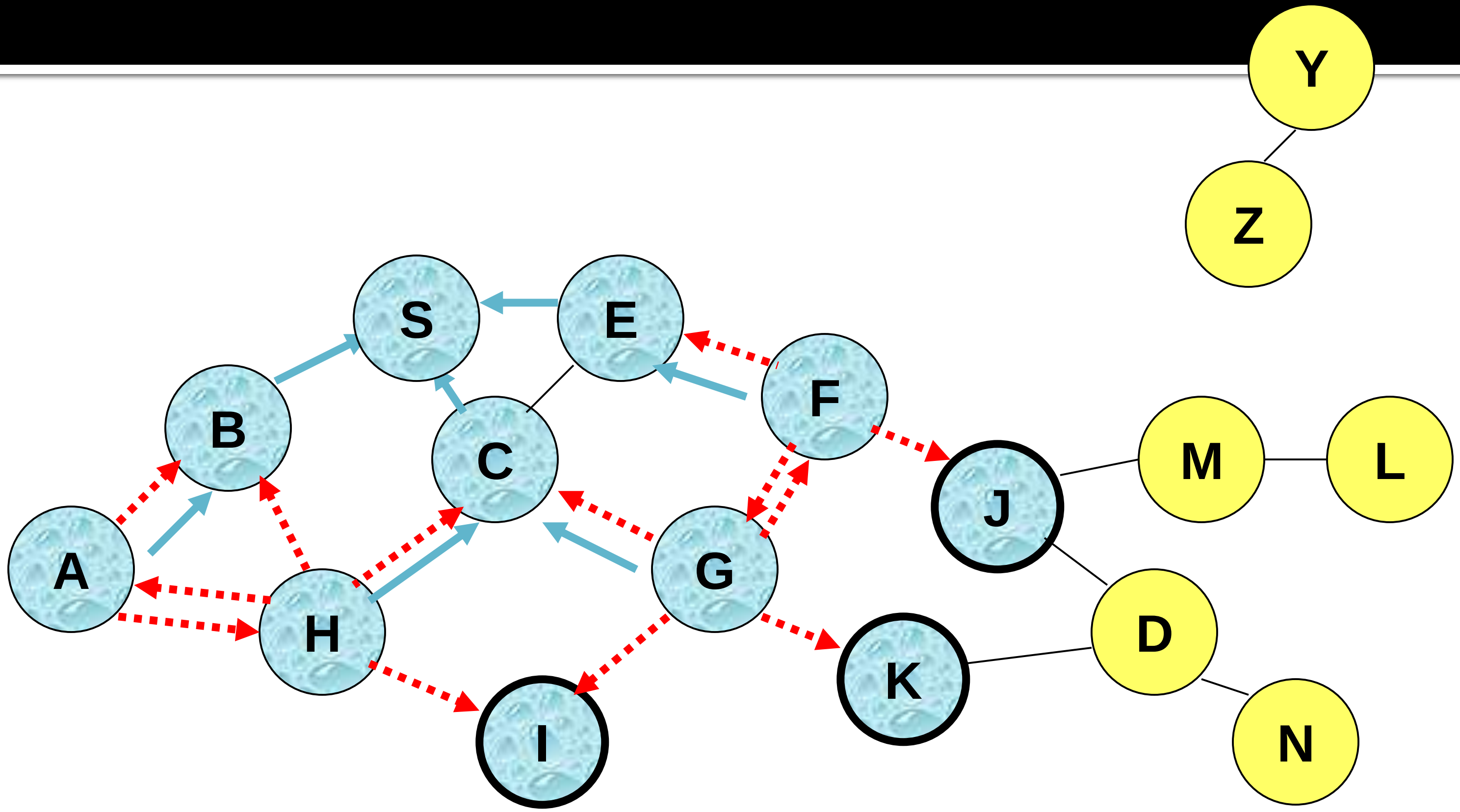
⇢ Represents transmission of RREQ

Route Requests in AODV



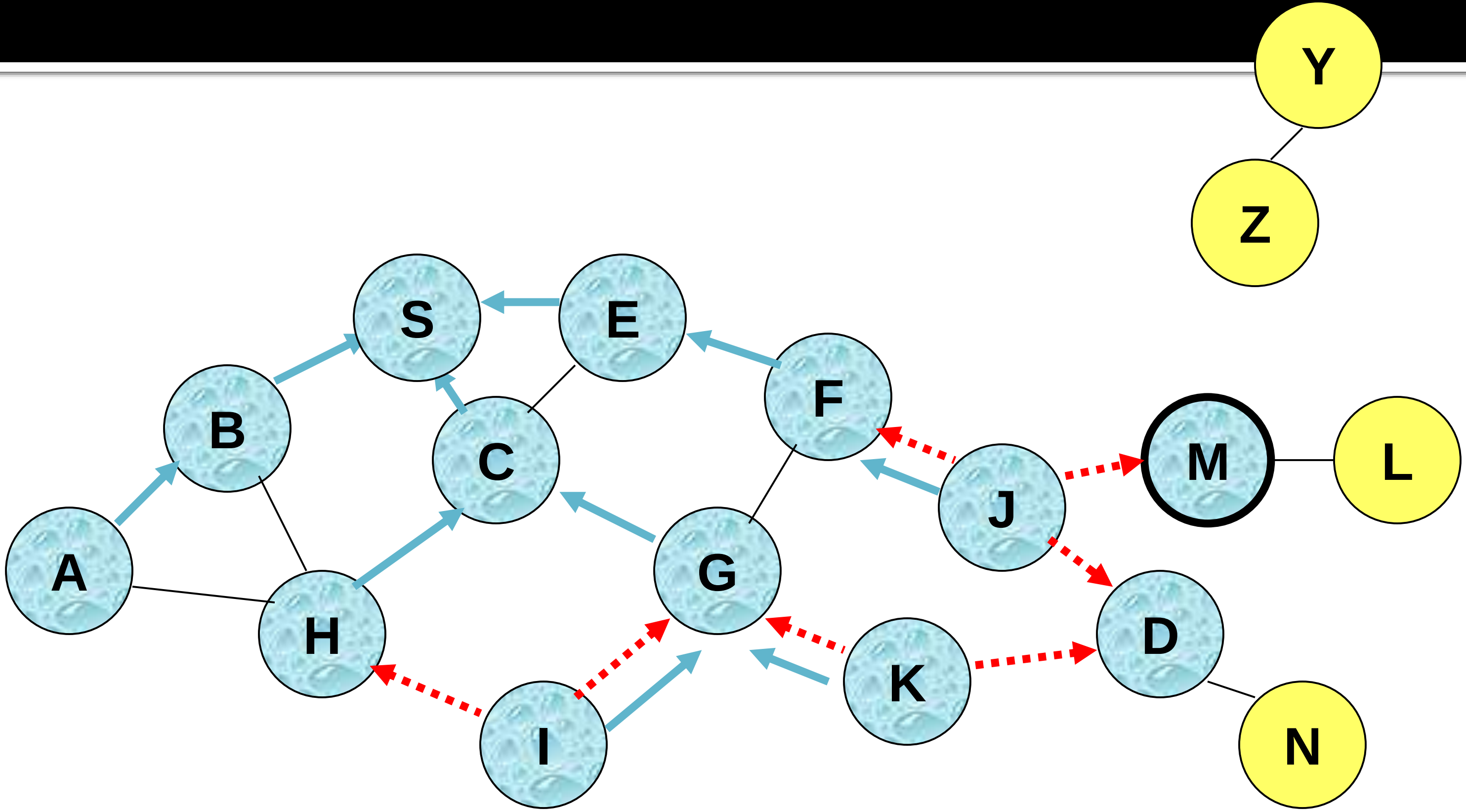
Represents links on Reverse Path

Reverse Path Setup in AODV

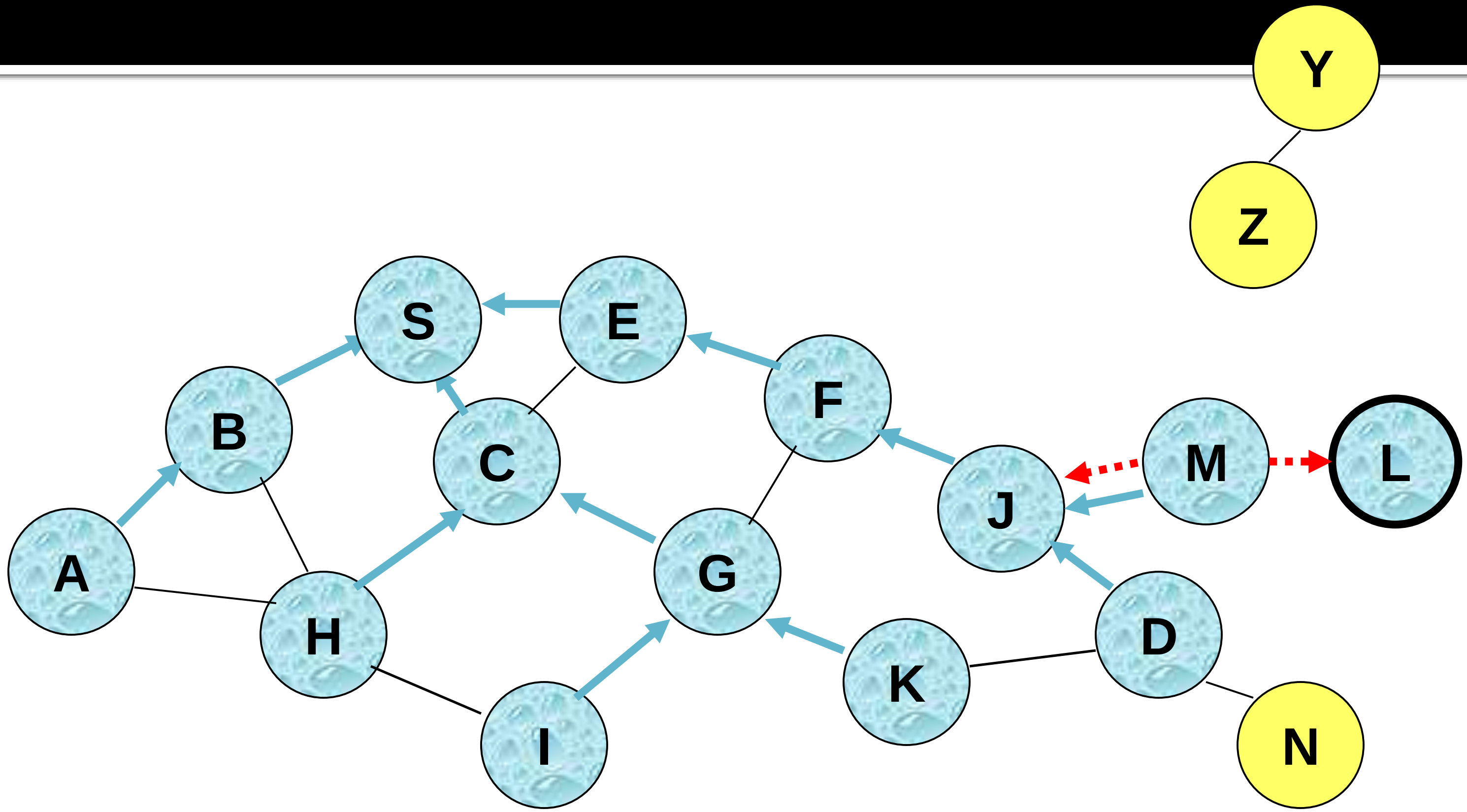


- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

Reverse Path Setup in AODV

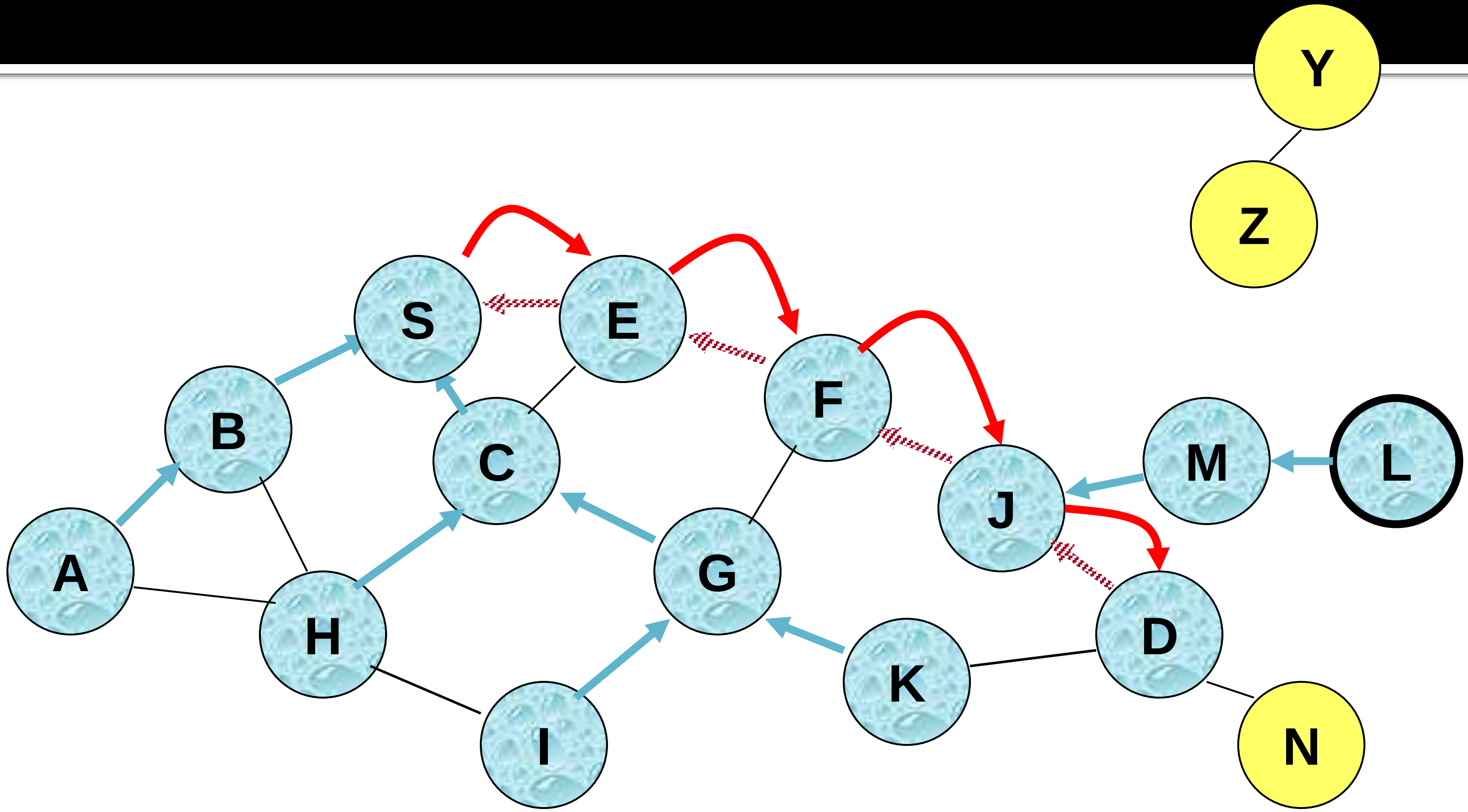


Reverse Path Setup in AODV



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

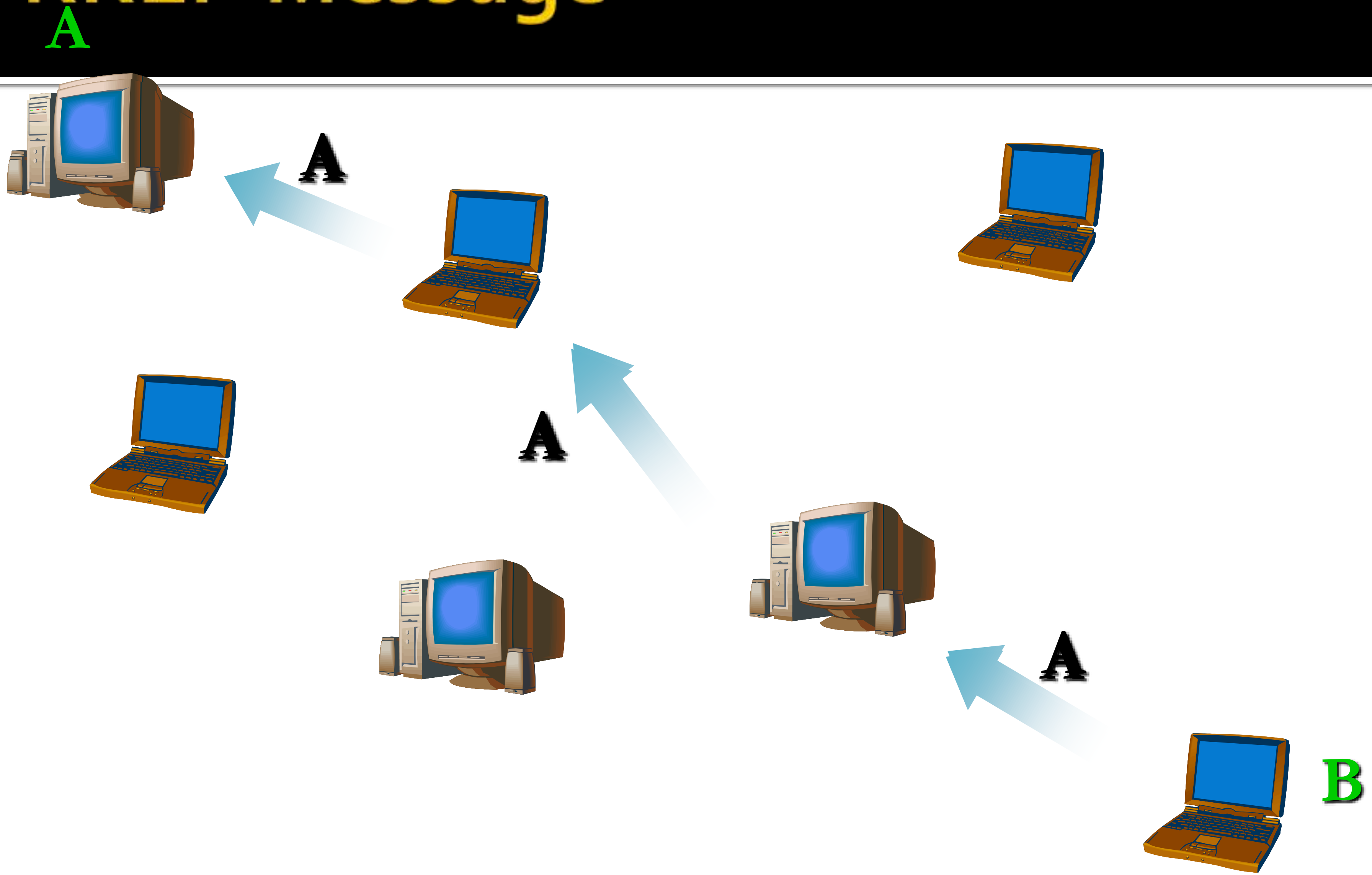
Forward Path Setup in AODV



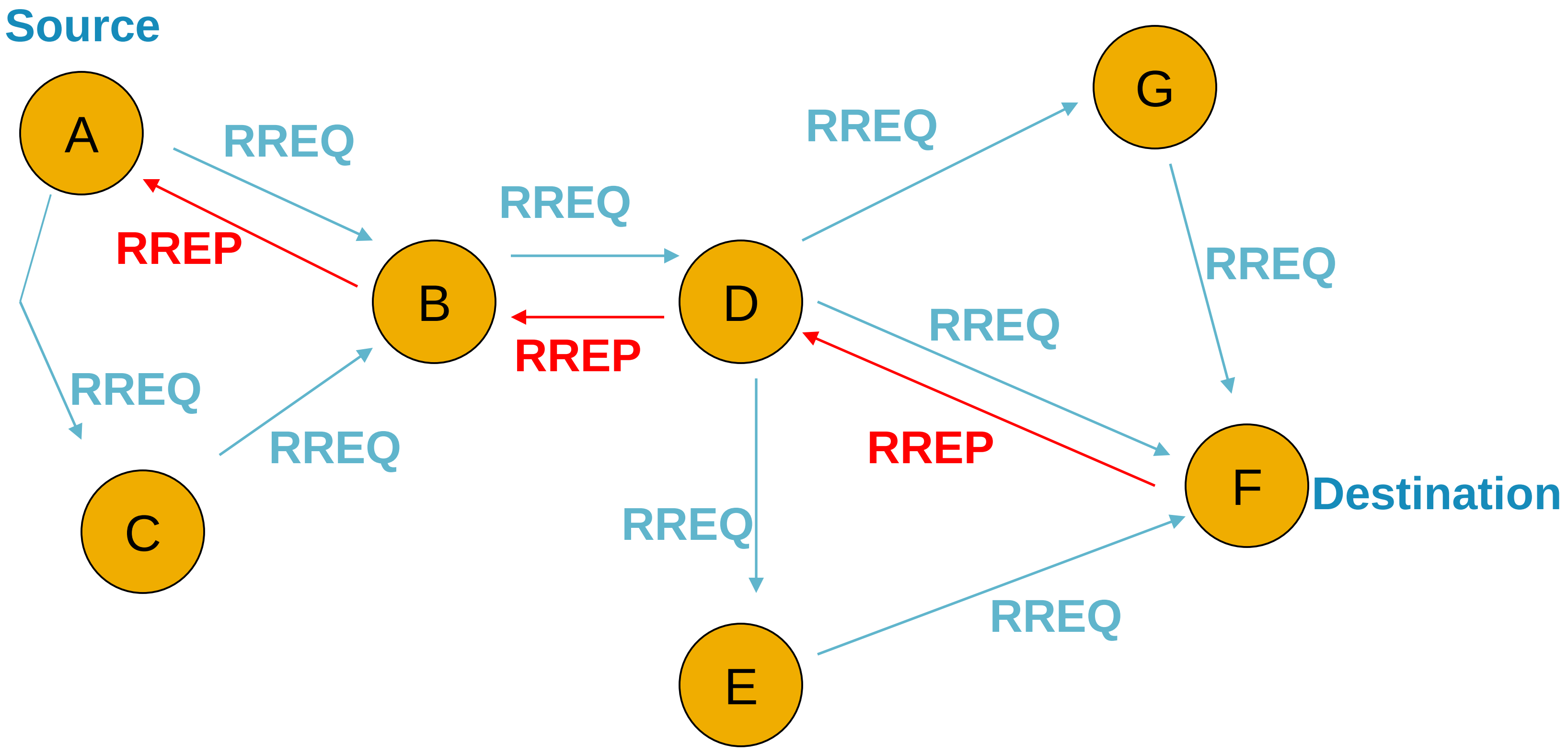
⇠ Forward links are setup when RREP travels along the reverse path

⤻ Represents a link on the forward path

RREP Message



Message routing

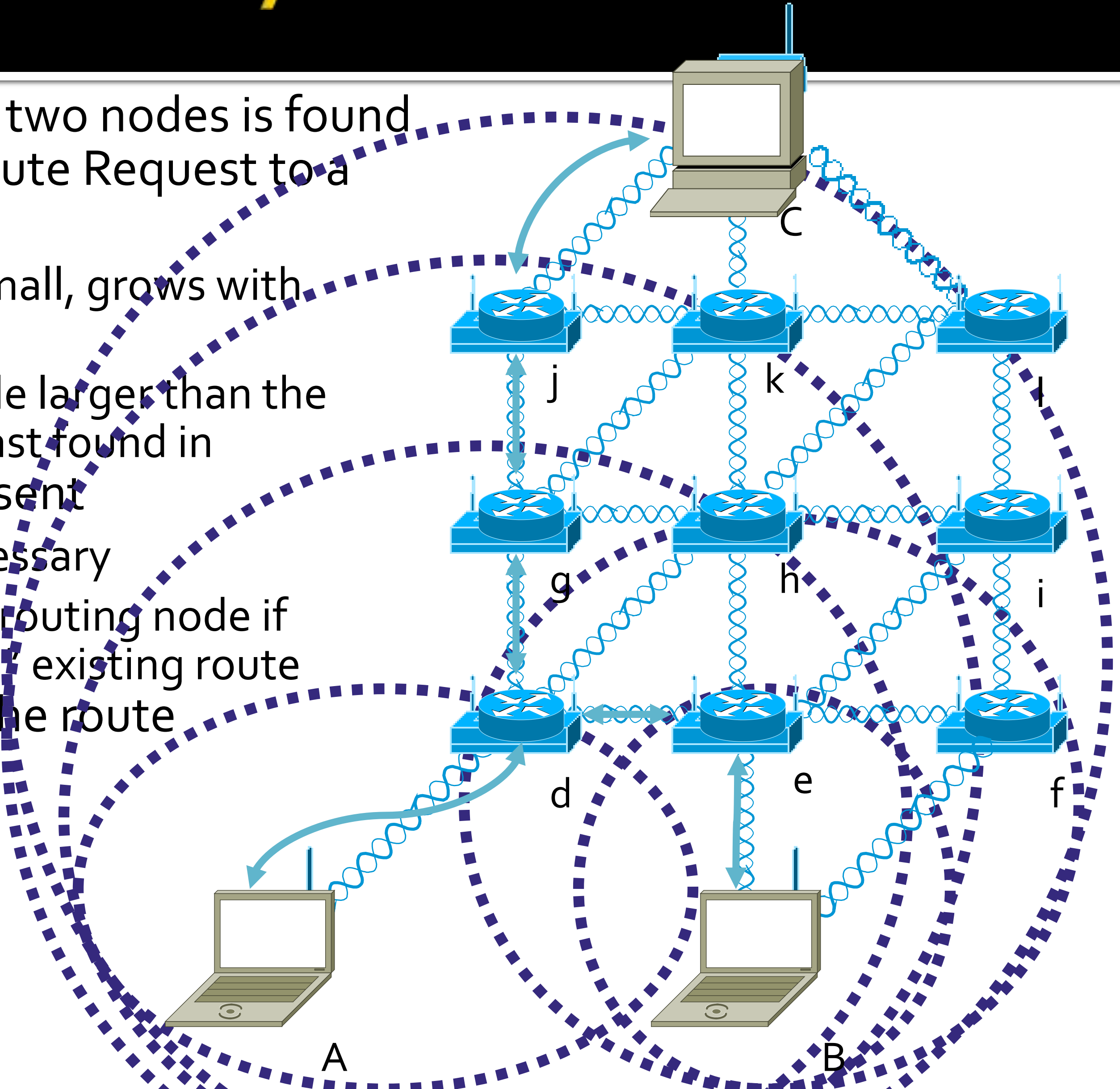


Discovery

- Broadcast RREQ messages.
- Intermediate nodes update their routing table
- Forward the RREQ if it is not the destination.
- Maintain back-pointer to the originator.
- Destination generates RREQ message.
- RREQ sent back to source using the reverse pointer set up by the intermediate nodes.
- RREQ reaches destination, communication starts.

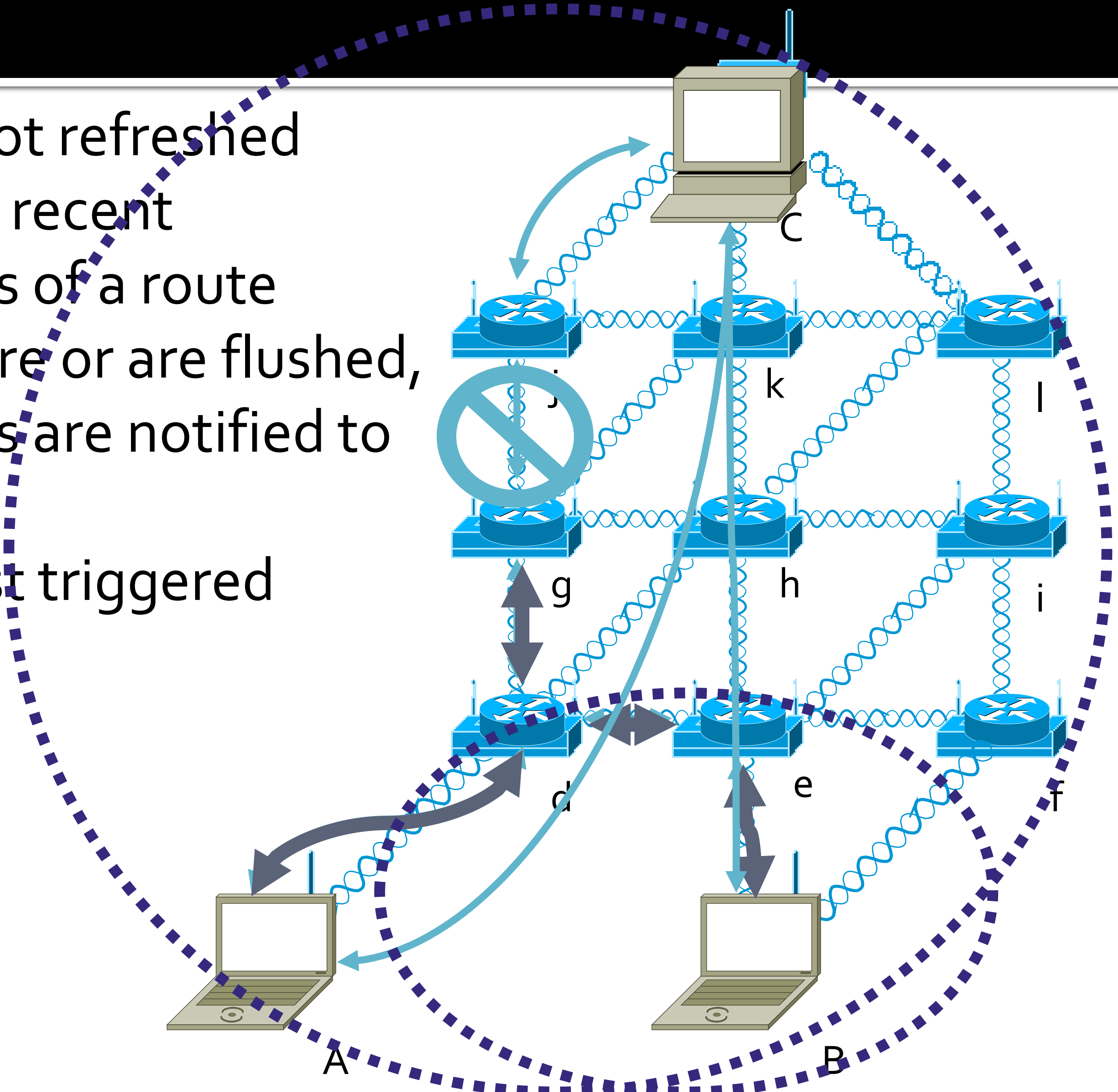
Route Discovery

- A route between two nodes is found by sending an Route Request to a locality
  - Initial locality small, grows with failure
  - After that, a little larger than the locality target last found in
- Route Response sent
  - By target if necessary
  - By neighboring routing node if possible to "join" existing route
- Network stores the route



Route Errors

- Routes expire if not refreshed
- routing nodes log recent downstream users of a route
- When routes expire or are flushed, downstream users are notified to flush
- New route request triggered



AODV Routing

- There are two phases
  - Route Discovery.
  - Route Maintenance.
- Each node maintains a routing table with knowledge about the network.

- AODV deals with route table management.
- Route information maintained even for short lived routes – reverse pointers.

Maintenance

- Hello messages broadcast by *active* nodes periodically HELLO_INTERVAL.
- No hello message from a neighbor in DELETE_PERIOD,link failure identified.
- A local route repair to that next hop initiated.
- After a timeout ,error propagated both to originator and destination.
- Entries based on the node invalidated.

Congestion Handling

- One method that AODV handle congestion is:
  - If the source node receives no RREP from the destination, it may broadcast another RREQ, up to a maximum of RREQ_RETRIES.
  - For each additional attempt that a source node tried to broadcast RREQ, the waiting time for the RREP is multiplied by 2.
- DSR is not capable of handling congestion.

Congestion Handling

- Other possible methods to improve AODV congestion handling:
  - A route may predict when congestion is about to occur and try to avoid it by reduce the transmission rate.
  - Schedule the requests so that it will not overload the network.

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

Security Attacks in AODV

1. Black hole attack
2. Message tampering attack
3. Message dropping attack

AODV: Summary

- Routes need not be included in packet headers
- Nodes maintain routing tables containing entries only for routes that are in active use
- At most one next-hop per destination maintained at each node
  - DSR may maintain several routes for a single destination
- Sequence numbers are used to avoid old/broken routes
- Sequence numbers prevent formation of routing loops
- Unused routes expire even if topology does not change

DSR vs AODV

I. Packet header overhead
II. Route learning capability
III. Handling multiple route replies
IV. Scalability
V. Security

Thank you!