THE CONCEPT OF FLOODING

How well does it work in a wireless network?

26

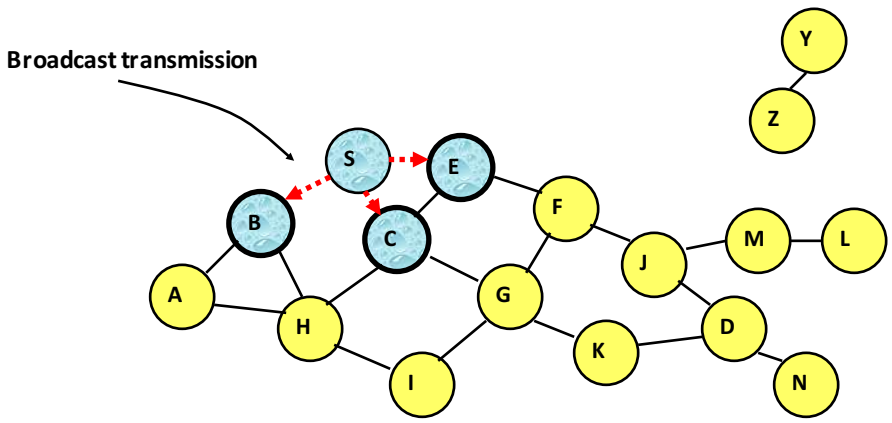
Data Delivery Using Flooding

- Sender S broadcasts data packet P to all its neighbors
- Each node receiving P forwards P to its neighbors
  - Sequence numbers used to avoid the possibility of forwarding the same packet more than once
- Packet P reaches destination D provided that D is reachable from sender S
- Node D does not forward the packet

What can go wrong?

27

Flooding Example

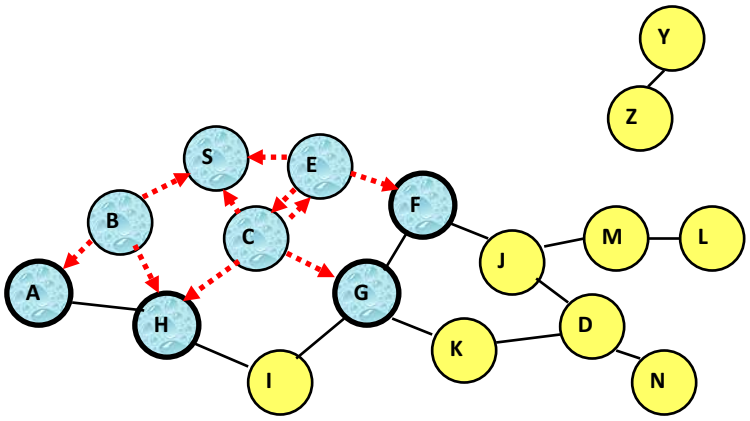


Represents a node that receives packet P for the first time

Represents transmission of packet P

28

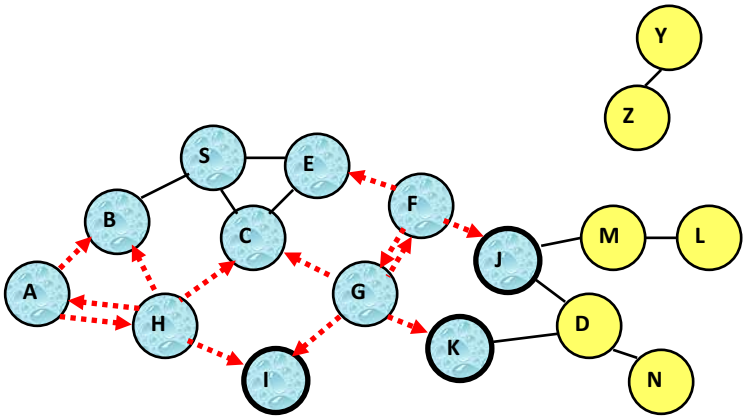
Flooding Example



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

29

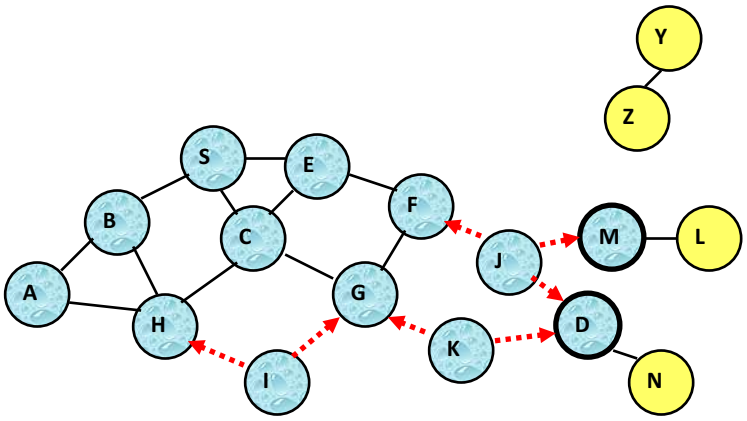
Flooding Example



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

30

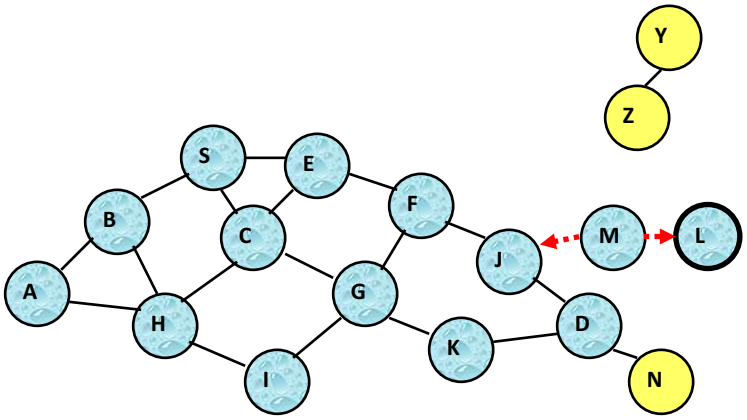
Flooding Example



- Nodes J and K both broadcast packet P to node D
- Since nodes J and K are hidden from each other, their transmissions may collide
  => Packet P may not be delivered to node D at all, despite the use of flooding

31

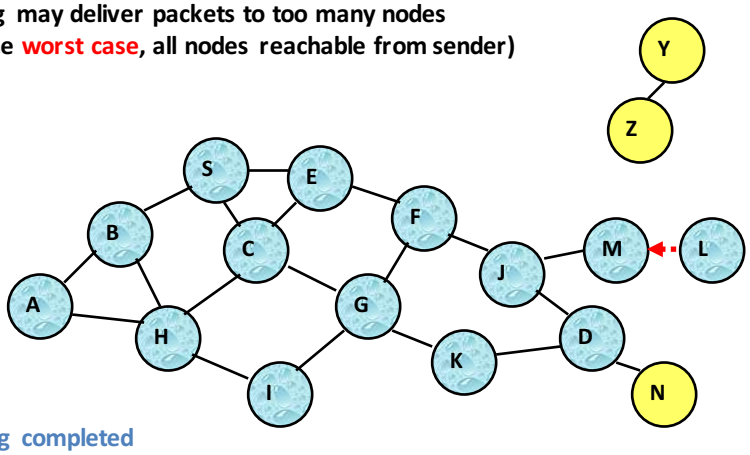
Flooding Example



- Node D does not forward packet P,
  because node D is the intended destination of packet P

Flooding Example

- Flooding may deliver packets to too many nodes
  (in the worst case, all nodes reachable from sender)



- Flooding completed
- Nodes unreachable from S do not receive packet P (e.g., node Z)
- Nodes for which all paths from S go through the destination D
  also do not receive packet P (example: node N)

Flooding for Data Delivery

- Advantages:
  - Simplicity
  - May be more efficient if infrequent communication
    - Route setup / maintenance not worth it
    - Especially, when changing topology / mobility
  - Potentially higher robustness to path failure
    - Because of multi-path redundancy
- Disadvantages:
  - Potentially, very high overhead
    - Packets delivered to too many nodes who don't need them
  - Potentially lower reliability of data delivery
    - Reliable broadcast is difficult
    - Hidden terminal because no channel reservation

34

Flooding as a Building Block

- Many protocols perform (potentially *limited*) flooding of control packets, instead of data packets
  - The control packets are used to discover routes
  - Discovered routes are subsequently used to send data packet(s)
- Overhead of control packet flooding is amortized over data packets transmitted between consecutive control packet floods

35

DYNAMIC SOURCE ROUTING (DSR)

(Johnson 96)

A Reactive Protocol

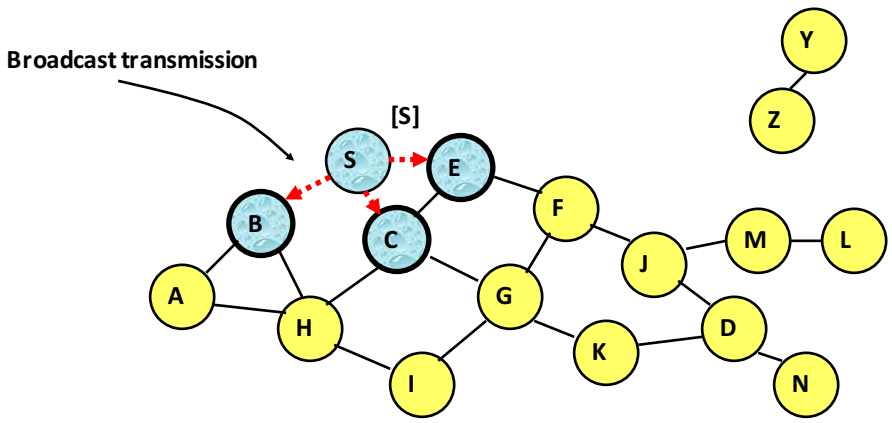
36

Route Discovery in DSR

- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a "route discovery"
- Route Discovery:
  - Source node S floods Route Request (RREQ)
  - Each node appends own identifier when forwarding RREQ

37

Route Discovery in DSR



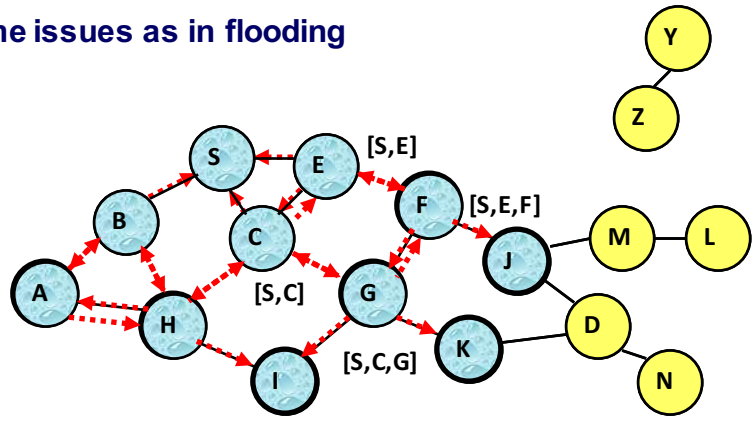
Represents transmission of RREQ

[X,Y] Represents list of identifiers appended to RREQ

38

Route Discovery in DSR

- Same issues as in flooding

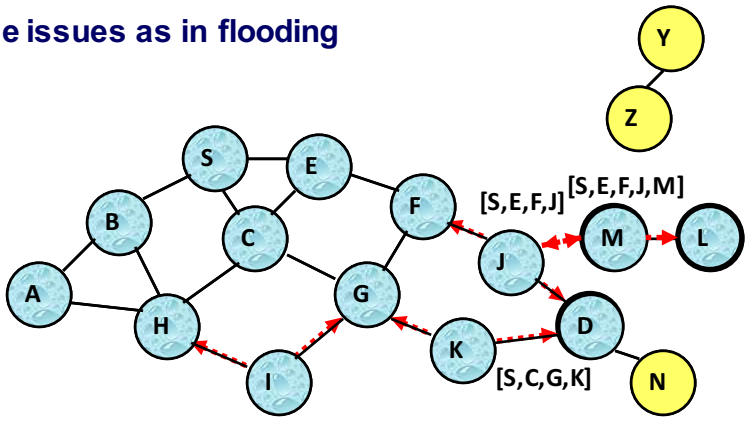


- Node H receives packet RREQ from two neighbors: potential for collision
- Node C receives RREQ from G and H, but does not forward it again
  - Because node C has already forwarded RREQ once

39

Route Discovery in DSR

- Same issues as in flooding



- Nodes J and K both broadcast RREQ to node D
  - Since J and K are hidden from each other, their transmissions may collide
- Node D does not forward RREQ
  - Because it is the intended target of route discovery

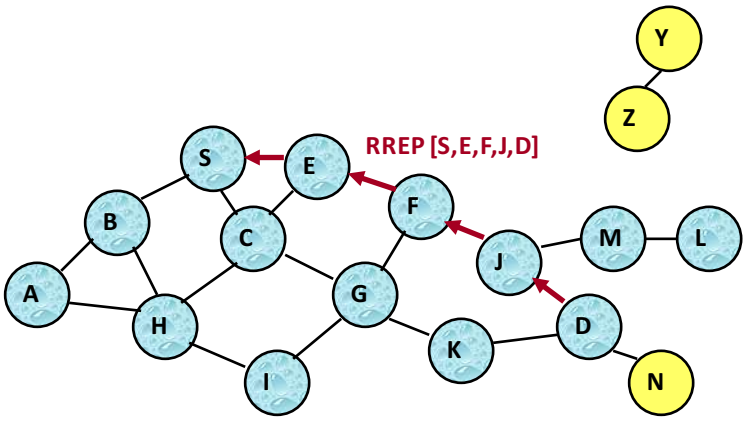
40

Route Discovery: Route Reply

- Route Reply:
  - Destination D on receiving the first RREQ
    - Sends a Route Reply (RREP)
  - RREP is sent on a route obtained by reversing the route appended to received RREQ
    - RREP includes the route from S to D on which RREQ was received by node D
- Route reversal => links need to be bi-directional
  - If unidirectional (asymmetric) links are allowed
    - Then RREP may need a route discovery for S from node D
  - 802.11 links always bi-directional (since ACK is used)

41

Route Reply in DSR



Represents RREP control message

42

Data Delivery in 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
  - Packet header grows with route length
- Intermediate nodes use the source route in packet
  - To determine to whom a packet should be forwarded

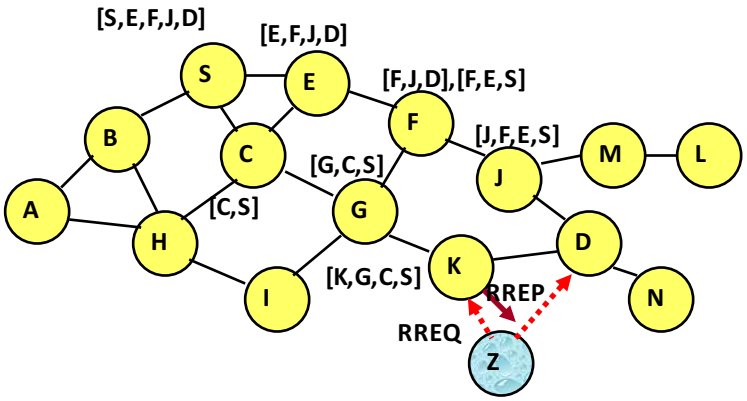
43

DSR Optimization: Route Caching

- 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 D,
  - 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 by overhearing Data packets

44

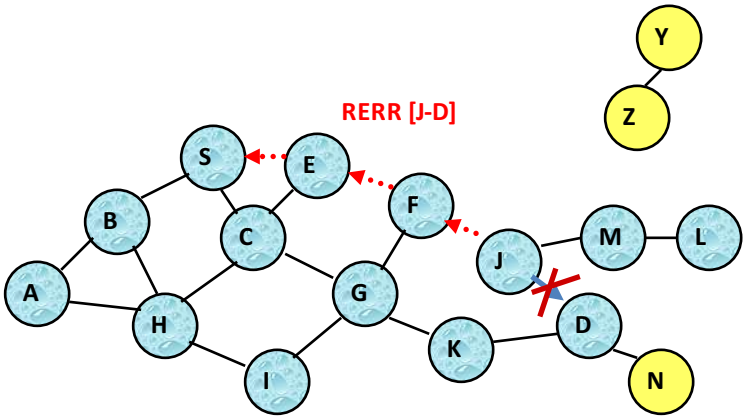
Route Caching: Speed up Discovery



When node Z sends a route request for node C,
node K sends back a route reply [Z,K,G,C] to node Z using its local cache

45

Route Error (RERR)



J sends a route error to S along route J-F-E-S when its attempt to forward the data packet S (with route SEFJD) on J-D fails

Nodes hearing RERR update their route cache to remove link J-D

46

Route Caching: Beware!

- With passage of time and host mobility, cached routes may become invalid
- Stale caches can adversely affect performance
  - Local caching by other nodes may result in stale routes
    - Even on multiple tries by sender host
  - May require several trials before finding a good route

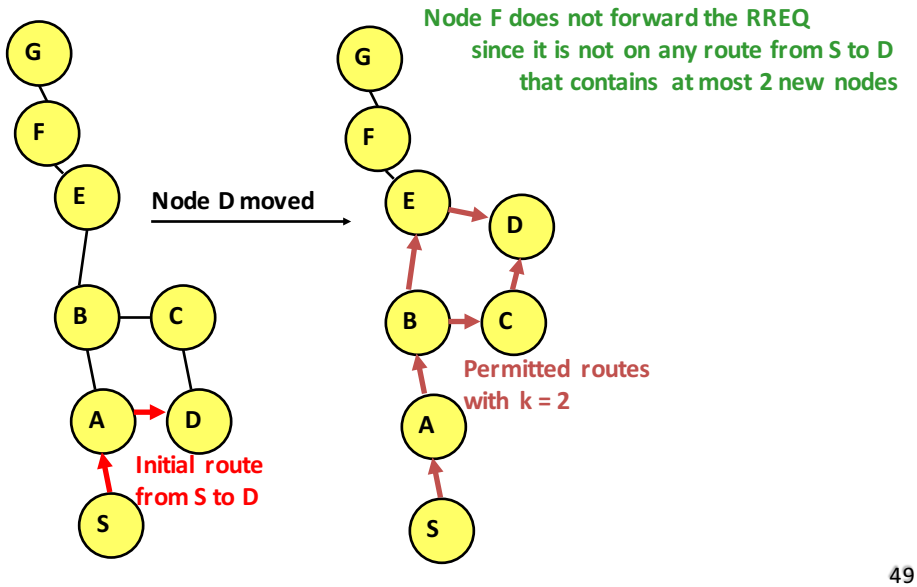
47

Query Localization

- Path locality heuristic:
  - Look for a new path that contains at most *k* nodes that were *not* present in the previously known route
- Old route is piggybacked on a Route Request
- Route Request is forwarded only if:
  - Accumulated route in the RREQ contains *at most k* new nodes that were absent in the old route
- ☺: Limits propagation of the route request

48

Query Localization: Example



49

DSR: Advantages

- Routes maintained reactively
  - Reduces overhead of maintenance
- Route caching can reduce route discovery overhead
- Discovery of multiple routes at D

50

DSR: Disadvantages

- Packet header size grows with route length
- Flood of RREQs may potentially reach all nodes
- Care must be taken to avoid collisions between route requests propagated by neighboring nodes
  - Insertion of random delays before forwarding RREQ
- Increased contention if too many RREPs come back
  - Due to nodes replying using their local cache
  - Route Reply *Storm* problem
    - May be eased by preventing a node from sending RREP
      - If it hears another RREP with a shorter route
- An intermediate node may RREP using a stale cache
  - Thus polluting other caches
  - Can be eased by purging invalid cached routes [Hu00]

51

AD-HOC ON-DEMAND DISTANCE VECTOR ROUTING

(Perkins 99)

Distance Vector Derivative

52

AODV Routing: Intro

- DSR includes source routes in packet headers
  - Resulting large headers can degrade performance
    - Particularly when data contents of a packet are small
- AODV attempts to improve on DSR
  - By maintaining routing tables at the nodes
  - Data packets do not contain long routes
- AODV is also reactive

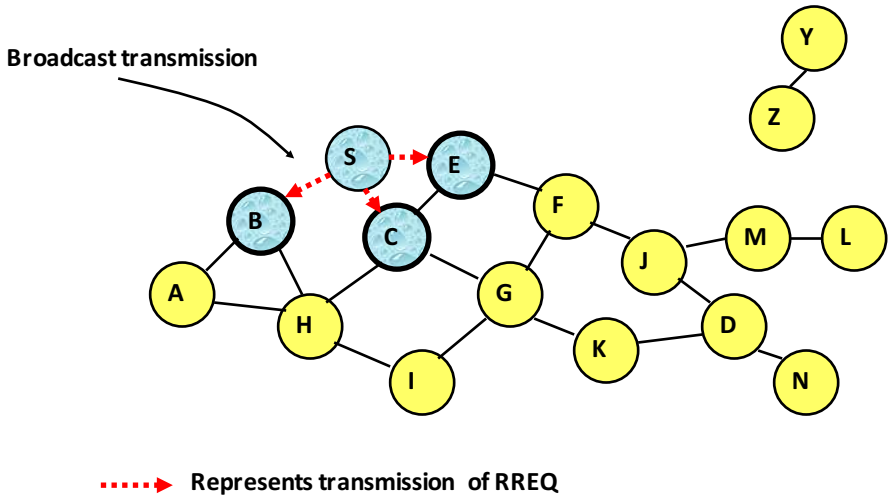
53

AODV: Basic Operation

- Route Requests (RREQ) forwarded like DSR
- When intermediate node re-broadcasts RREQ
  - It sets up a reverse path pointing towards previous node
  - AODV assumes symmetric (bi-directional) links
- Destination replies by sending a Route Reply
- Intermediate nodes forward RREP up the reverse path
  - They also remember the downstream path in local cache

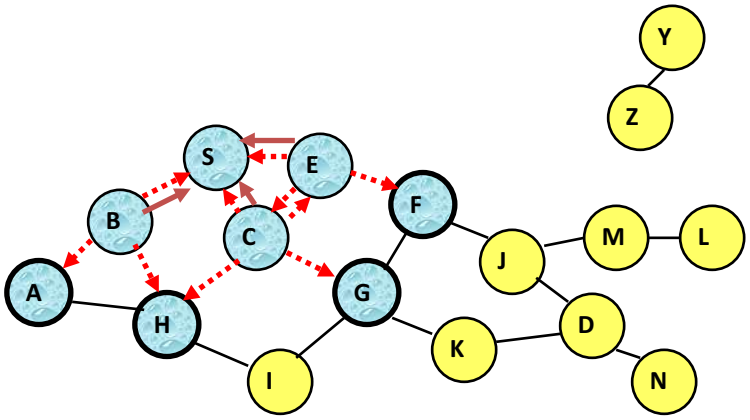
54

Route Requests in AODV



55

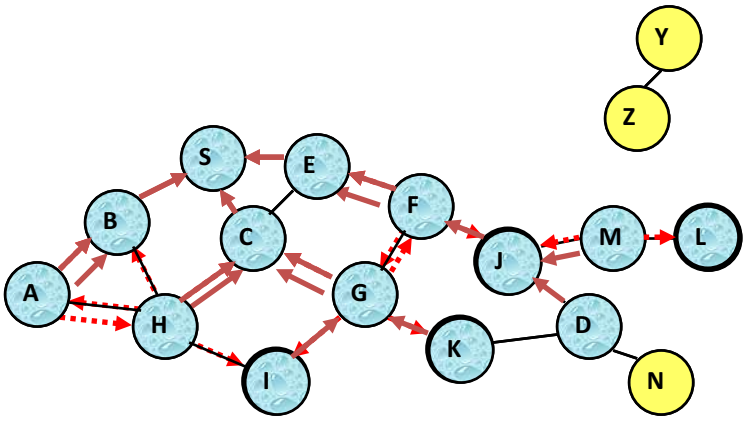
Route Requests in AODV



Represents links on Reverse Path

56

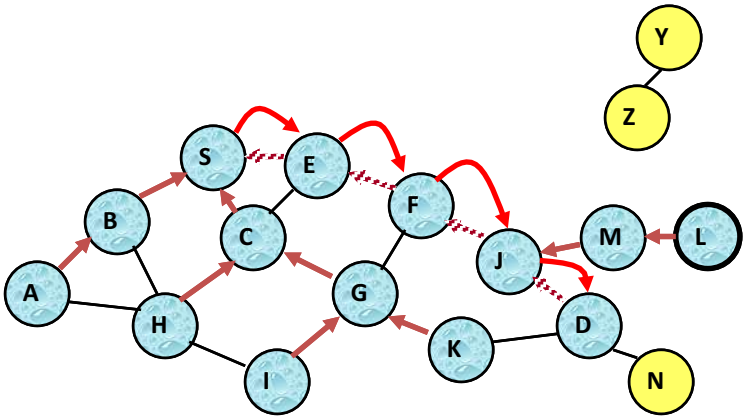
Reverse Path Setup in AODV



- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once
- Node D does not forward RREQ, because it is the intended target of the RREQ

57

Route Reply in AODV



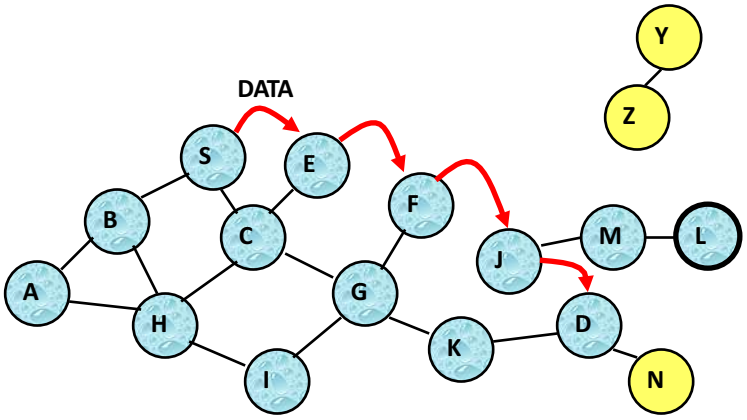
Represents links on path taken by RREP

Forward links are setup when RREP travels along the reverse path

Represents a link on the forward path

58

Data Delivery in AODV



Routing table entries used to forward data packet.

Route is *not* included in packet header.

59

Route Reply in AODV

- An intermediate node may also send a RREP
  - If it knows a more recent path than the one previously known to sender S
- To determine whether the intermediate node's path is more recent
  - *Destination sequence numbers* are used
- The likelihood that an intermediate node will send a RREP when using AODV not as high as DSR
  - A new RREQ by node S for a destination is assigned a higher destination sequence number
    - An intermediate node which knows a route, but with a smaller sequence number, cannot send RREP

60

Timeouts

- A routing table entry maintaining a reverse path is purged after a timeout interval
  - Timeout should be enough to allow RREP to come back
- A routing table entry maintaining a forward path is purged if *not used* for a *active_route_timeout* interval
  - If no is data being sent, routing entry will be deleted
    - Even if the route may actually still be valid
- Link Failure Reporting
  - Neighbor X is considered "active for a routing table entry" if it sent a packet, within *active_route_timeout*, which was forwarded using that entry
    - When the next hop link in a routing table entry breaks, all corresponding active neighbors are informed (using RREQ)

61

Route Error

- When X is unable to forward a packet (from S to D) on link (X,Y), it generates an RERR message
  - X increments the cached destination seq number for D
  - The incremented seq 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 > *N*
- When node D receives the RREQ with destination sequence number N,
  - D will set its seq number to N, unless it is already larger

62

Link Failure Detection

- *Hello* messages:
  - Neighboring nodes periodically exchange hello message
  - Absence of hello message is used as an indication of link failure
- Alternatively, failure to receive several MAC-level acknowledgement may be used as an indication of link failure

63

Summary: AODV

- Routes need not be included in packet headers
- Nodes maintain routing tables – contain 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
- Unused routes expire even if topology does not change

64