African University of Science and Technology

# Introduction to Ad Hoc Networks

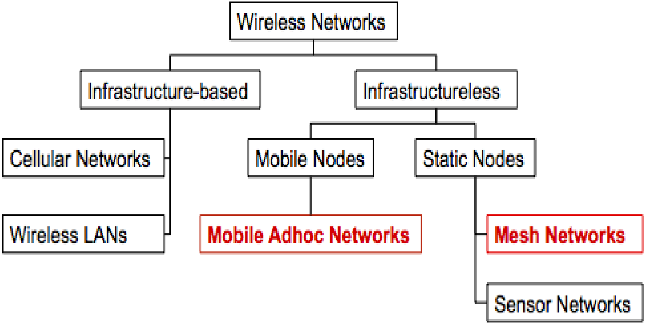
Prof. Ousmane THIARE

[www.ousmanethiare.com]

April 16, 2020

# Outline

## Taxonomy of Wireless systems

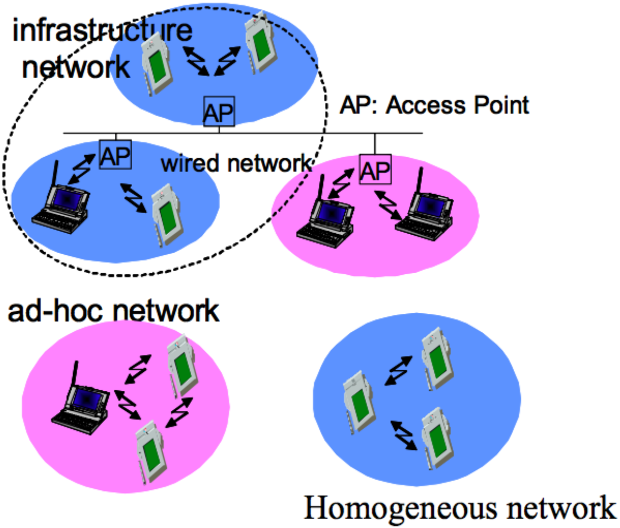


# Mobile Ad hoc Networks (MANETs)

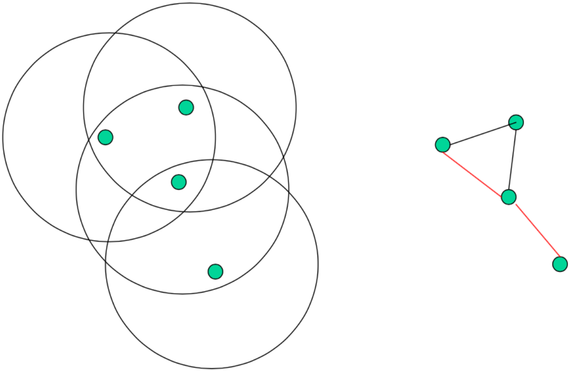
- No infrastructure (no base stations or access points)
- Mobile nodes
  - Form a network in an ad-hoc manner
  - Act both as hosts and routers
  - Communicate using single or multi-hop wireless links
- Topology, locations, connectivity, transmission quality are variable.

- A network without any base stations “infrastructure-less” or multi-hop
- A collection of two or more devices equipped with wireless communications and networking capability
- Supports anytime and anywhere computing
- Two topologies:
  - Heterogeneous (left)
    - Differences in capabilities
  - Homogeneous or fully symmetric (Right)
    - all nodes have identical capabilities and responsibilities

- Self-organizing and adaptive – Allows spontaneous formation and deformation of mobile networks
- Each mobile host acts as a AP router
- Supports peer-to-peer communications
- Reduced administrative cost
- Ease of deployment

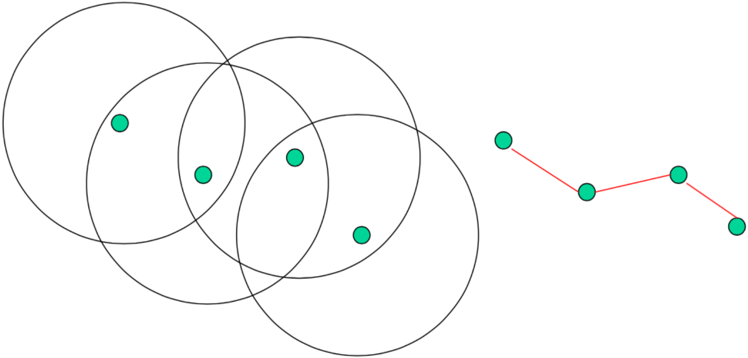

infrastructure network
AP: Access Point
AP
AP
wired network
AP
ad-hoc network
Homogeneous network

# Mobile Ad Hoc Networks



# Mobile Ad Hoc Networks

- Mobility causes route changes



# Why Ad Hoc Networks?

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

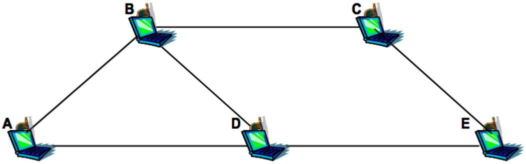



Figure: Example of an Ad Hoc Network

- Fig. depicts a peer-to-peer multihop ad hoc network
- Mobile node A communicates directly with B (single hop) when a channel is available
- If Channel is not available, then multi-hop communication is necessary e.g. $A \rightarrow D \rightarrow B$
- For multi-hop communication to work, the intermediate nodes should route the packet i.e. they should act as a router
- Example: For communication between A-C, B, or D & E, should act as routers

## Bringing up an Ad hoc Network

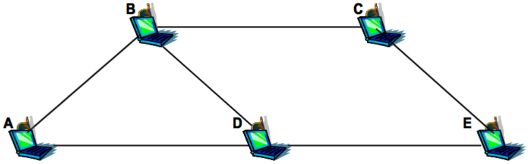



Figure: Example of an Ad Hoc Network

- Ad hoc network begins with at least two nodes broadcasting their presence (beaconing) with their respective address information
- They may also include their location info if GPS equipped
- Beaconing messages are control messages. If node A is able to establish a direct communication with node B verified by appropriate control messages between them, they both update their routing tables

## Bringing up an Ad hoc Network

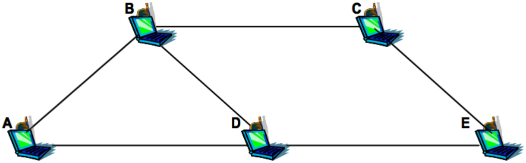



Figure: Example of an Ad Hoc Network

- Third node C joins the network with its beacon signal. Two scenarios are possible:
  (i) A & B both try to determine if single hop communication is feasible
  (ii) Only one of the nodes e.g. B tries to determine if single hop communication is feasible and establishes a connection
- The distinct topology updates consisting of both address and the route updates are made in three nodes immediately.

## Bringing up an Ad hoc Network

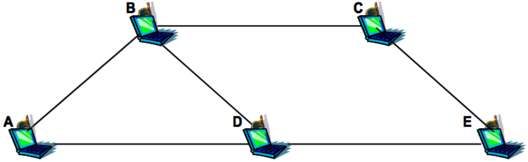
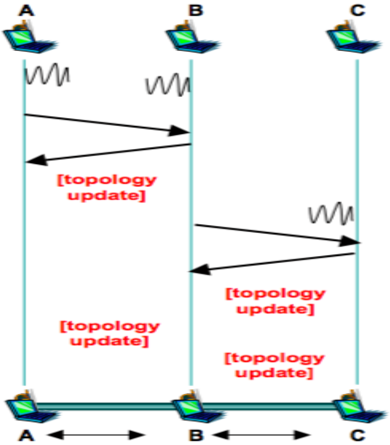



Figure: Example of an Ad Hoc Network

- In first scenario, all routes are direct i.e. $A \rightarrow B, B \rightarrow C$, and $A \rightarrow C$ (Lets assume bi-directional links)

## Bringing up an Ad hoc Network




- In the second scenario, the routes are updated

## Bringing up an Ad hoc Network

- In the second scenario, the routes are updated
- First between B & C,
- then between B & A,
- Then between B & C again confirming that A and C both can reach each other via B

## Topology update due to a link failure

- Mobility of nodes may cause link breakage requiring route updates
- Assume link between B & C breaks because of some reason
- Nodes A & C are still reachable via D and E
- So old route between A & C was $A \rightarrow B \rightarrow C$ is to be replaced by $A \rightarrow D \rightarrow E \rightarrow C$
- All five nodes are required to incorporate this change in their routing table
  - This change will happen first in nodes B & C
  - Then A & E
  - Then D

# Challenges in Ad hoc networks

- Host is no longer an end system - can also be an acting intermediate system
- Changing the network topology over time
- Potentially frequent network partitions
- Every node can be mobile
- Limited power capacity
- Limited wireless bandwidth
- Presence of varying channel quality

# Challenges in Ad hoc networks

- No centralized entity – distributed
- How to support routing?
- How to support channel access?
- How to deal with mobility?
- How to conserve power?
- How to use bandwidth efficiently?

# Challenges in Ad hoc networks

- Routers are now moving
- Link changes are happening quite often
  - Packet losses due to transmission errors
- Event updates are sent often – a lot of control traffic
- Routing table may not be able to, converge
- Routing loop may exist
- Current wired routing uses shortest path metric

# Problems facing channel access in Ad hoc Networks

- Distributed channel access, i.e. no fixed base station concept
- Very hard to avoid packet collisions
- Very hard to support QoS
- Early work on packet radio is based on CSMA

# Problems of Mobility in Ad hoc Networks

- Mobility affects signal transmission $\rightarrow$ Affects communication
- Mobility affects channel access
- Mobility affects routing
  - Mobility-induced route changes
  - Mobility-induced packet losses
- Mobility affects multicasting
- Mobility affects applications

# Mobility in Ad hoc Networks

- Mobility patterns may be different
  - people sitting at an airport lounge
  - Mobility-induced packet losses
  - New York taxi cabs
  - kids playing
  - military movements
  - personal area network
- Mobility characteristics
  - speed
  - predictability
    - direction of movement
    - pattern of movement
  - uniformity (or lack thereof) of mobility characteristics among different nodes

# Problems of Power in Ad hoc

- Ad hoc devices come in many different forms
- Most of them battery powered
- Battery technology is not progressing as fast as memory or CPU technologies
- Wireless transmission, reception, retransmission, beaconing, consume power!

# Why not use routing protocols designed for wired networks?

- Mainly design issues:
  - Too dynamic (i.e. mobile nodes)
  - No specific nodes dedicated for control
  - Different link characteristics (e.g. delay, bandwidth)
  - Different node characteristics (e.g. power constraints, multiple access issues)

# Network Environments

- Fully symmetric
  - Nodes have identical characteristics
  - Nodes are all equally responsible to route
- Asymmetric
  - Any node characteristic can vary
    - ransmitter, processor, memory, mobility, etc.
  - Nodes are all still equally responsible to route
- Asymmetric responsibility
  - Only some nodes will route packets

# MANET Routing Protocol Requirements

1. Fully distributed, no critical nodes
2. Allow for random node events (e.g. entering, leaving, neighbor changes)
3. Minimum delay to determine path (at transmission time)
4. Minimize storage requirements
5. Must remove (or not propagate) invalid paths

# MANET Routing Protocol Requirements

6. Minimize packet collisions
7. Low convergence time to optimal paths
8. Minimize resource use (e.g. processing time, bandwidth usage, power consumption)
9. Nodes should store local information only
10. Provide a minimum QoS

# Routing protocol inputs

- Traditional route update
  - Proactive (table-based)
  - Reactive (on-demand)
  - Hybrid
- Temporal information
  - Past information
  - Future information
- Topology
  - Flat topology
  - Hierarchical topology
- Other network resource
  - Power levels
  - Geographical information

# Reactive vs. Proactive

- Reactive
  - Routes are established after a transmission request is made
  - Advantages:
    - Allows for more flexible powers scenarios
    - Less state needed at each node
  - Disadvantages:
    - Delay before transmission to establish routes
    - High short-term overhead needed to establish routes
    -
- Proactive
  - Routes are established initially and already exist before requests are made
  - Advantages:
    - No delay needed to establish routes
    - Low short-term overhead needed
  - Disadvantages:
    - High long-term overhead needed to maintain routes
    - Need dedicated memory to store long term routing information

# Singlepath vs. Multipath

- Singlepath
  - Use one path from source to destination
  - Similar to wired routes
  - Advantages:
    - Simple to implement
  - Disadvantages
    - Source must find a new route to destination if old one fails

- Multipath
  - Use more than one path from source to destination
  - Advantages:
    - Load balancing can occur
    - Higher tolerance to link failures
  - Disadvantages
    - Adds complexity to receiver and sender

# Some Existing Wireless Routing Protocols

- DSDV
- WRP
- CGSR
- STAR
- OLSR
- FSR
- HSR
- GSR
- DSR
- AODV
- ABR
- SSA
- FORP
- PLBR
- CEDAR
- ZRP
- ZHLS
- RABR
- LBR
- COSR
- PAR
- LAR
- OLSB

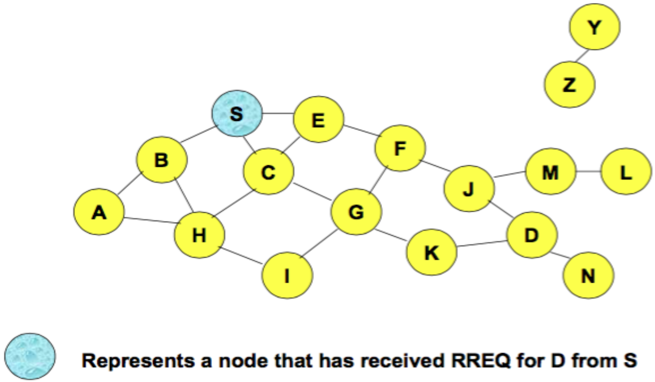
# Dynamic Source Routing (DSR)

- Reactive,source-based
- To determine the route to a destination:
  1. Source floods RouteRequest messages to its neighbors
  2. Each neighbor will flood RouteRequest messages, storing the path in the header
  3. When the destination responds with a RouteReply message containing the path

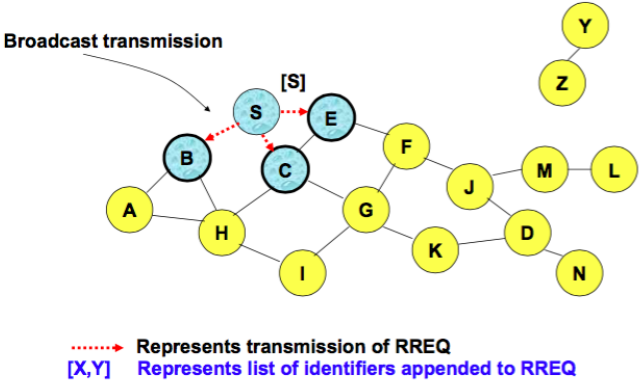
# Dynamic Source Routing (DSR)

- Sequence numbers are used to prevent loops
  - A node can only flood the RouteRequest packet if it has not already flooded it
- On link failure:
  - Adjacent node sends a RouteError message to the source
  - The source will remove the route from its route entry list

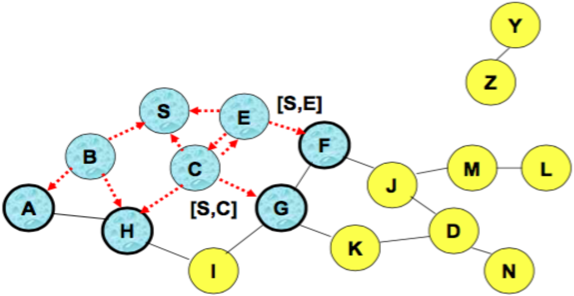
# Dynamic Source Routing (DSR)



# Route Discovery in DSR

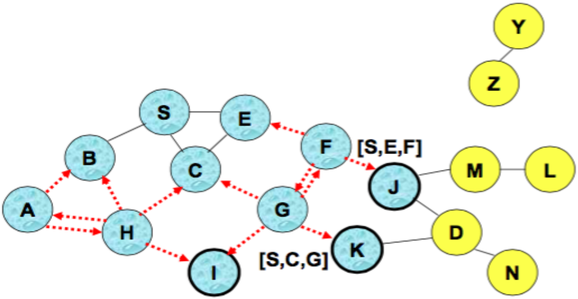


# Route Discovery in DSR



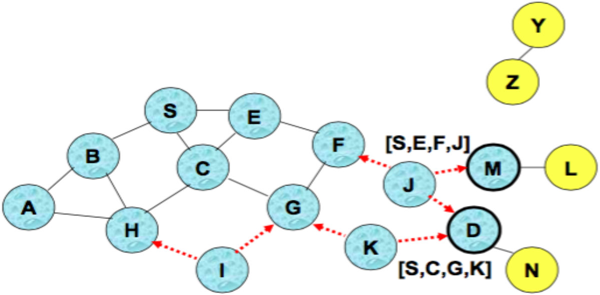

- **Node H receives packet RREQ from two neighbors: potential for collision**

# Route Discovery in DSR



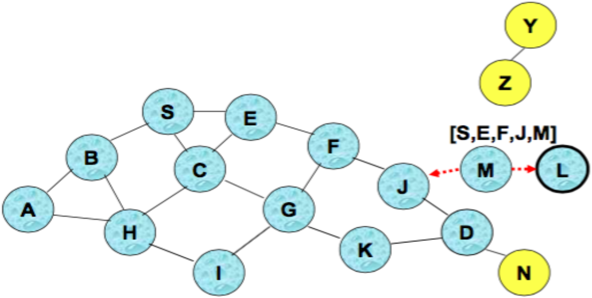

- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

# Route Discovery in DSR



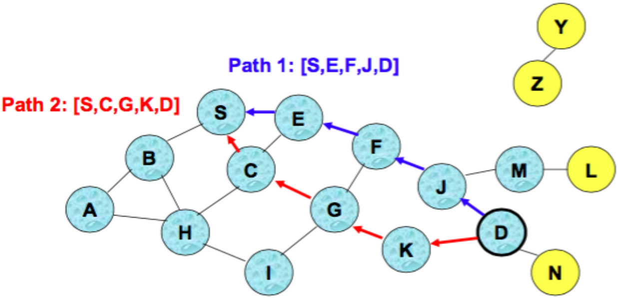

- Nodes J and K both broadcast RREQ to node D
- Since nodes J and K are hidden from each other, their transmissions may collide

# 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




- **Node D replies with a RouteReply message for each path**

# DSR Pros and Cons

- Advantages:
  - Less memory storage needed at each node if a full routing table is not needed
  - Lower overhead needed because no periodic update message are necessary
  - Nodes do not need to continually inform neighbors they are still operational
- Disadvantages:
  - Possible transmission latency due to reactive approach
  - Stale routes can occur if links change frequently
  - Message size increases as path length increases
  - .

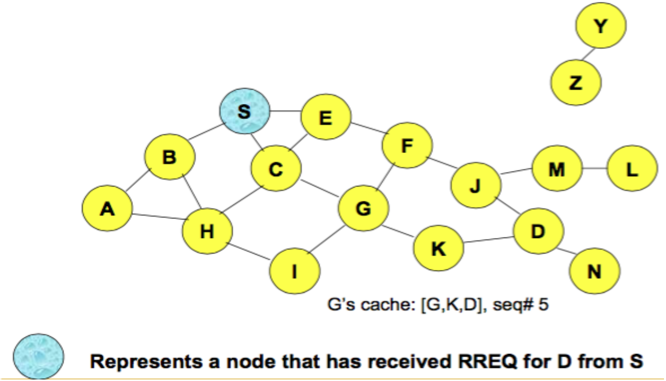
# Ad Hoc On-Demand Distance Vector Routing Protocol (AODV)

- Reactive, source-based
- Uses sequence numbers to determine route age to prevent usage of stale routes
- Source assigns sequence number to RouteRequest
  - Intermediate node is allowed to send RouteReply only if its cached sequence number is greater than the source's assignment
- On link failure:
  - Detected by periodic acknowledgements
  - Nodes send RouteError message. Source must restart path-finding process to destination.

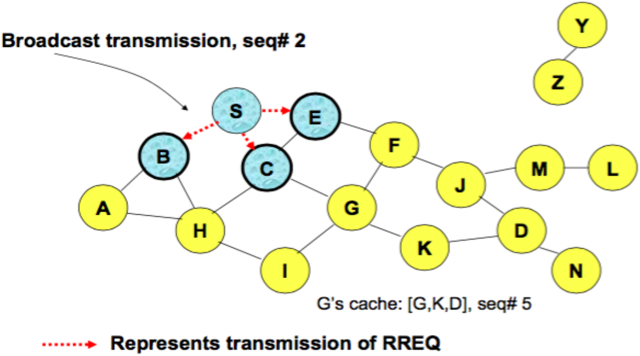
# AODV

- To determine the route to a destination:
  1. Source floods RouteRequest message to neighbors with a sequence number to the destination
  2. If an intermediate node has a cached entry to the destination with a higher sequence number, it responds with a RouteReply message. Else, the previous hop information is cached and the request is flooded further
  3. If the request reaches the destination, a RouteReply is sent back along the path it was received. Intermediate nodes mark the next hop information in the cache.

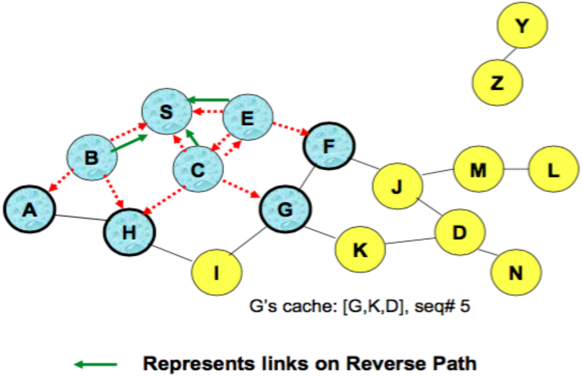
# Route Request in AODV



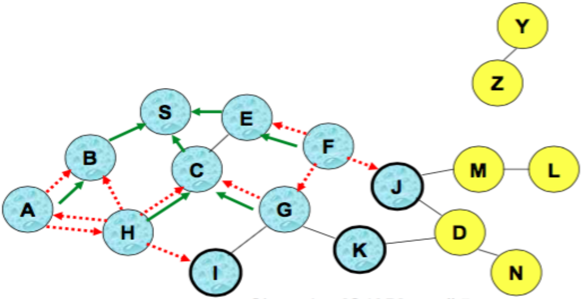
# Route Request in AODV



# Route Request in AODV

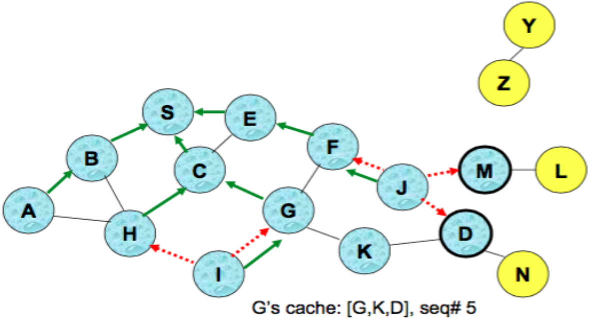


# Reverse Path Setup in AODV



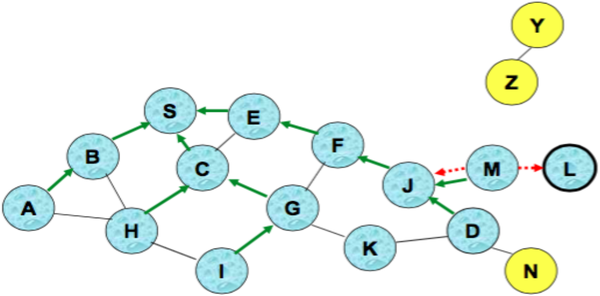

- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

# Reverse Path Setup in AODV



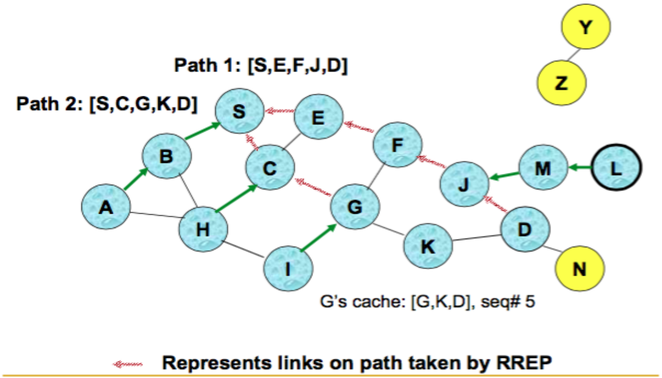

- **Node G does not forward RREQ, because node G has a cached path to D.**

# Reverse Path Setup in AODV




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

# Reverse Path Setup in AODV



# AODV Pros and Cons

- Advantages:
  - Smaller message size than DSR since full route is not transmitted to source
  - Lower connection setup time than DSR
- Disadvantages:
  - If source sequence number is low and intermediate nodes have higher numbers but old routes, stale routes can be used
  - Still have possible latency before data transmission can begin
  - Link break detection adds overhead

# AODV: Path Accumulation

- Combines the route information of DSR into AODV
- RouteRequest:
  - Upon receiving a RouteRequest message, a node will append its identifier to the header. The normal AODV procedure is then followed.
  - Intermediate nodes can change their table entries if a newer path, or lower hop count is detected in the header
- RouteReply:
  - A node will append its identifier to the header.
  - Intermediate nodes can change their table entries using the rule specified above.

# Zone Routing Protocol (ZRP)

- Hybrid, source-based
- Uses reactive inter-zone (IERP) and proactive intra-zone (IARP) routing protocols to maintain routes
- Nodes use intra-zone routing protocol to maintain local routing tables to neighbors
- Nodes use inter-zone routing protocol to communicate with nodes outside of their zone
- On link failure:
  - Intermediate nodes find alternate routes to the destination and inform the sender. Can result in sub-optimal paths.
  - Sender must restart the path-finding process to find a more optimal path.
- Nodes have radius zones for transmission. All nodes use the same radius for zones.

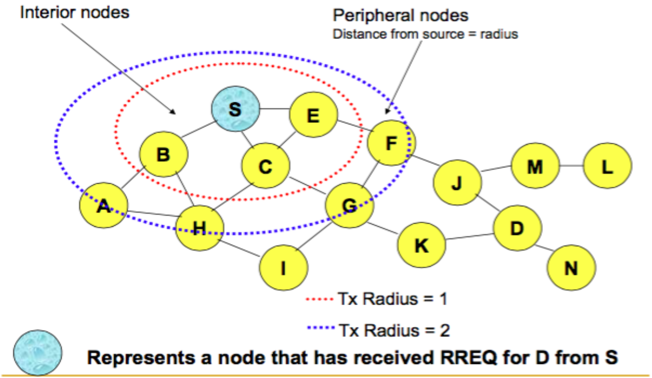
# ZRP

- To determine a route to a destination:
  1. If destination is in source's zone, direct delivery of data. Else, source broadcasts RouteRequest to all peripheral nodes of its zone
  2. If destination is in border node's zone, border node responds with RouteReply.
  3. Source forwards data to appropriate border node to reach destination.
- Nodes will only forward a RREQ into new areas of the network. This is done by listening to neighbor transmissions.

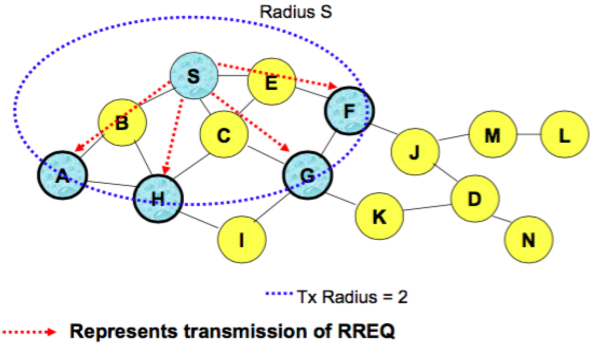
# ZRP

- To determine a route to a destination:
  1. If destination is in source's zone, direct delivery of data. Else, source broadcasts RouteRequest to all peripheral nodes of its zone
  2. If destination is in border node's zone, border node responds with RouteReply.
  3. Source forwards data to appropriate border node to reach destination.
- Nodes will only forward a RREQ into new areas of the network. This is done by listening to neighbor transmissions.

# Route Determination in ZRP

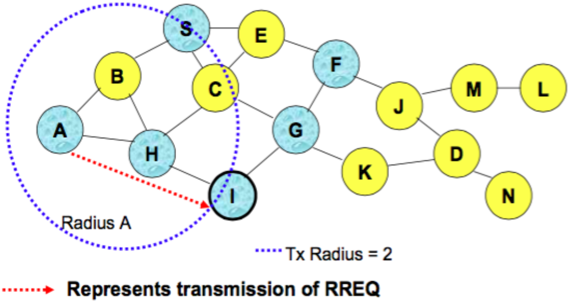


# Route Determination in ZRP

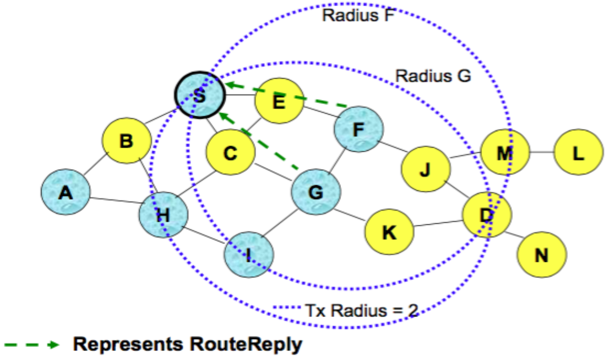


# Route Determination in ZRP

A does not send the RREQ to C because C is within S's routing zone
H does not forward the RREQ because all 2-hop neighbors are within S's routing zone

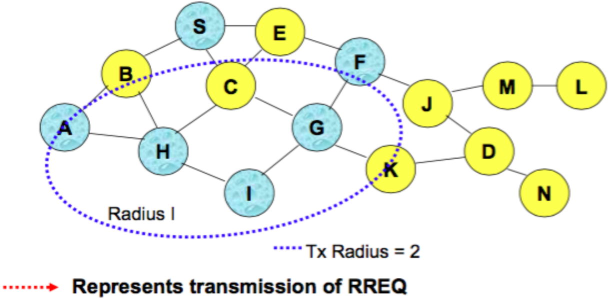


# Route Determination in ZRP

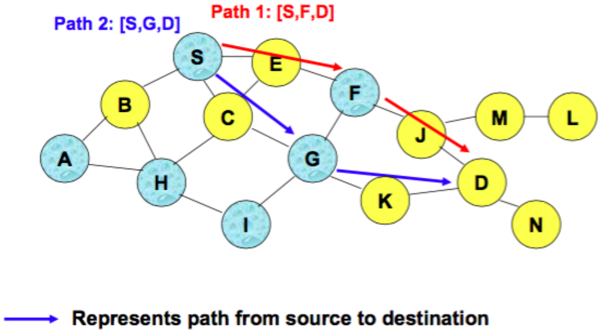


# Route Determination in ZRP

I does not forward the RREQ because it heard G and F receive the request



# Route Determination in ZRP



# ZRP Pros and Cons

- Advantages:
  - Theoretically reduces table maintenance inherent to proactive protocols
  - Theoretically reduces route determination delay inherent to reactive protocols
  - Can use single and multipath
- Disadvantages:
  - Realistically has higher overhead than proactive and reactive protocols
  - If zones greatly overlap, redundant RouteRequest messages are flooded through the network
  - Optimum zone radius must be determined for each situation
  - High stress for intermediate nodes on link failure

# Conclusion

- Many routing protocols exist
- Still much discussion over proactive vs. reactive approaches
- Much work still needs to be done because most research only answers part of the questions
- Need a better way to contrast and compare all available routing protocols