TELE303 Mobile Systems

Lecture 7 – Mobile Ad hoc Networks & Routing

Jeremiah Deng
TELE Programme / InfoSci
University of Otago, 2016

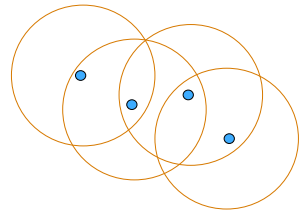
Overview

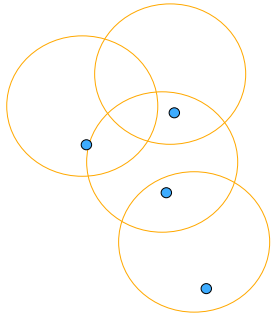
Mobile Ad Hoc Networks (MANET)

- Formed by wireless hosts which may be mobile without (necessarily) using a pre-existing infrastructure
  - Topology changes frequently
  - Multi-hop wireless links
  - Data must be routed via intermediate nodes
- Advantages:
  - Ease and speed of deployment
  - Decreased dependence on infrastructure
- Many application:
  - Personal area networking (phones, sensors, wrist-watches)
  - Military environments
  - Civilian environments: e.g. taxi cab network, boats
  - Emergency operations: search-and-rescue

Challenges

- Limited wireless transmission range
- Broadcast nature of the wireless medium
- Packet losses due to transmission errors
- Mobility-induced route changes
- Mobility-induced packet losses
- Battery constraints
- Ease of snooping on wireless transmissions (security hazard)





Approaches

- **Proactive** protocols
  - Traditional distributed shortest-path protocols
  - Maintain routes between every host pair at all times
  - Based on periodic updates; High routing overhead
- **Reactive** protocols
  - Determine route if and when needed
  - Source initiates route discovery
- Hybrid protocols

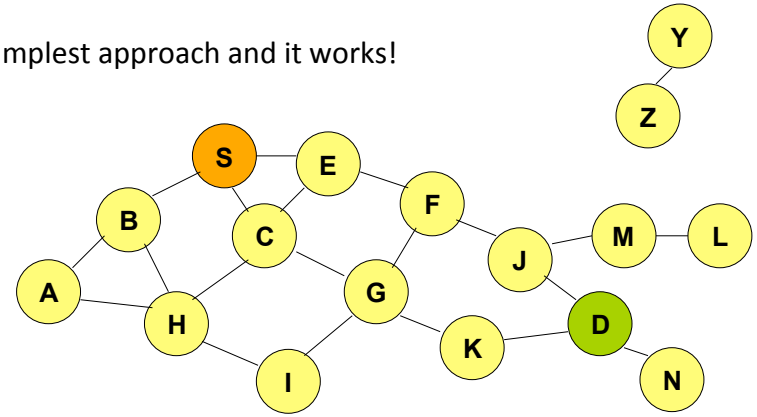
Trade-Off

- **Latency** of route discovery
  - Proactive protocols may have lower latency since routes are maintained at all times
  - Reactive protocols may have higher latency because a route from X to Y will be found only when X attempts to send to Y
- **Overhead** of route discovery/maintenance
  - Reactive protocols may have lower overhead since routes are determined only if needed
  - Proactive protocols can (but not necessarily) result in higher overhead due to continuous route updating
- Which approach achieves a better trade-off depends on the traffic and mobility patterns

Flooding

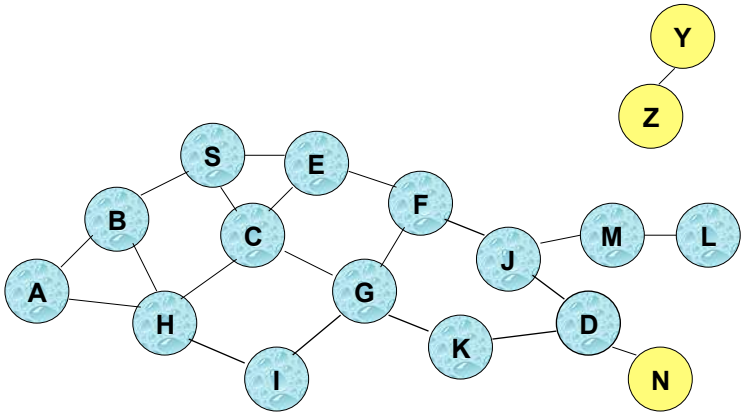
Data Delivery: Flooding

The simplest approach and it works!



Connected nodes are within each other's transmission range

Flooding for Data Delivery



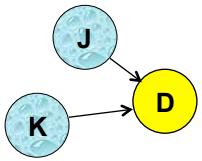
- Flooding may deliver packets to too many nodes
  - In the worst case, all nodes reachable from sender may receive the packet)

Flooding: Advantages

- **Simplicity**
- More ***efficient*** when rate of information transmission is low enough that the overhead of explicit route discovery/maintenance incurred by other protocols is relatively higher
- Potentially higher ***reliability*** of data delivery
  - Packets may be delivered to the destination on multiple paths

Flooding: Disadvantages

- Potentially, very high **overhead**
  - Data packets may be delivered to too many nodes who do not need to receive them
- Potentially **lower reliability** of data delivery
  - Flooding uses broadcasting - hard to implement reliable broadcast delivery without significantly increasing overhead
    - Broadcasting in IEEE 802.11 MAC is unreliable
    - E.g., nodes J and K may transmit to D simultaneously, resulting in loss



Flooding of Control Packets

- 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 amortised over data packets transmitted between consecutive control packet floods.

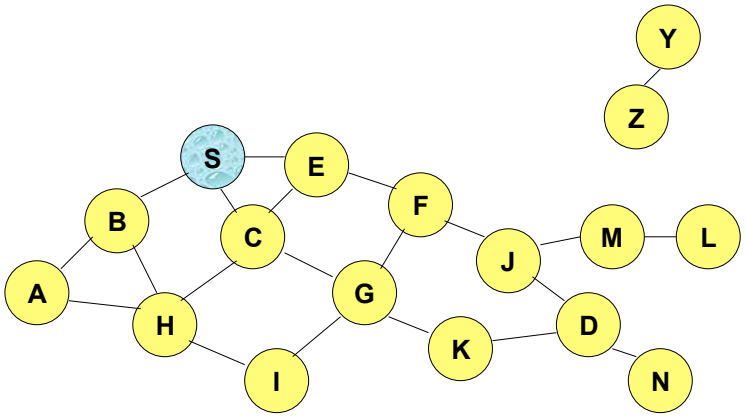
• • •

DSR

Dynamic Source Routing (DSR)

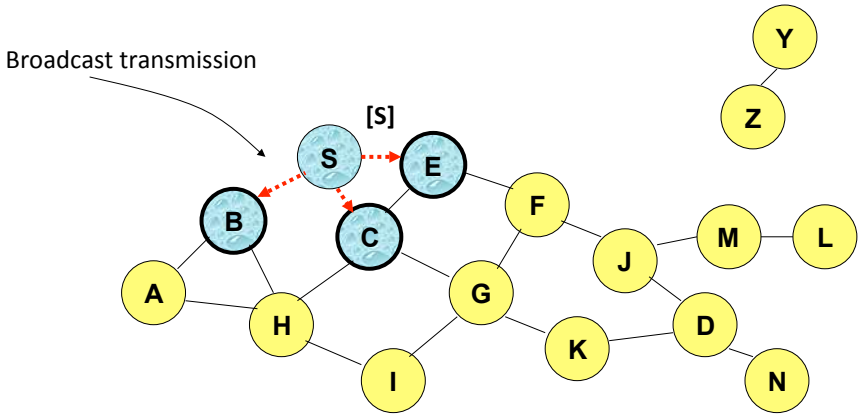
- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a **route discovery.**
- Source node S floods **Route Request** (RREQ).
- Each node **appends own identifier** when forwarding RREQ.

Route Discovery in DSR



Represents a node that has received RREQ for D from S

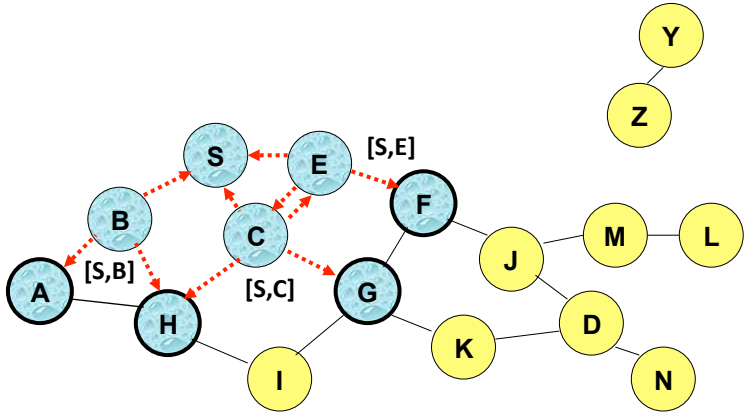
Route Discovery in DSR



Represents transmission of RREQ

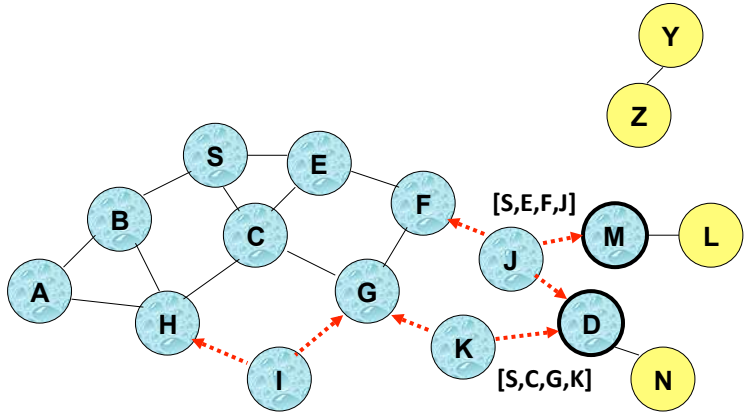
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



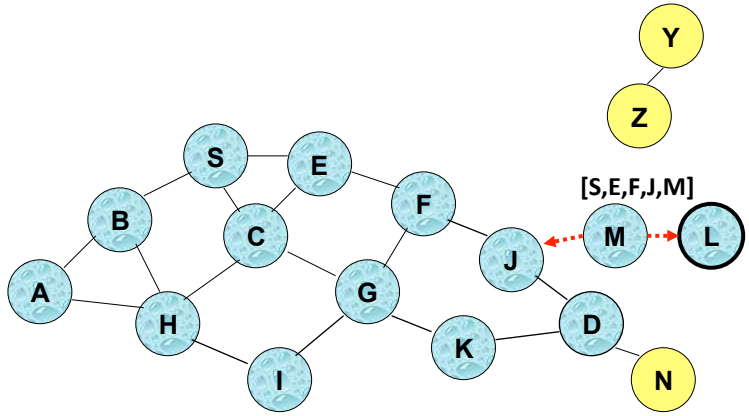
- Node H receives packet RREQ from two neighbours: potential for collision

Route Discovery in DSR



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

Route Discovery in DSR

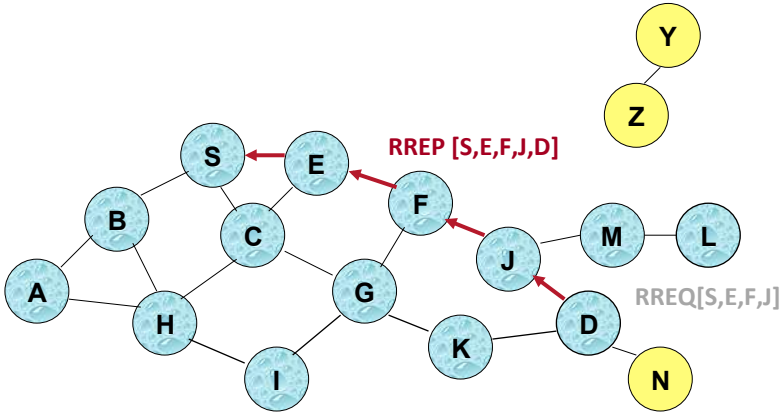


- Node D does not forward RREQ, because node D is the intended target of the route discovery

Route Discovery in DSR

- 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 Reply in DSR

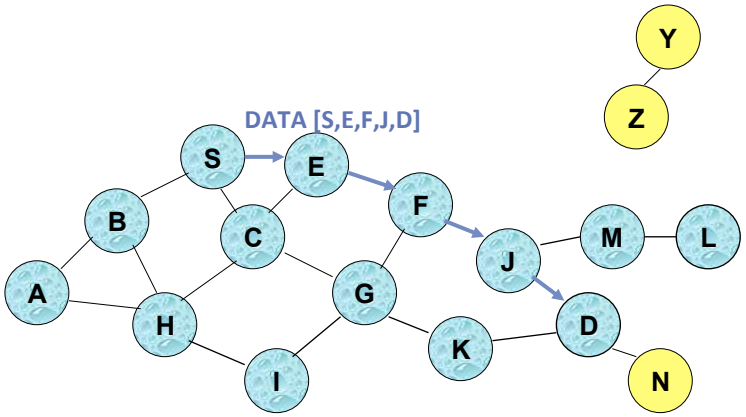


Represents RREP control message

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 'source routing'
- Intermediate nodes use the source route included in a packet to determine to whom a packet should be forwarded.

Data Delivery in DSR



Packet header size grows with route length

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
  - Node F forwards Route Reply RREP [S,E,F,J,D], node F learns route [F,J,D] to node D.
  - Node K receives Route Request [S,C,G] destined for a node, node K learns route [K,G,C,S] to node S.
- A node may also learn a route when it overhears Data packets.

DSR: Advantages

- Routes maintained only between nodes who *need* to communicate
  - ☺reduces overhead of route maintenance

☺Route caching can further reduce route discovery overhead

☺A single route discovery may yield **multiple routes** to the destination, esp. with intermediate nodes replying from local caches

DSR: Disadvantages

☹ Packet header size grows with route length due to source routing

☹ Flood of route requests may potentially reach all nodes in the network

☹ Care must be taken to avoid collisions between route requests propagated by neighbouring 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
  - *aka* 'Route Reply Storm problem'
  - Reply storm may be eased by preventing a node from sending RREP if it hears another RREP with a shorter route

Take a lesson from the ants, you lazybones. Learn from their ways and become wise! (Proverbs 6:6)

AODV

A Better Reactive Protocol?

- DSR includes source routes in packet headers, resulting large headers can sometimes degrade performance
  - Particularly when data contents of a packet are small

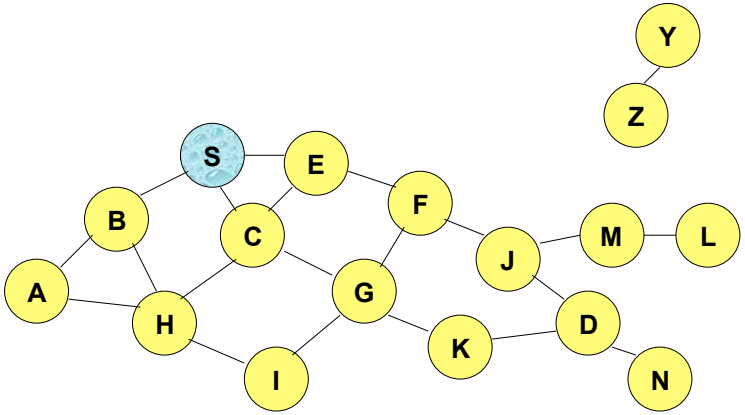
→ Can we improve it by maintaining routing tables at the nodes, so that data packets do not have to contain routes?

- We still intend to retain the desirable feature of DSR that routes are maintained only between nodes which need to communicate.

AODV

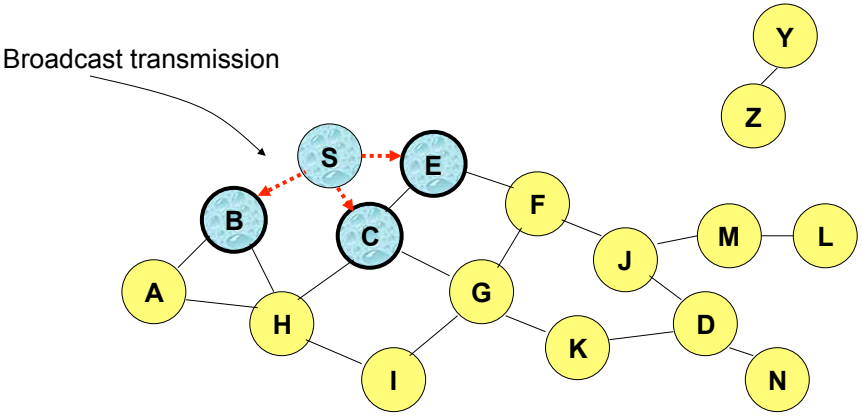
- Route Requests (RREQ) are forwarded in a manner similar to DSR
- When a node re-broadcasts a **Route Request**, it sets up a **reverse path** pointing towards the source
  - AODV assumes symmetric (bi-directional) links
- When the intended destination receives a Route Request, it replies by sending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

Route Requests in AODV



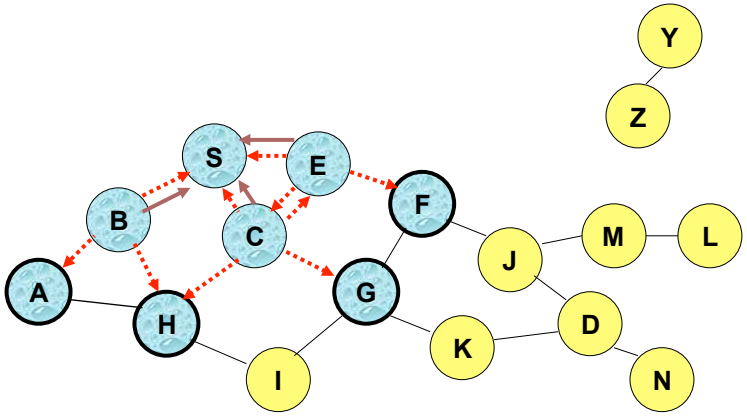
Represents a node that has received RREQ for D from S

Route Requests in AODV



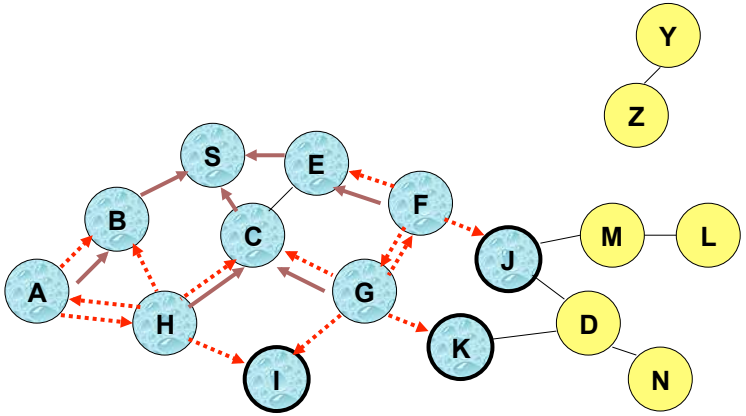
Represents transmission of RREQ

Route Requests in AODV



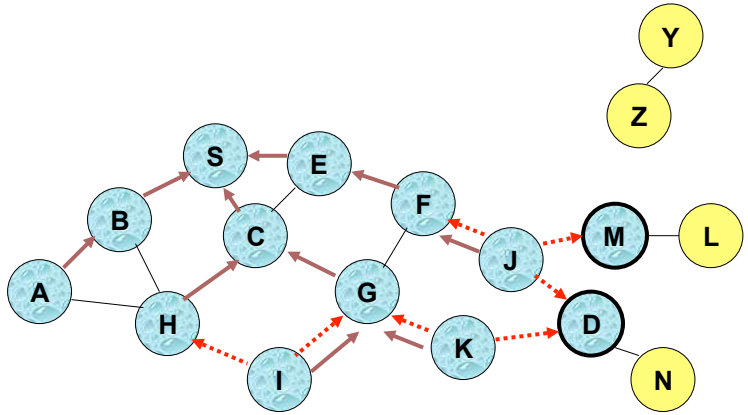
Represents links on Reverse Path

Reverse Path Setup in AODV

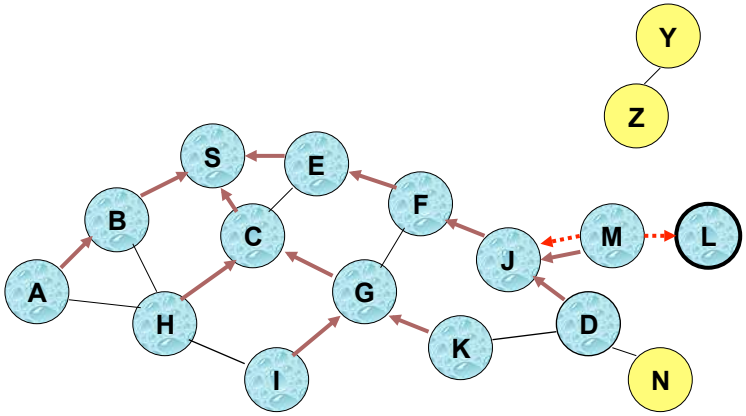


- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

Reverse Path Setup in AODV

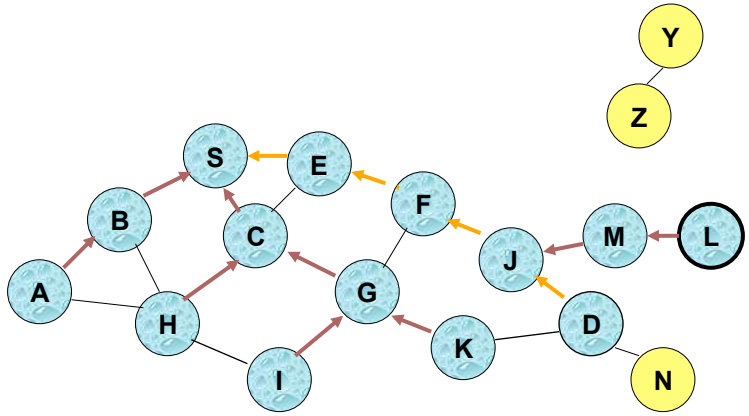


Reverse Path Setup in AODV



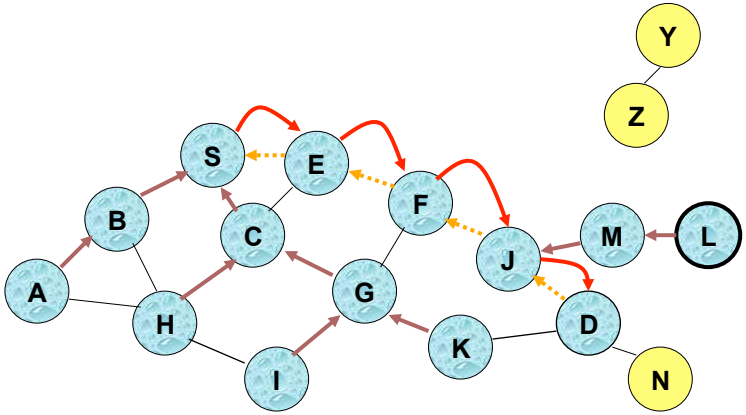
- Node D does not forward RREQ, because node D is the intended target of the RREQ

Route Reply in AODV



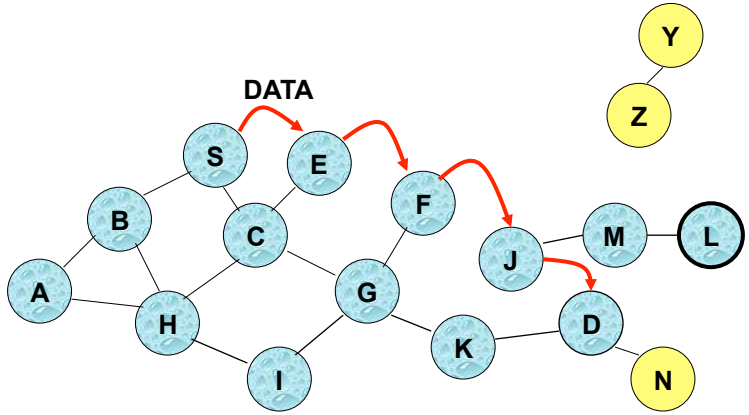
← Links on path taken by RREP

Forward Path Setup in AODV



Forward links are setup when RREP travels along the reverse path

Data Delivery in AODV



Routing table entries used to forward data packet.

Route is *not* included in packet header.

Coping with Link Failure

- A neighbour of node X is considered active for a routing table entry if the neighbour sent a packet within *active_route_timeout* interval which was forwarded using that entry
- Neighbouring nodes periodically exchange **hello** message
- When the next hop link in a routing table entry breaks, all active neighbours are informed
  - Link failures are propagated by means of **Route Error** (RERR) messages, which also update destination sequence numbers.
- AODV uses incremental **sequence number** to handle route failures.
  - avoid old/broken routes
  - prevent formation of routing loops

Recap

- Reactive routing
- DSR
  - Uses RREQ flooding and RREP replies
  - Includes source routes in packet headers
- AODV
  - Retains DSR's desirable feature of Reactive Routing
  - Improves on efficiency

- **Next Lecture**:
  - TCP on MANETs