EEC173B/ECS152C, Winter 2006

MANET Unicast Routing

- Reactive Protocol
  - Flooding
  - DSR
  - LAR
  - AODV

Acknowledgment: Selected slides from Prof. Nitin Vaidya

Flooding of Control Packets

- How to reduce the scope of the route request flood ?
  - LAR
    - [KV98] J. Ko and N. Vaidya, "Location-Aided Routing (LAR) Mobile Ad Hoc networks," *ACM Mobicom*, 1998.
  - Query localization
    - [CD99] R. Castaneda and S. Das, "Query Localization Techniques for On-demand Routing Protocols in Ad Hoc Networks," *ACM Mobicom*, 1999.
- How to reduce redundant broadcasts ?
  - The Broadcast Storm Problem
    - [NTC+99] S. Ni, Y. Tseng, Y. Chen, and J. Sheu, "The Broadcast Storm Problem in a Mobile Ad Hoc Network," *ACM Mobicom*, 1999.

Location-Aided Routing (LAR)

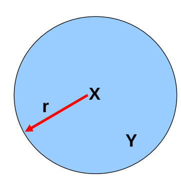
- Exploits location information to limit scope of route request flood
  - Location information may be obtained using GPS
- *Expected Zone* is determined as a region that is expected to hold the current location of the destination
  - Expected region determined based on potentially old location information,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

Expected Zone in LAR

X = last known location of node D, at time t0

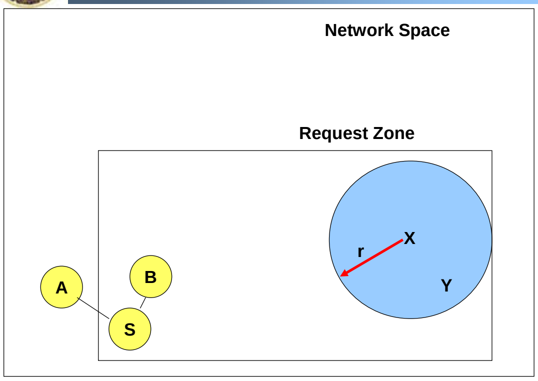
Y = location of node D at current time t1, unknown to node S

r = (t1 - t0) * estimate of D's speed



Expected Zone

Request Zone in LAR

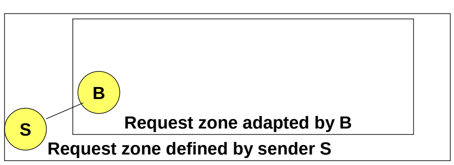


LAR

- Only nodes within the request zone forward route requests
  - Node A does not forward RREQ, but node B does (see previous slide)
- Request zone explicitly specified in the route request
- Each node must know its physical location to determine whether it is within the request zone
- If route discovery using the smaller request zone fails to find a route, the sender initiates another route discovery (after a timeout) using a larger request zone
  - the larger request zone may be the entire network
- Rest of route discovery protocol similar to DSR

LAR Variations: Adaptive Request Zone

- Each node may modify the request zone included in the forwarded request
- Modified request zone may be determined using more recent/accurate information, and may be smaller than the original request zone



LAR Variations: Implicit Request Zone

- In the previous scheme, a route request explicitly specified a request zone
- Alternative approach: A node X forwards a route request received from Y if node X is deemed to be closer to the expected zone as compared to Y
- The motivation is to attempt to bring the route request physically closer to the destination node after each forwarding

Location-Aided Routing

- The basic proposal assumes that, *initially,* location information for node X becomes known to Y only during a route discovery
- This location information is used for a future route discovery
  - Each route discovery yields more updated information which is used for the next discovery

Variations

- Location information can also be piggybacked on any message from Y to X
- Y may also proactively distribute its location information
  - Similar to other protocols discussed later (e.g., DREAM, GLS)

9

Location Aided Routing (LAR)

- 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 obstructions for radio transmissions

10

Query Localization [CD99]

- Limits route request flood without using physical information
- Route requests are propagated only along paths that are *close* to the previously known route
- The *closeness* property is defined without using physical location information

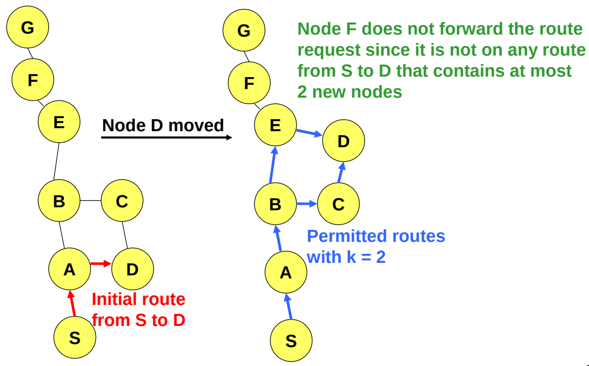
11

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 the accumulated route in the Route Request contains at most *k* new nodes that were absent in the old route
  - this limits propagation of the route request

12

Query Localization: Example



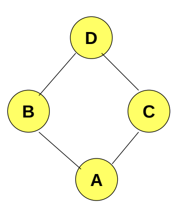
Query Localization

- Advantages:
  - Reduces overhead of route discovery without using physical location information
  - Can perform better in presence of obstructions by searching for new routes in the *vicinity* of old routes
- Disadvantage:
  - May yield routes longer than LAR

    (Shortest route may contain more than k new nodes)

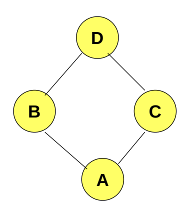
Broadcast Storm Problem [NTC+99]

- When node A broadcasts a route query, nodes B and C both receive it
- B and C both forward to their neighbors
- B and C transmit at about the same time since they are reacting to receipt of the same message from A
- This results in a high probability of collisions



Broadcast Storm Problem

- Redundancy: A given node may receive the same route request from too many nodes, when one copy would have sufficed
- Node D may receive from nodes B and C both



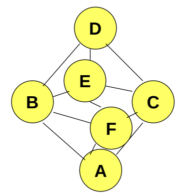
Solutions for Broadcast Storm

- Probabilistic scheme: On receiving a route request for the first time, a node will re-broadcast (forward) the request with probability p
- Also, re-broadcasts by different nodes should be staggered by using a collision avoidance technique (wait a random delay when channel is idle)
  - This would reduce the probability that nodes B and C would forward a packet simultaneously in the previous example

17

Solutions for Broadcast Storms

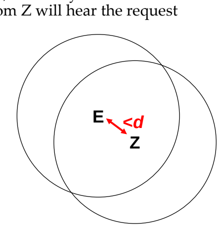
- Counter-Based Scheme: If node E hears more than *k* neighbors broadcasting a given route request, before it can itself forward it, then node E will not forward the request
- Intuition: *k* neighbors together have probably already forwarded the request to all of E's neighbors



18

Solutions for Broadcast Storms

- Distance-Based Scheme: If node E hears RREQ broadcasted by some node Z within physical distance *d*, then E will not re-broadcast the request
- Intuition: Z and E are too close, so transmission areas covered by Z and E are not very different
  - If E re-broadcasts the request, not many nodes who have not already heard the request from Z will hear the request



19

Summary: Broadcast Storm Problem

- Flooding is used in many protocols, such as Dynamic Source Routing (DSR)
- Problems associated with flooding
  - Collisions
  - Redundancy
- Collisions may be reduced by "jittering" (waiting for a random interval before propagating the flood)
- Redundancy may be reduced by selectively re-broadcasting packets from only a subset of the nodes

20

EEC173B/ECS152C, Winter 2006

MANET Unicast Routing

- Reactive Protocol
  - Flooding
  - DSR
  - LAR
  - AODV

Ad Hoc On-Demand Distance Vector Routing (AODV)

- [PR99] C. E. Perkins and E. M. Royer. "Ad hoc On-Demand Distance Vector Routing," *WMCSA*, 1999.
- DSR includes source routes in packet headers
- Resulting large headers can sometimes degrade performance
  - Particularly when data contents of a packet are small
- AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to contain routes
- AODV retains the desirable feature of DSR that routes are maintained only between nodes which need to communicate

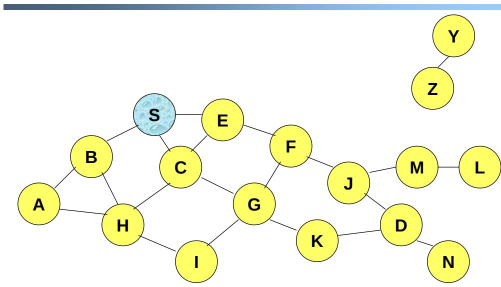
22

AODV

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

23

Route Requests in AODV

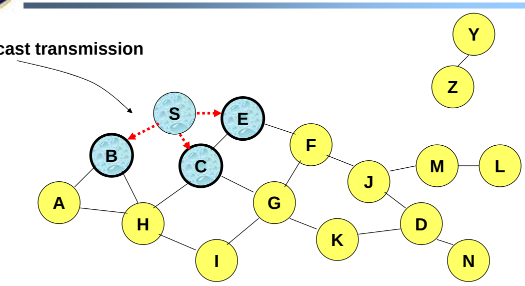


Represents a node that has received RREQ for D from S

24

Route Requests in AODV

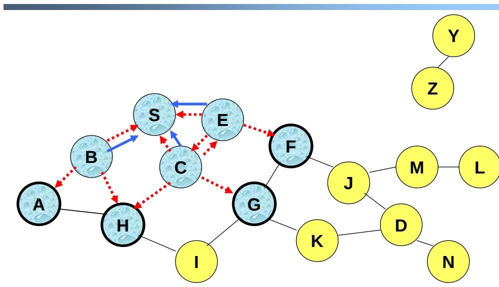
Broadcast transmission



Represents transmission of RREQ

25

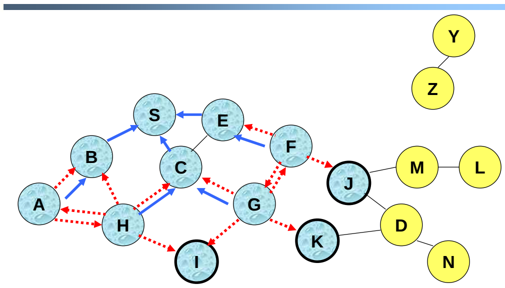
Route Requests in AODV



Represents links on Reverse Path

26

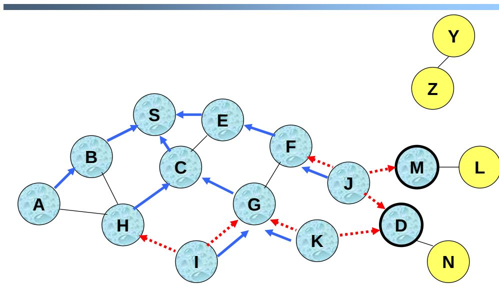
Reverse Path Setup in AODV



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

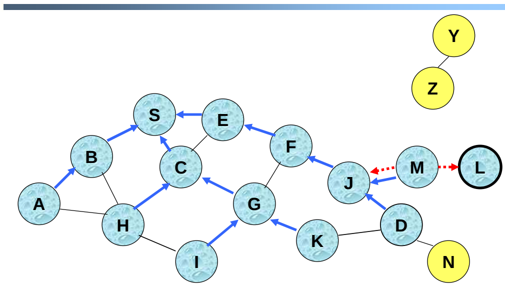
27

Reverse Path Setup in AODV



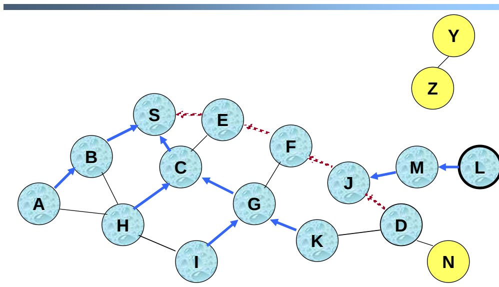
28

Reverse Path Setup in AODV



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

Route Reply in AODV

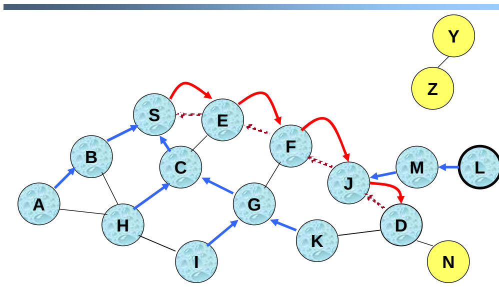


Represents links on path taken by RREP

Route Reply in AODV

- An intermediate node (not the destination) may also send a Route Reply (RREP) provided that it knows a more recent path than the one previously known to sender S
- To determine whether the path known to an intermediate node is more recent, *destination sequence numbers* are used
- The likelihood that an intermediate node will send a Route Reply when using AODV not as high as DSR
  - A new Route Request 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 Route Reply

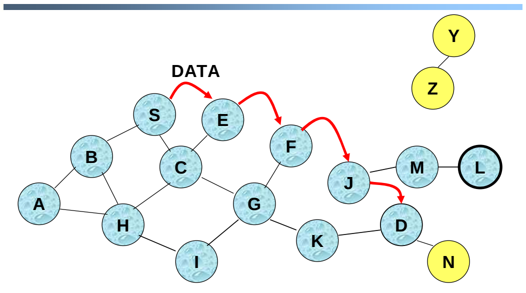
Forward Path Setup in AODV



Forward links are setup when RREP travels along the reverse path

Represents a link on the forward path

Data Delivery in AODV



Routing table entries used to forward data packet.
Route is *not* included in packet header.

33

Timeouts

- A routing table entry maintaining a reverse path is purged after a timeout interval
  - Timeout should be long 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 data is being sent using a particular routing table entry, that entry will be deleted from the routing table (even if the route may actually still be valid)

34

Link Failure Reporting

- 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
- 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 messages, which also update destination sequence numbers

35

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*

36

Destination Sequence Number

- Continuing from the previous slide …
- 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

37

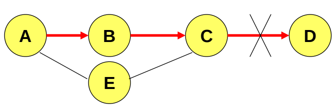
Link Failure Detection

- *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

38

Why Sequence Numbers in AODV

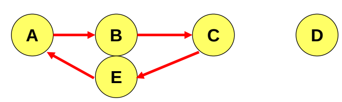
- To avoid using old/broken routes
  - To determine which route is newer
- To prevent formation of loops



- Assume that A does not know about failure of link C-D because RERR sent by C is lost
- Now C performs a route discovery for D. Node A receives the RREQ (say, via path C-E-A)
- Node A will reply since A knows a route to D via node B
- Results in a loop (for instance, C-E-A-B-C)

39

Why Sequence Numbers in AODV



- Loop C-E-A-B-C

40

Optimization: Expanding Ring Search

- Route Requests are initially sent with small Time-to-Live (TTL) field, to limit their propagation
  - DSR also includes a similar optimization
- If no Route Reply is received, then larger TTL tried

41

Summary: AODV

- 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
- Unused routes expire even if topology does not change

42