Routing Protocol: DSR

Instructor: Dr. Sunho Lim (Ph.D., Assistant Professor)

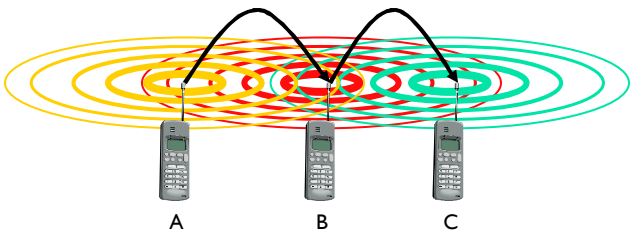
Lecture 09

sunho.lim@ttu.edu

Adapted partially from Mobile Communications, Jochen Schiller, and Prof. Nitin Vaidya in UIUC.

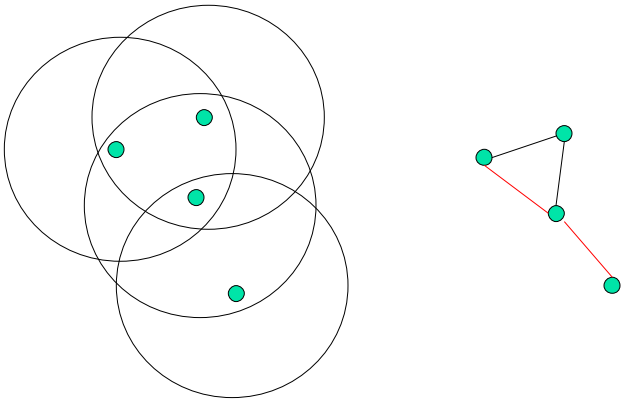
Mobile Ad hoc NETworks (MANETs)

- Sometimes there is NO infrastructure!
  - remote areas, ad-hoc meetings, disaster areas
  - cost can also be an argument against an infrastructure!
- Main topic: routing
  - no default router available
  - every node should be able to forward



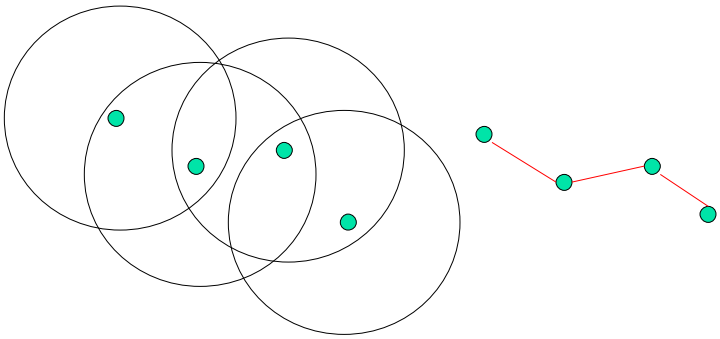
Mobile Ad hoc NETworks (MANETs) (cont.)

- May need to traverse multiple links to reach a destination



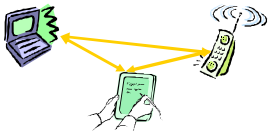
Mobile Ad hoc NETworks (MANETs) (cont.)

- Mobility causes route changes



Mobile Ad hoc NETworks (MANETs) (cont.)

- Network without infrastructure
  - Use components of participants for networking
- Examples
  - Single-hop: All partners max. one hop apart
    - Bluetooth piconet, PDAs in a room, gaming devices…
  - Multi-hop: Cover larger distances, circumvent obstacles
    - Bluetooth scatternet, TETRA police network, car-to-car networks (i.e., vehicular ad hoc networks (VANETs) – V2V, V2I)



- Internet: MANET (Mobile Ad-hoc Networking) group

Why Ad Hoc Networks ?

- Ease of deployment
- Speed of deployment
- Decreased dependence on infrastructure

- Many Applications:
  - Personal area networking
    - cell phone, laptop, ear phone, wrist watch, etc.
  - Military environments
    - soldiers, tanks, planes, etc.
  - Civilian environments
    - taxi cab network, meeting rooms, sports stadiums, boats, small aircraft, etc.
  - Emergency operations
    - search-and-rescue, policing and fire fighting, etc.

Traditional Routing Algorithms

- Link State:
  - periodic notification of all routers about the current state of all physical links
  - router get a complete picture of the network
- Distance Vector:
  - periodic exchange of messages with all physical neighbors that contain information about who can be reached at what distance
  - selection of the shortest path if several paths available

Problems of Traditional Routing Algorithms

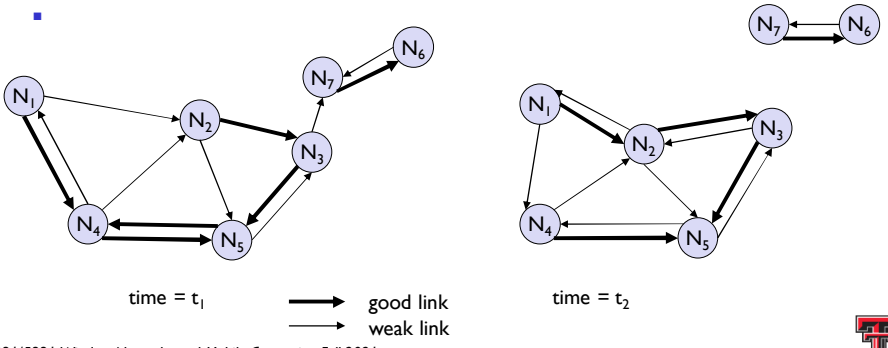
- Dynamic of the topology
  - frequent changes of connections, connection quality, participants
- Limited performance of mobile systems
  - periodic updates of routing tables need energy without contributing to the transmission of user data,
    - sleep modes difficult to realize
  - limited bandwidth of the system is reduced even more due to the exchange of routing information
  - links can be asymmetric, i.e., they can have a direction dependent transmission quality

Routing in Ad-hoc Networks

- THE big topic in many research projects
  - Far more than 50 different proposals exist
  - The most simplest one: Flooding!
- Reasons:
  - Classical approaches from fixed networks fail
    - Very slow convergence, large overhead
  - High dynamicity, low bandwidth, low computing power
- Metrics for routing:
  - Minimal
    - Number of nodes, loss rate, delay, congestion, interference …
  - Maximal
    - Stability of the logical network, battery run-time, time of connectivity …

Problem No. 1: Routing

- Highly dynamic network topology
  - device mobility plus varying channel quality
  - separation and merging of networks possible
  - asymmetric connections possible
-



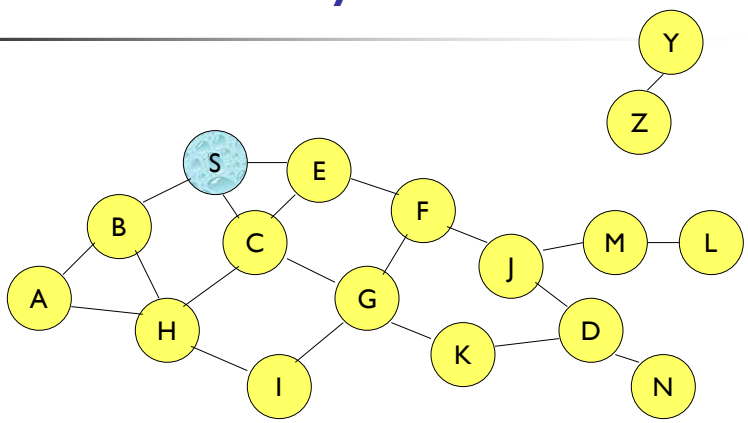
Dynamic Source Routing (DSR)

- 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

Dynamic Source Routing (DSR) (cont.)

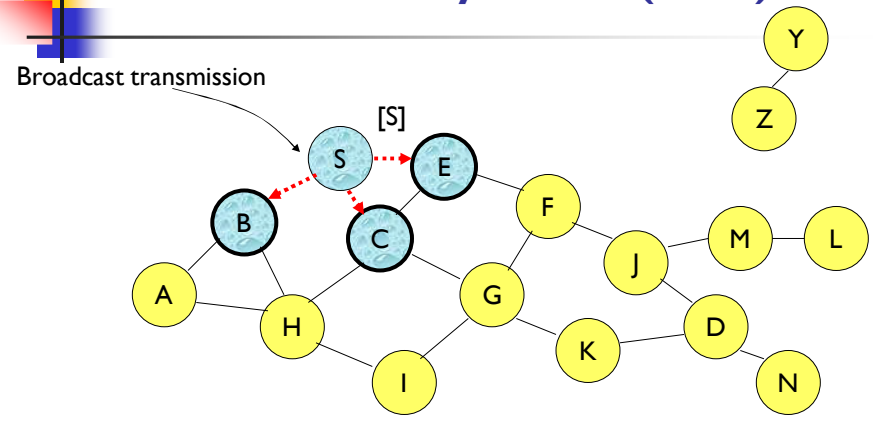
- Path discovery
  - broadcast a packet with destination address and unique ID
  - if a node receives a broadcast packet
    - if the node is the receiver (i.e., has the correct destination address) then return the packet to the sender (path was collected in the packet)
    - if the packet has already been received earlier (identified via ID) then discard the packet
    - otherwise, **append own address** and broadcast packet
  - sender receives packet with the current path (address list)
- Optimizations
  - limit broadcasting if maximum diameter of the network is known
  - caching of address lists (i.e. paths) with help of passing packets
    - stations can use the cached information for path discovery (own paths or paths for other hosts)

Route Discovery in DSR



Represents a node that has received RREQ for D from S

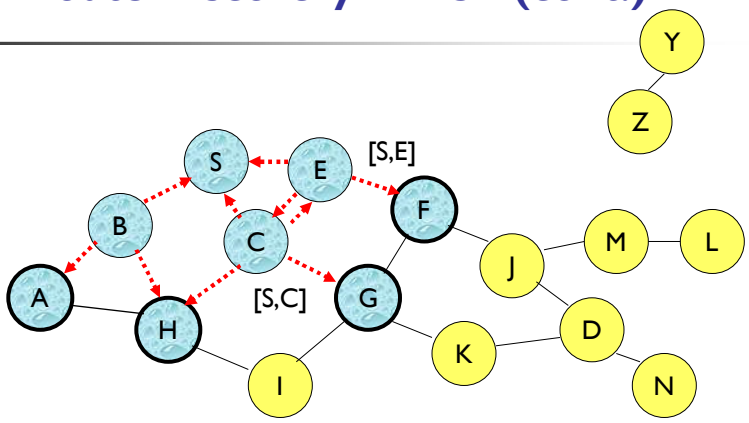
Route Discovery in DSR (cont.)



Represents transmission of RREQ

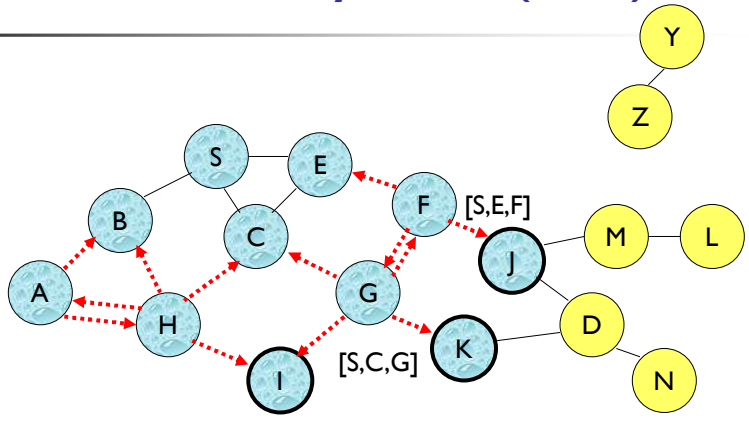
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR (cont.)



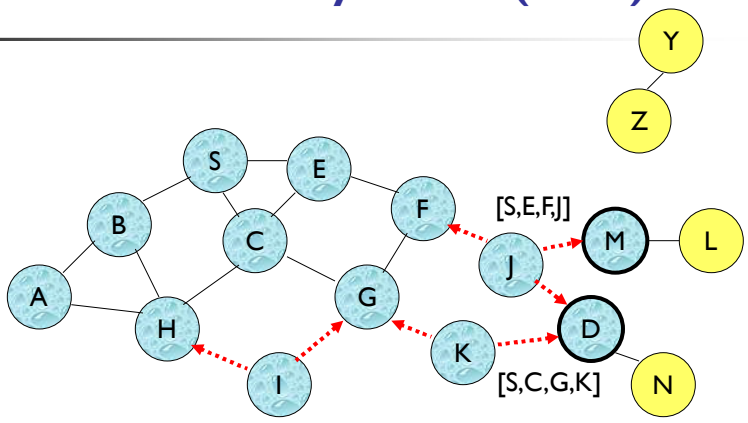
- Node H receives packet RREQ from two neighbors: potential for collision

Route Discovery in DSR (cont.)



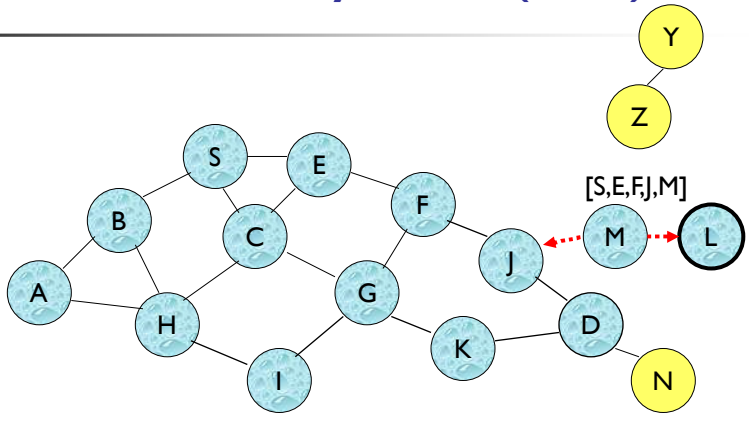
- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

Route Discovery in DSR (cont.)



- 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 (cont.)

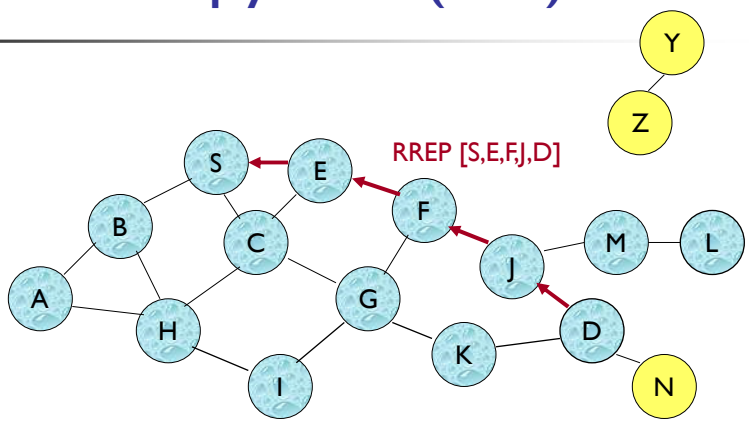


- Node D does not forward RREQ, because node D is the intended target of the route discovery

Route Reply 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 (cont.)



Represents RREP control message

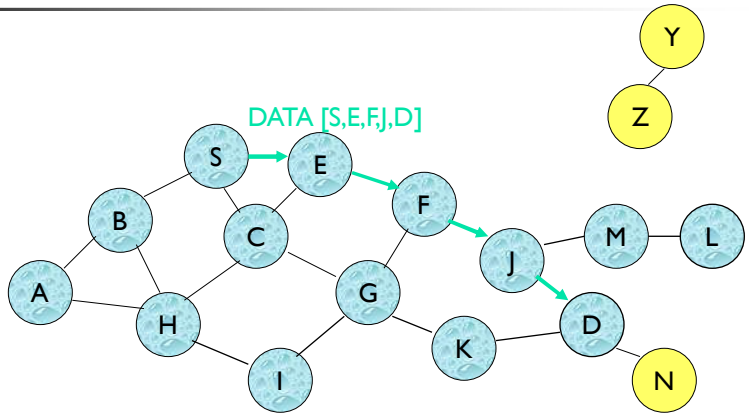
Route Reply in DSR (cont.)

- Route Reply can be sent by reversing the route in Route Request (RREQ) only if links are guaranteed to be bi-directional
  - To ensure this, RREQ should be forwarded only if it received on a link that is known to be bi-directional
- If unidirectional (asymmetric) links are allowed, then RREP may need a route discovery for S from node D
  - Unless node D already knows a route to node S
  - If a route discovery is initiated by D for a route to S, then the Route Reply is piggybacked on the Route Request from D.
- If IEEE 802.11 MAC is used to send data, then links have to be bi-directional (since Ack is used)

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

Data Delivery in DSR (cont.)

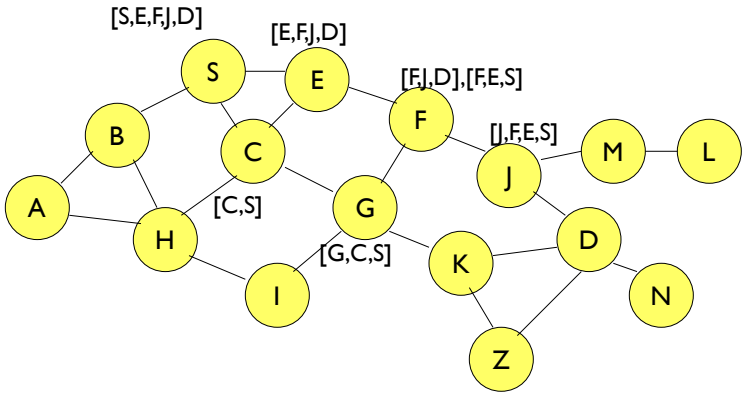


Packet header size grows with route length

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
- 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 [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 packets

Use of Route Caching (cont.)

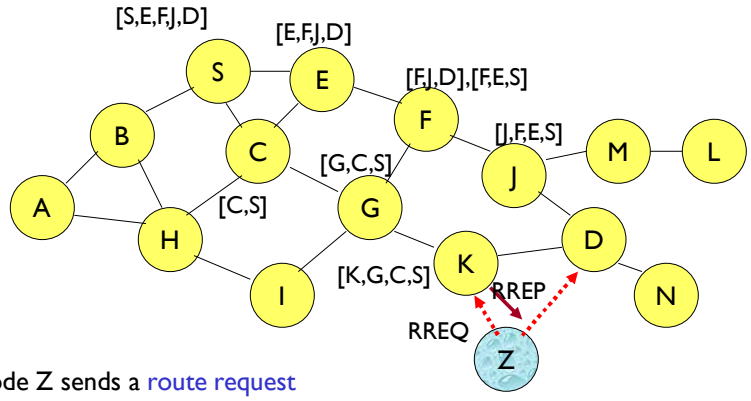


Represents cached route at a node (DSR maintains the cached routes in a tree format)

Use of Route Caching

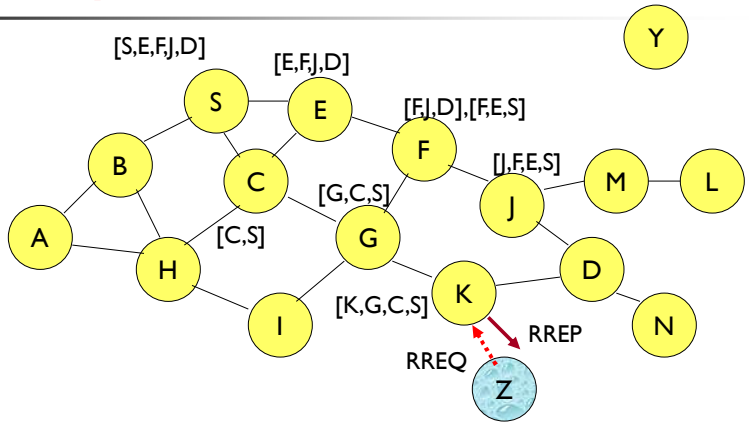
- When node S learns that a route to node D is broken,
  - it uses another route from its local cache, if such a route to D exists in its cache.
  - Otherwise, node S initiates route discovery by sending a route request
- Node X on receiving a Route Request for some node D can send a Route Reply if node X knows a route to node D
- Use of route cache
  - can speed-up route discovery
  - can reduce propagation of route requests

Use of Route Caching: Can Speed-up Route Discovery



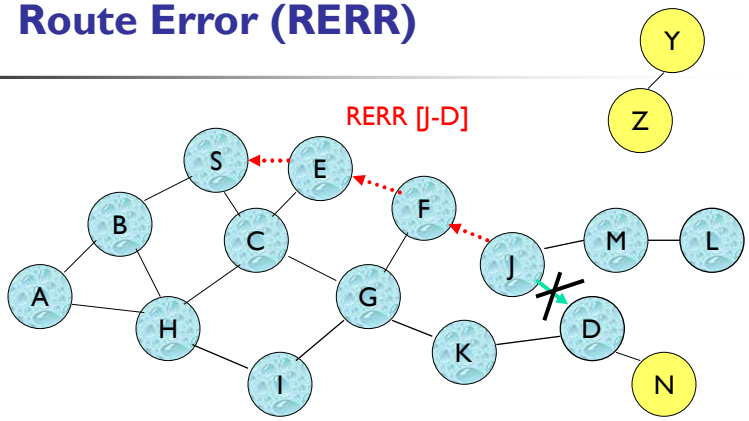
When node Z sends a route request for node C, node K sends back a route reply [Z,K,G,C] to node Z using a locally cached route

Use of Route Caching: Can Reduce Propagation of Route Requests



Assume that there is no link between D and Z.
Route Reply (RREP) from node K limits flooding of RREQ.
In general, the reduction may be less dramatic.

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

Route Caching: Beware!

- Stale caches can adversely affect performance
- With passage of time and host mobility, cached routes may become invalid
- A sender host may try several stale routes (obtained from local cache, or replied from cache by other nodes), before finding a good route

Dynamic Source Routing: 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 many routes to the destination, due to intermediate nodes replying from local caches

Dynamic Source Routing: 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 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
  - Reply storm may be eased by preventing a node from sending RREP if it hears another RREP with a shorter route

Dynamic Source Routing: Disadvantages (cont.)

- An intermediate node may send Route Reply using a stale cached route, thus polluting other caches
  - Route cache pollution
  - This problem can be eased if some mechanism to purge (potentially) invalid cached routes is incorporated.