CCN

Infrastructure less Networks: Network Layer Routing Protocols

Credits and Acknowledgement

- Many of the slides for this lecture series are copied directly from Prof. CUI Yong's and Dr. Ali Khayam's lecture slides.

Outline

- Introduction
- MANET Routing Overview and Background
- MANET Routing Protocol Design
  - Reactive protocols
  - Proactive protocols
  - Hybrid protocols
- Conclusion

Network Layer in Infrastructure Wireless LANs

- In an infrastructure wireless LAN, all packets are routed through the access point

- Consequently, routing is trivial and the Internet Protocol (IP) is generally used by infrastructure clients

Network Layer in Infrastructure Wireless LANs

For a Single Basic Service Set

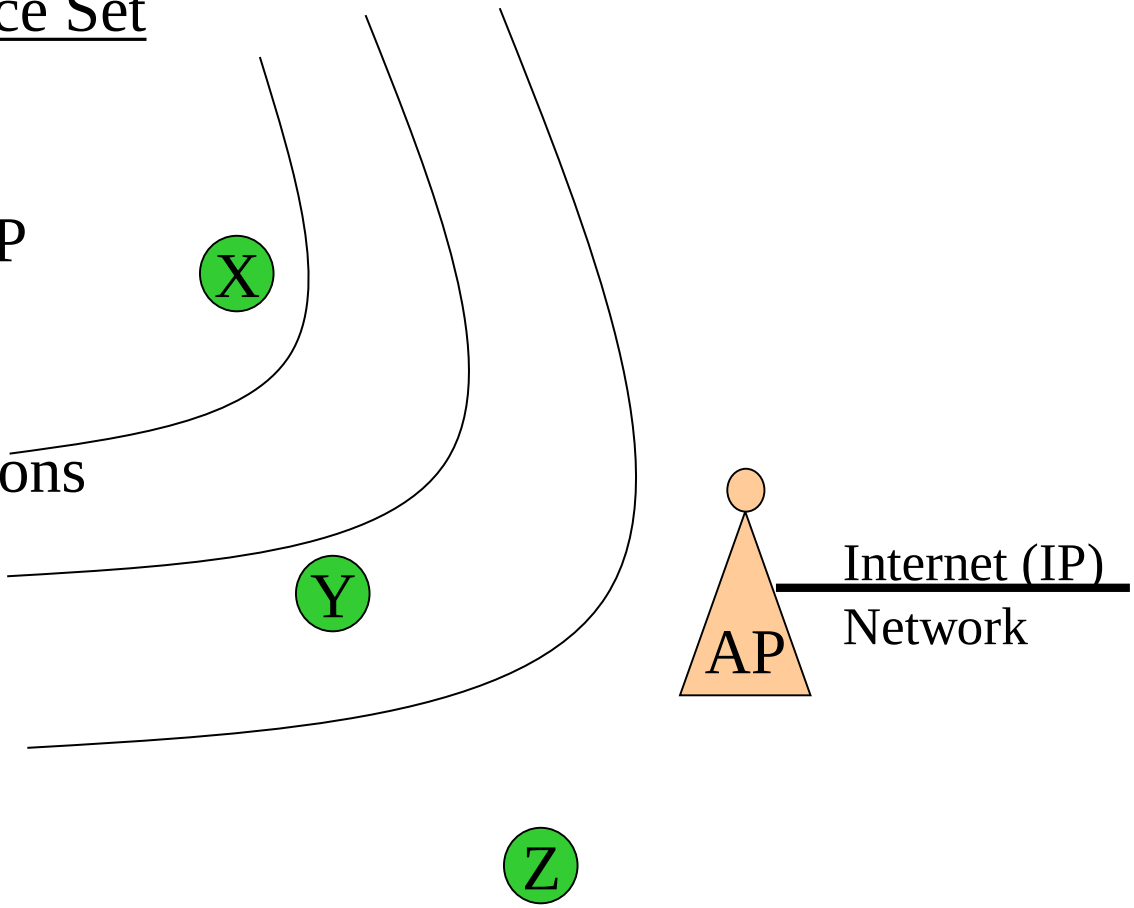
X wants to talk to Z

X sends its data to the AP

AP sends it to Z

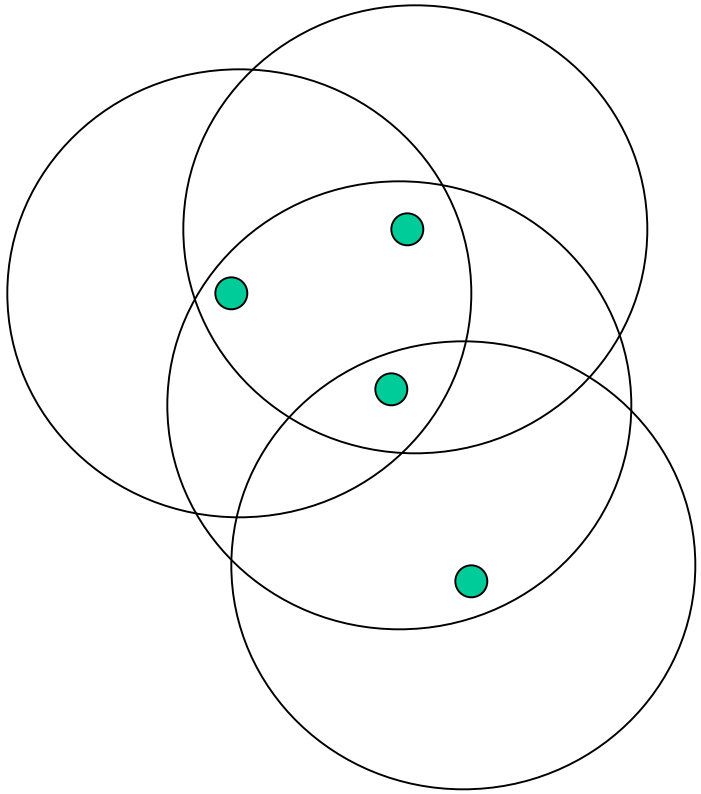
Only MAC layer operations

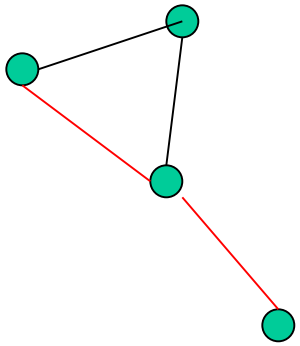
No routing needed



Network Layer Challenges

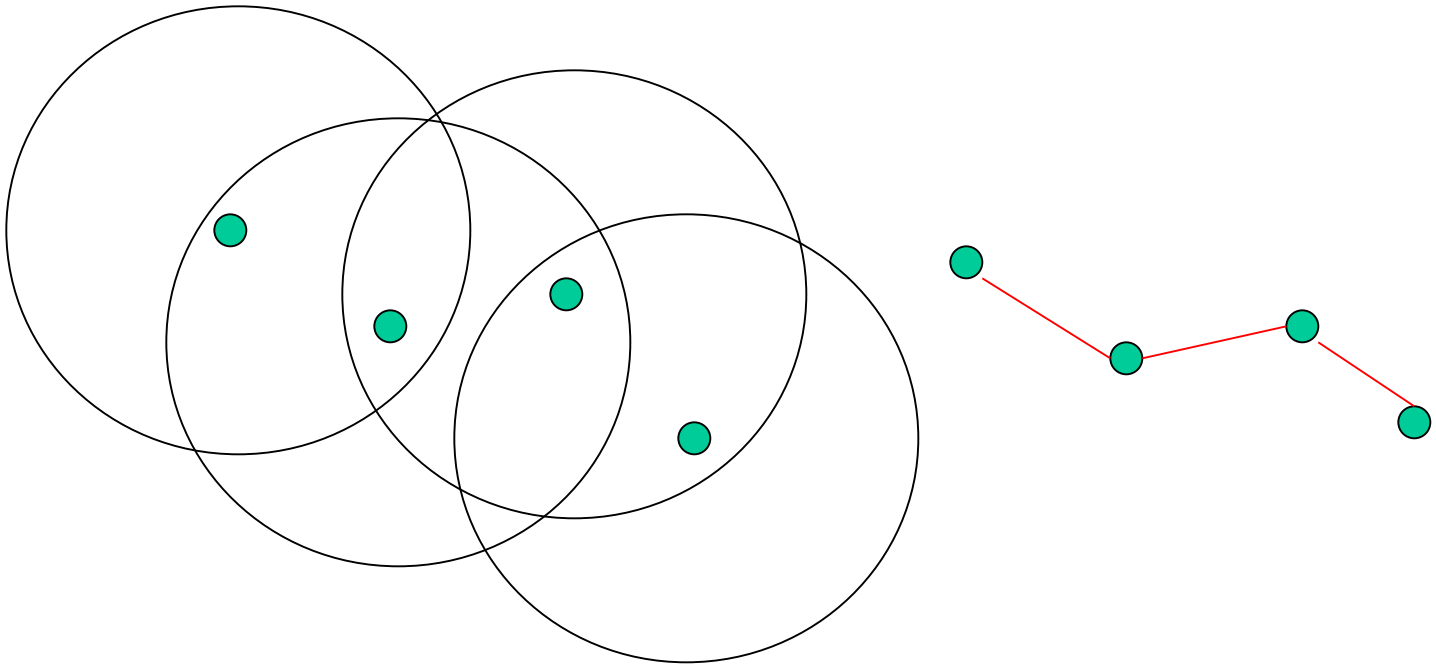
- Traverse multiple links to reach a destination





Network Layer Challenges

- Mobility causes route changes



Network Layer Challenges

- **Host mobility**
  - link failure/repair due to mobility may have different characteristics than those due to other causes
- **Instability**
  - Rate of link failure/repair may be high when nodes move fast
- **New performance criteria needed**
  - route stability despite mobility (Routes have to be discovered without any centralized control)
  - energy consumption (energy limitations)

Network Layer Challenges

- **Proposed protocols**
  - Some have been invented specifically for MANET
  - Others are adapted from older protocols for wired networks
- **No single protocol works well**
  - some attempts made to develop adaptive protocols
- **Bandwidth Limitations:**
  - Wireless bandwidth is scarce
- **Shared Medium:**
  - Channel contention and collisions can introduce significant delays

Network Layer Challenges

- A fundamental assumption in all infrastructure less network routing protocols is that all nodes are **cooperative.**
- These cooperative nodes route packets for each other.
- Thus each MANET node acts as a router.

Classification of Routing protocols

- Can be classified into several types based on different criteria
- The classification is not mutually exclusive and some protocols fall in more than one class.

Types of MANET

- In MANET, routing algorithms can be classified into three broad categories:
  - Reactive Algorithms
  - Proactive Algorithms
  - Hybrid Algorithms

Types of Protocols

- **On-demand/reactive**
  - the routes are determined when they are required by the source using a route discovery process;

- In Reactive Protocols, a route is established only when it is needed

- That is, a route between two nodes is established in reaction to one of the node's desire to communicate with the other node

- Also referred to as on-demand routing protocols

Types of Protocols

- The main advantage of reactive routing protocols is the relatively low overhead messaging for route establishment

- The main disadvantage is the route establishment latency when a node needs to communicate with another node

Types of Protocols

- Reactive/ On demand routing is appropriate for networks with:
  - Scalable size
  - High mobility
  - Relatively low communication rates

Types of Protocols

- **Global/proactive**
  - determine routes to all the destinations at the start up
  - maintain by using periodic route update process;

- In Proactive Algorithms, routes are maintained even when there is no communication between two nodes

- So a route is always available when two nodes need to communicate

- Distance Vector and Link State Routing Algorithms are proactive

Types of Protocols

- The main advantage of Proactive routing is no route setup latency
- The main disadvantage is the high maintenance overhead when many of the routes are never used

Types of Protocols

- Proactive routing is appropriate for networks with:
  - Small size
  - Low mobility
  - High communication rates

Types of Protocols

- **Hybrid**
  - combine the basic properties of the first two classes of protocols into one.

- Different deployment configurations are possible:
  - The network switches between the two (reactive and proactive) routing techniques.
  - Parts of the network employ reactive routing, while other parts use proactive routing

- Hybrid protocols should dynamically expand/contract the scope of reactive and proactive algorithms based on network and traffic characteristics

Types of Protocols

- The main advantage of hybrid protocols is the combination of reactive and proactive algorithms
- The disadvantages or challenges include:
  - Continuous and real-time measurement of network and traffic characteristics
  - Network reconfiguration in response to changing network and traffic characteristics

Routing Choice

- The choice of a routing algorithm should be based on:
  - Number and types of nodes in the network
  - Network Topology
  - Mobility Speeds and Patterns
  - Application-specific requirements: QoS, bandwidth, reliability, etc.

- A large number of routing algorithms have been proposed in the last twenty years

- In this part, we will discuss some examples of these algorithms

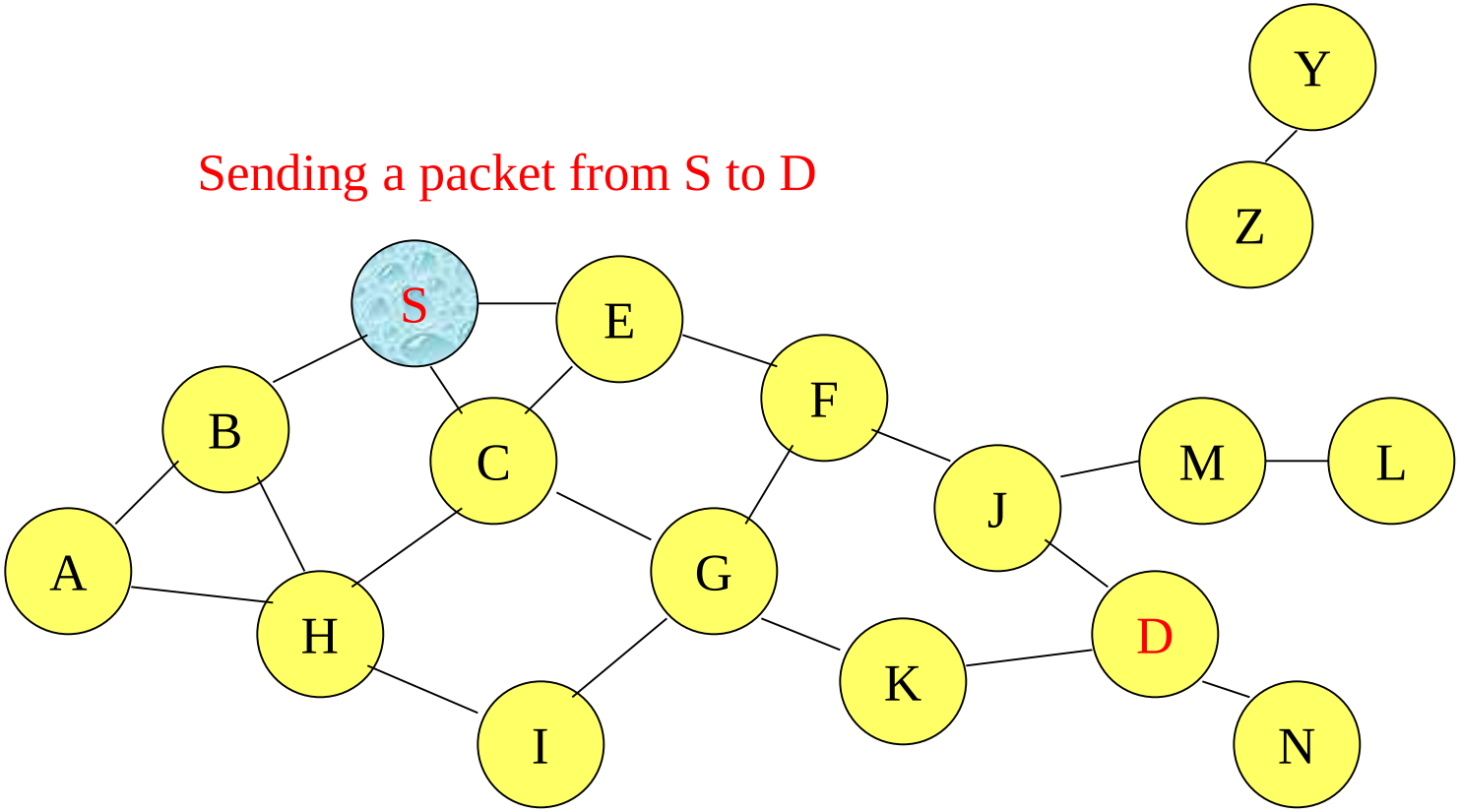
How to send msg to destination

- Routing
  - Reactive
  - Proactive
- No routing in advance?
  - Any simple solutions?

Flooding for Data Delivery

- 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

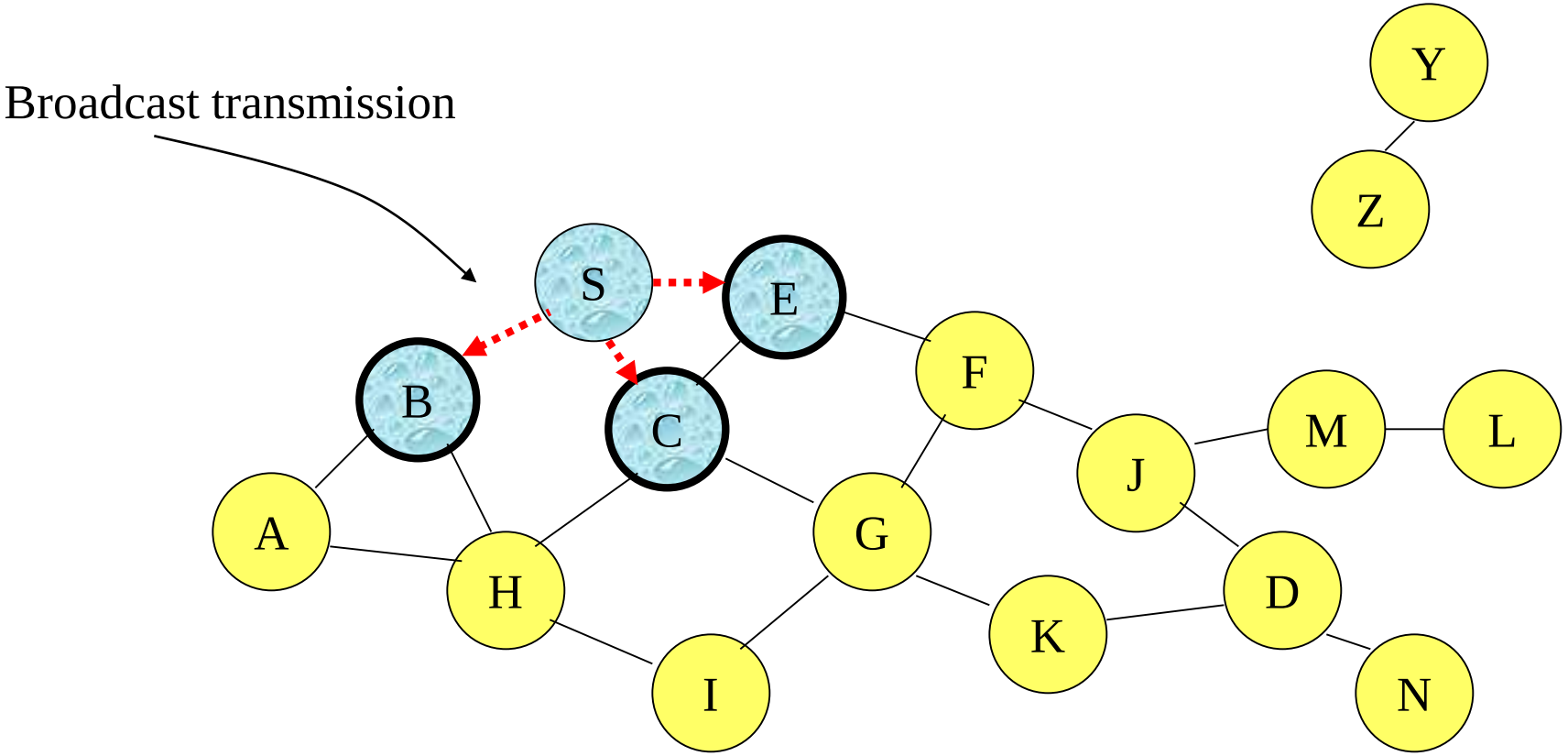
Flooding for Data Delivery



Represents a node that has received packet P

Represents that connected nodes are within each other's transmission range

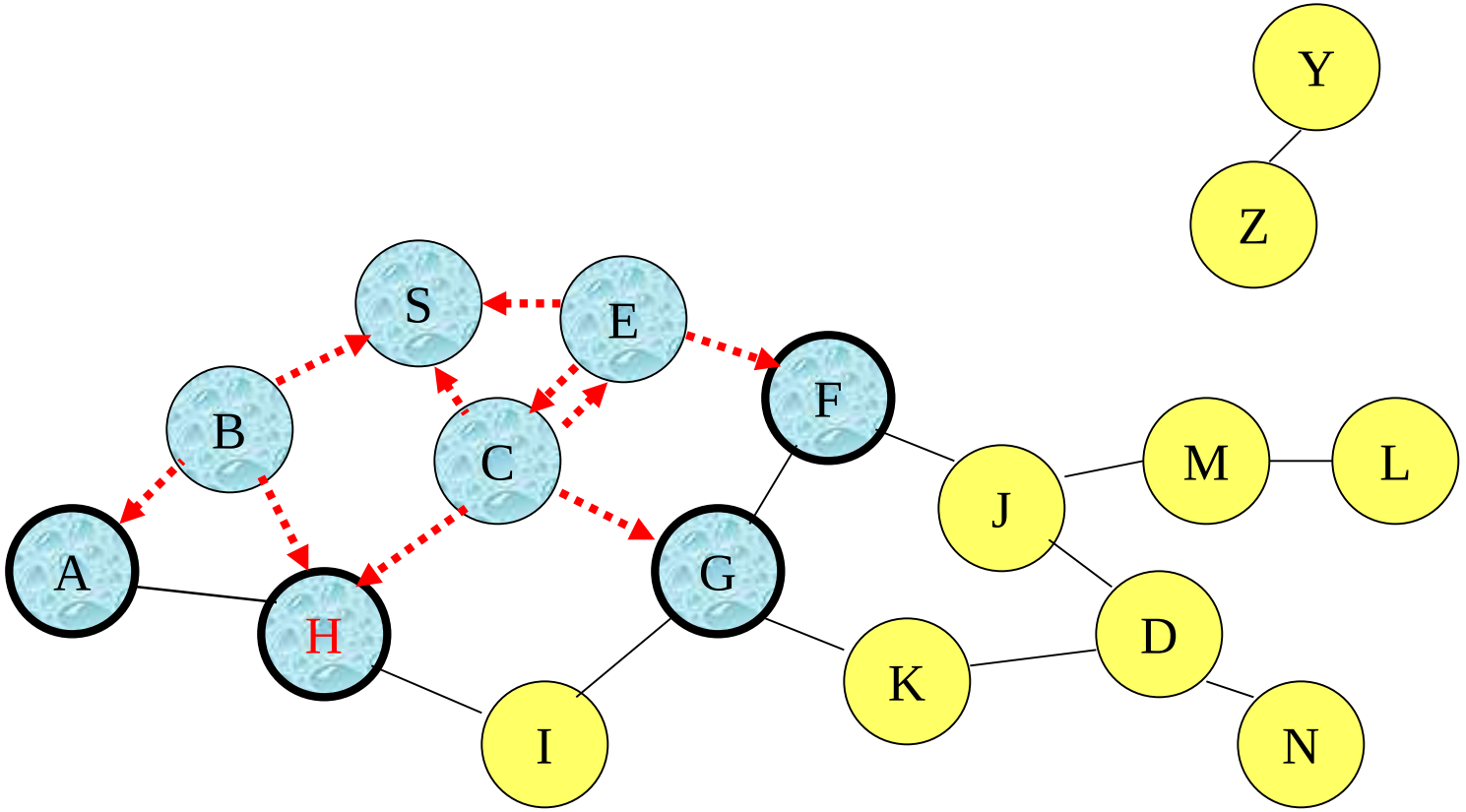
Flooding for Data Delivery



Represents a node that receives packet P for the first time

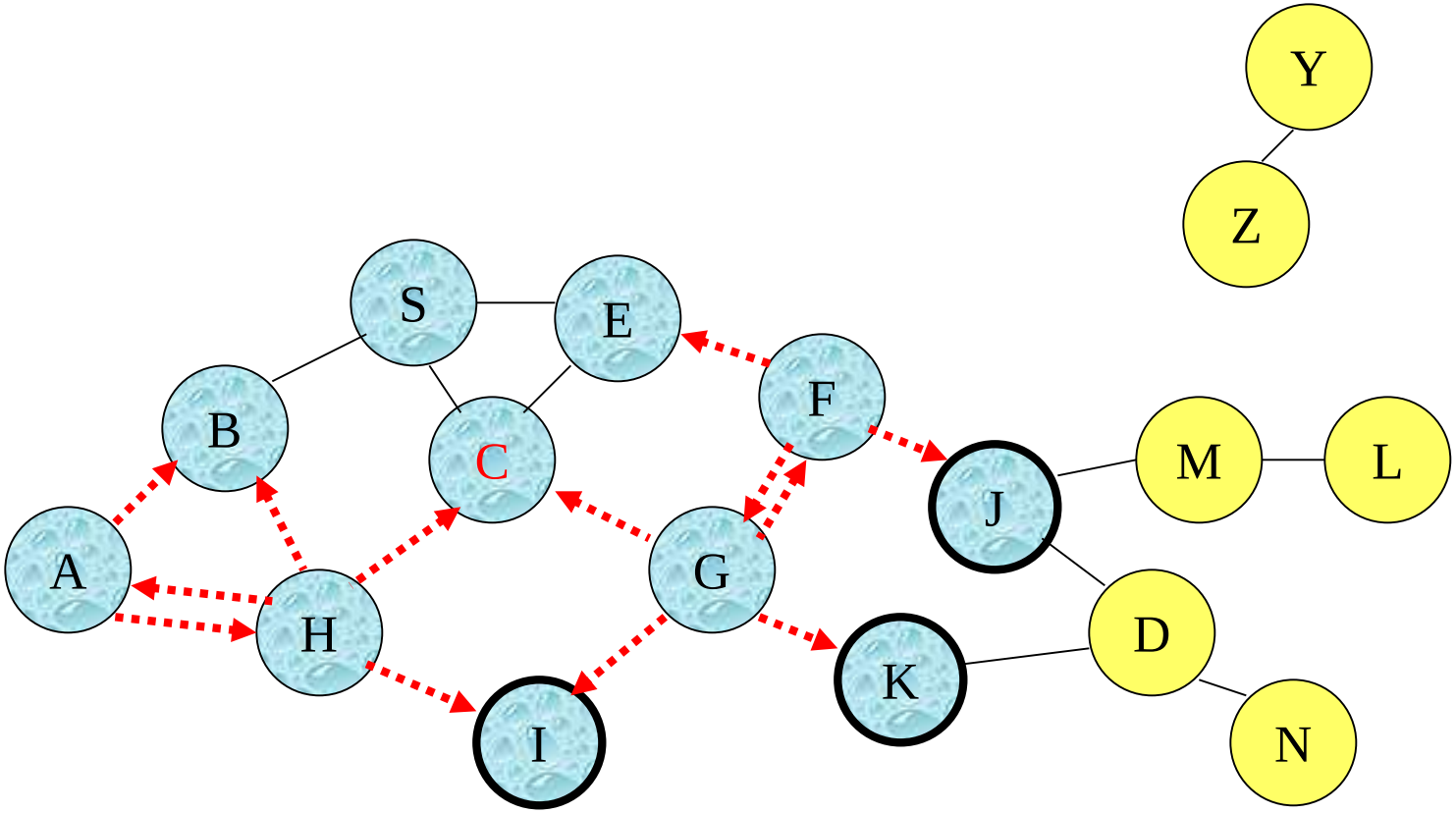
Represents transmission of packet P

Flooding for Data Delivery



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

Flooding for Data Delivery

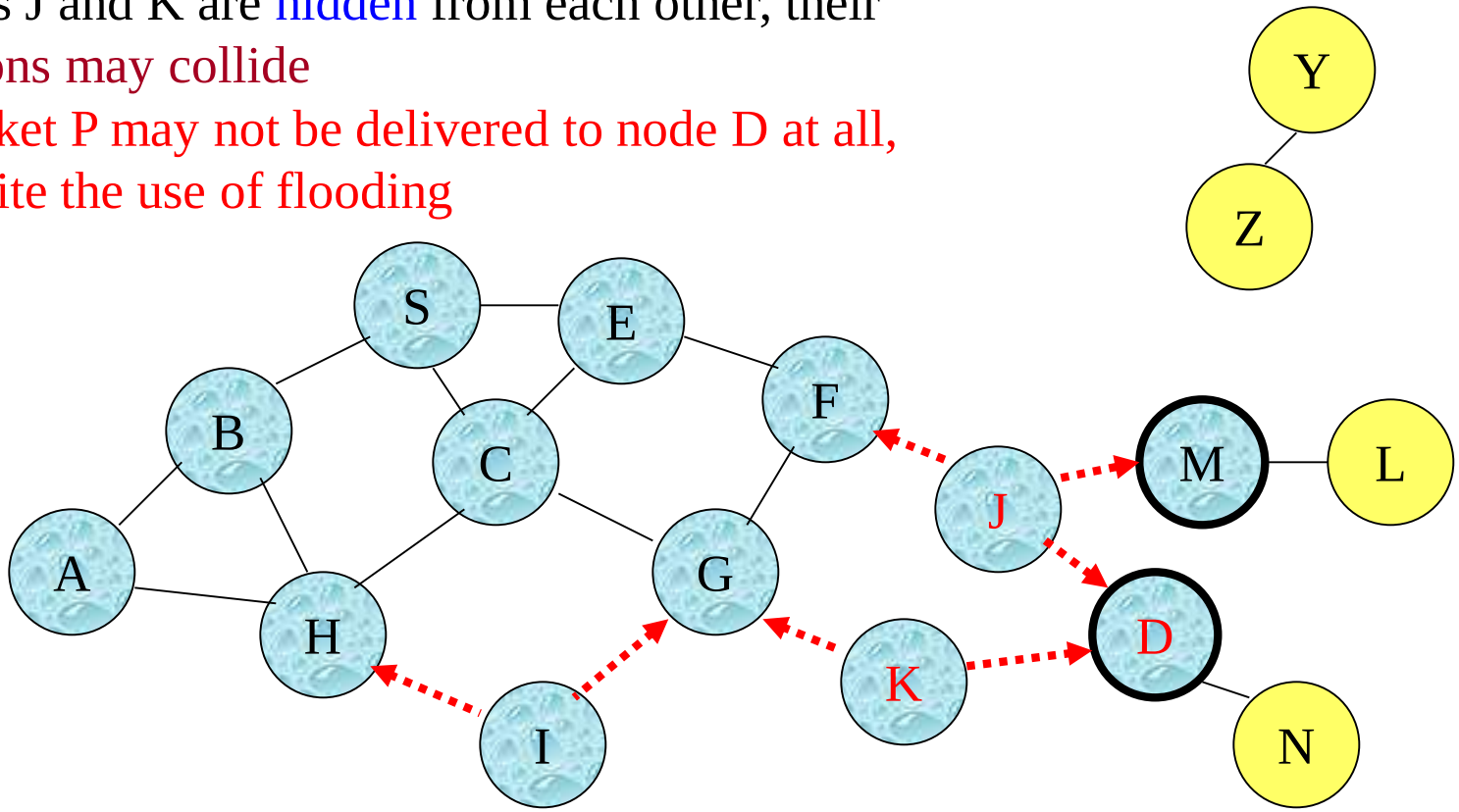


- Node C receives packet P from G and H, but does not forward it again, because node C has already forwarded packet P once

Flooding for Data Delivery

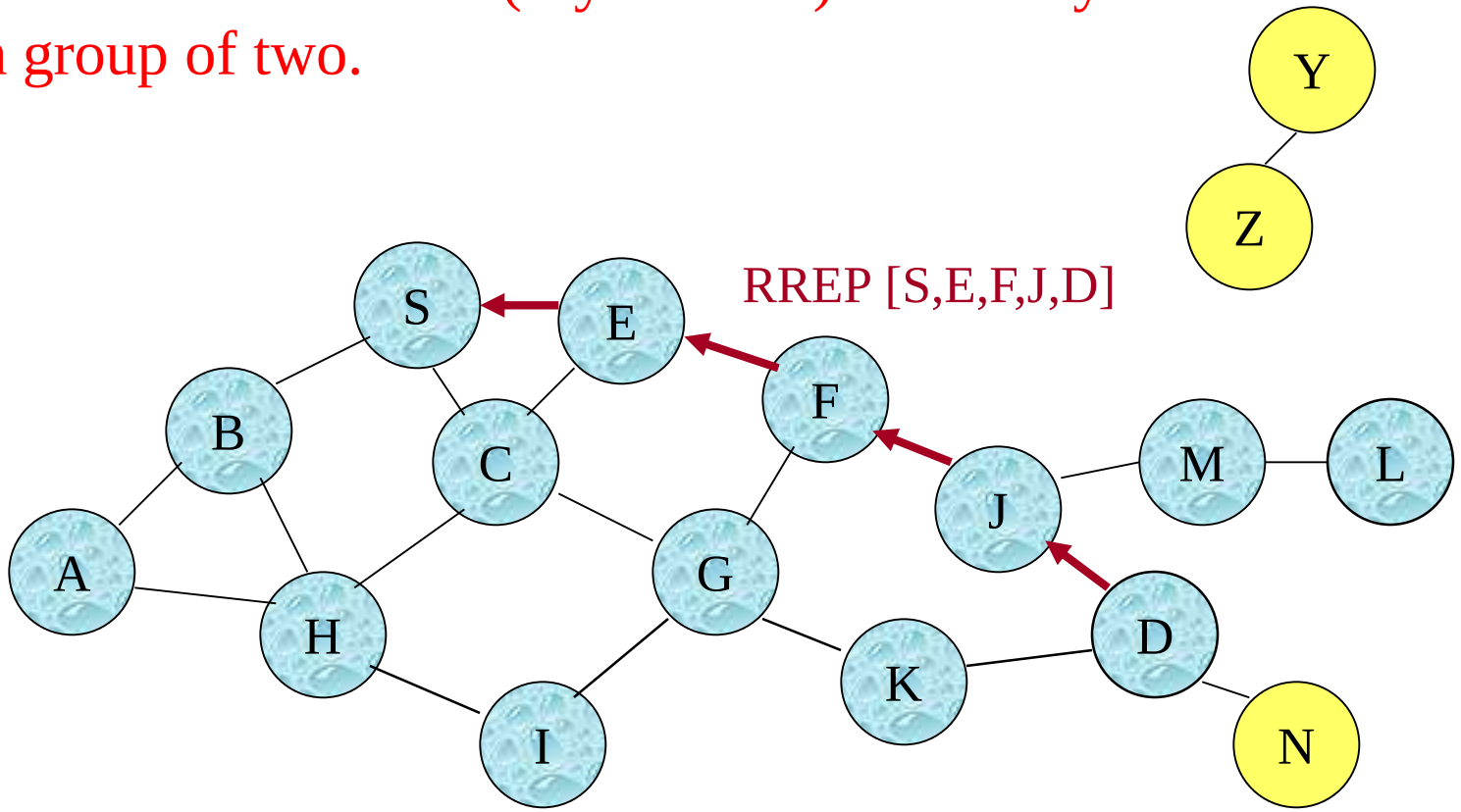
- Nodes J and K both broadcast packet P to node D
- Since nodes J and K are hidden from each other, their transmissions may collide

  => Packet P may not be delivered to node D at all, despite the use of flooding



Route Reply in DSR

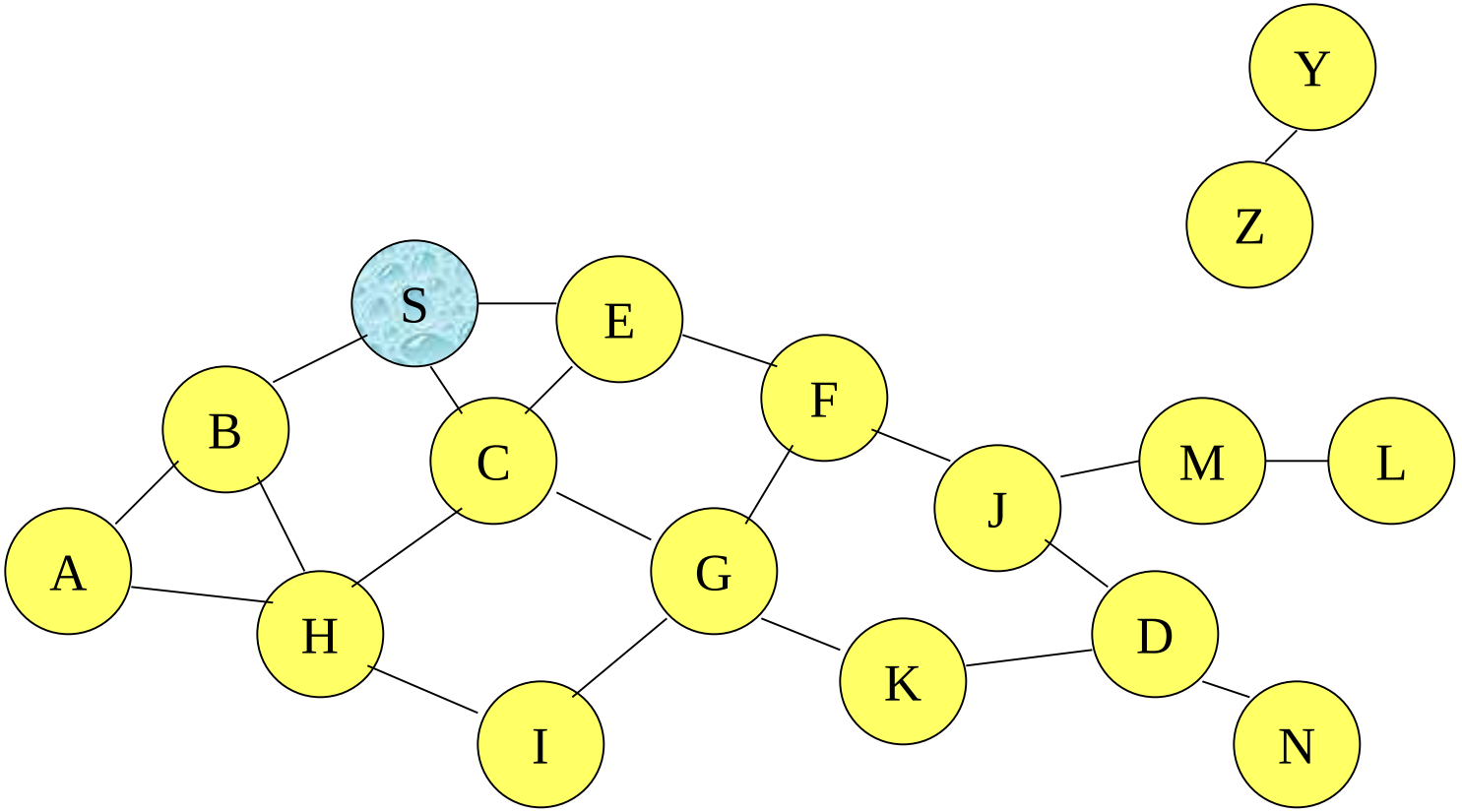
How to do on unidirectional (asymmetric) links? Try to find in group of two.



Represents RREP control message

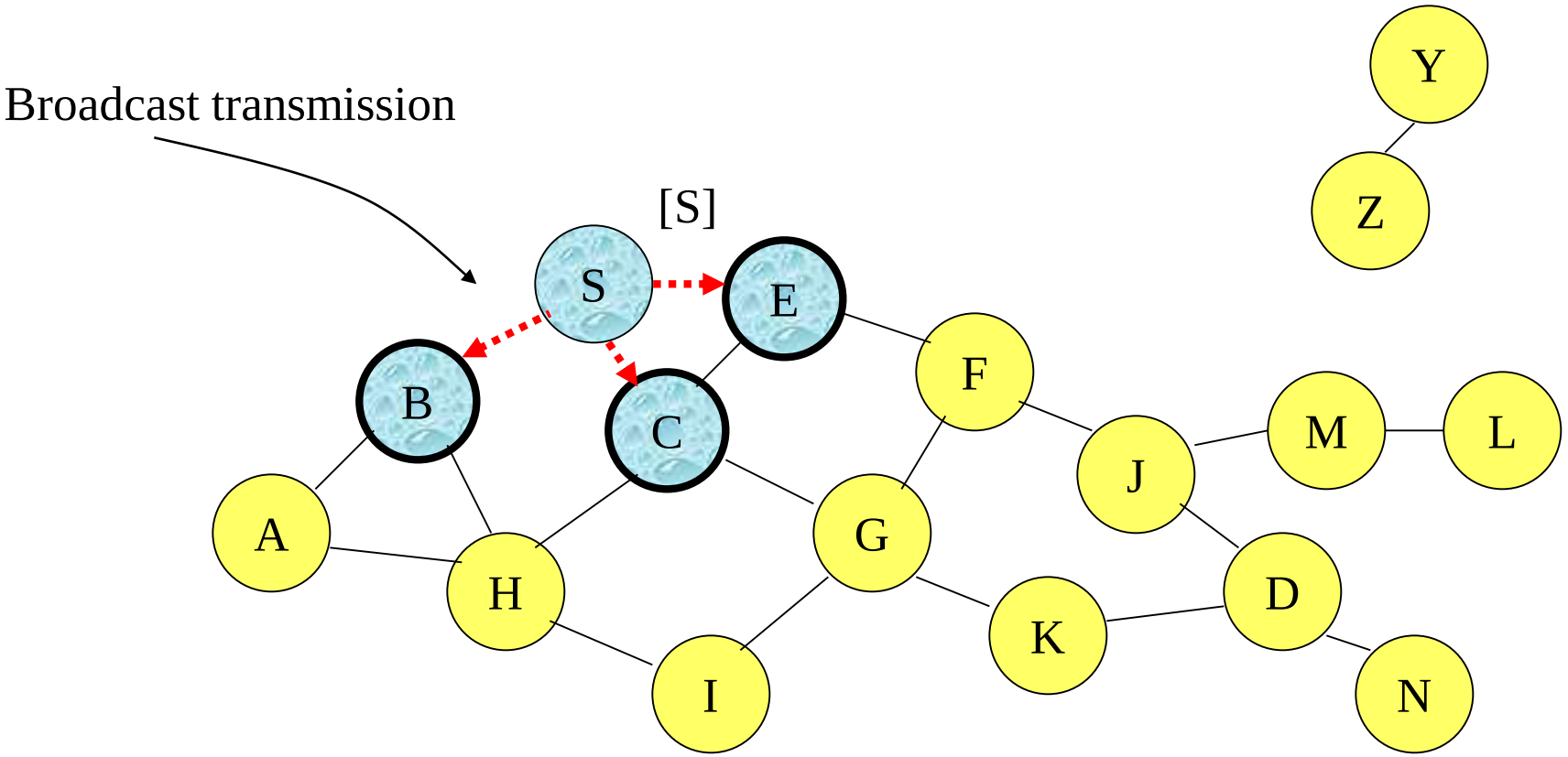
- Three steps in DSR
  - Route Discovery
  - Data Delivery
  - Route maintenance
- Route Discovery
  - When node S wants to send a packet to node D, but does not know a route to D, node S initiates a route discovery
  - Source node S floods Route Request (RREQ)
  - Each node appends own identifier when forwarding RREQ

Route Discovery in DSR



Represents a node that has received RREQ for D from S

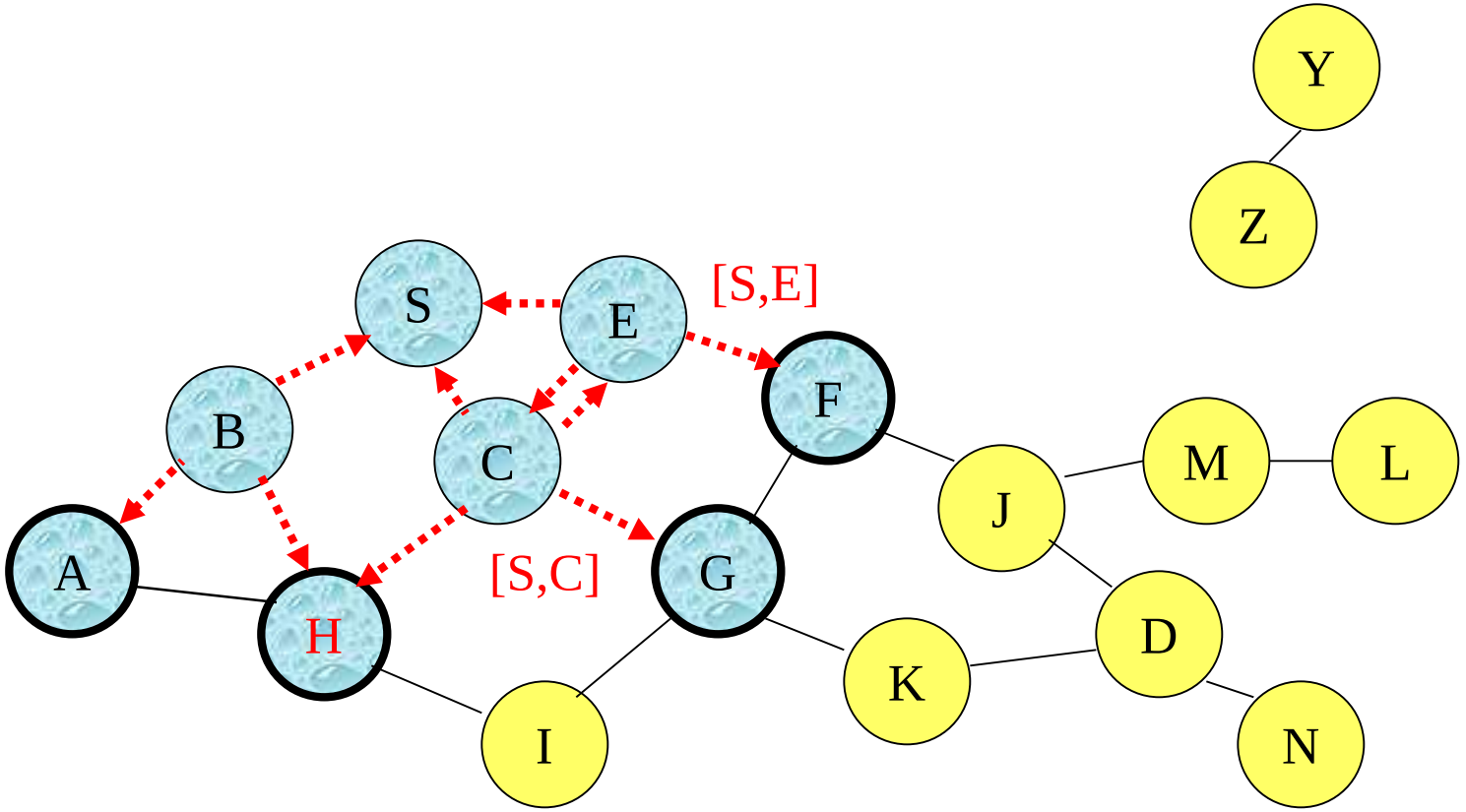
Route Discovery in DSR



Represents transmission of RREQ

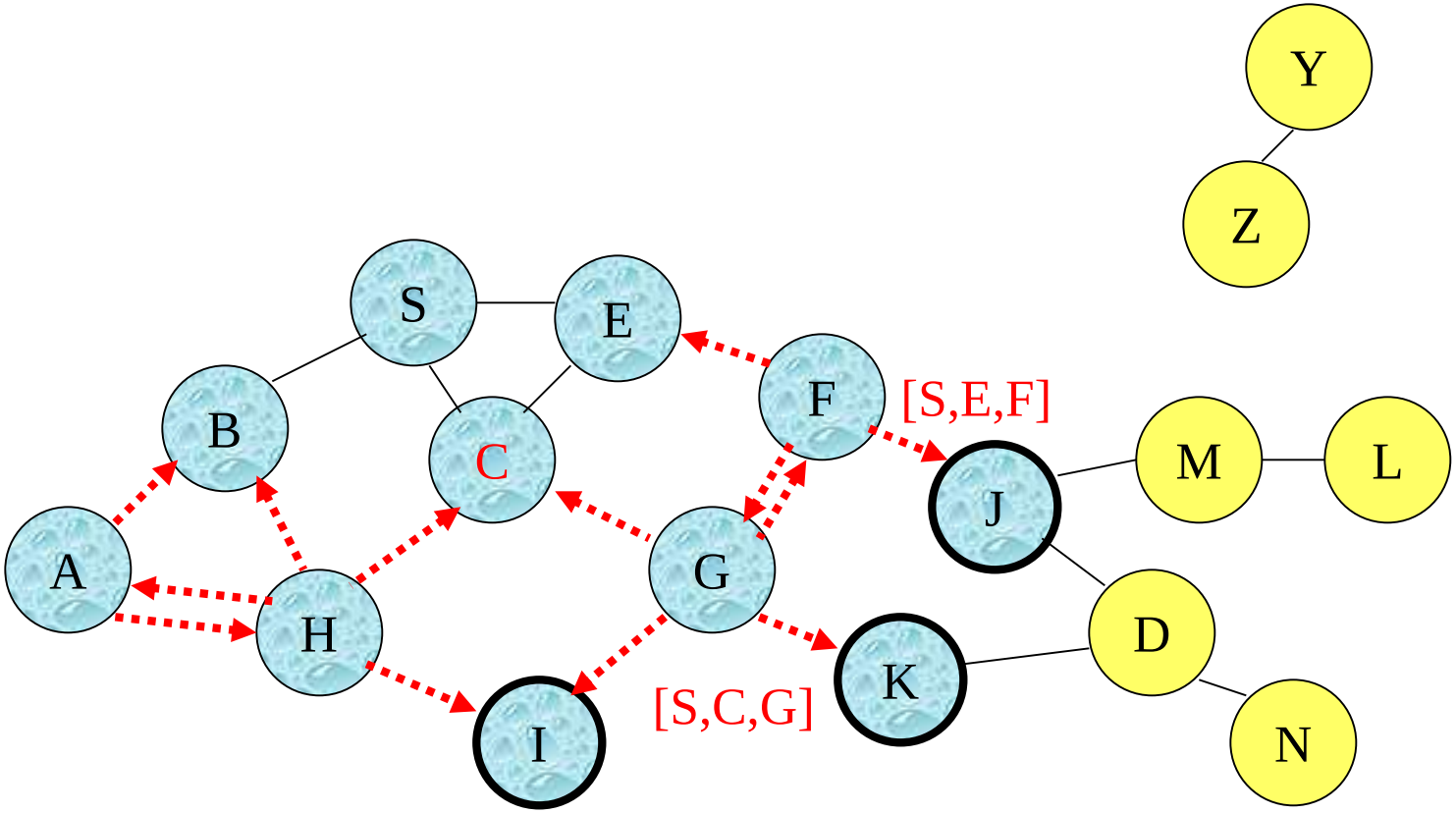
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



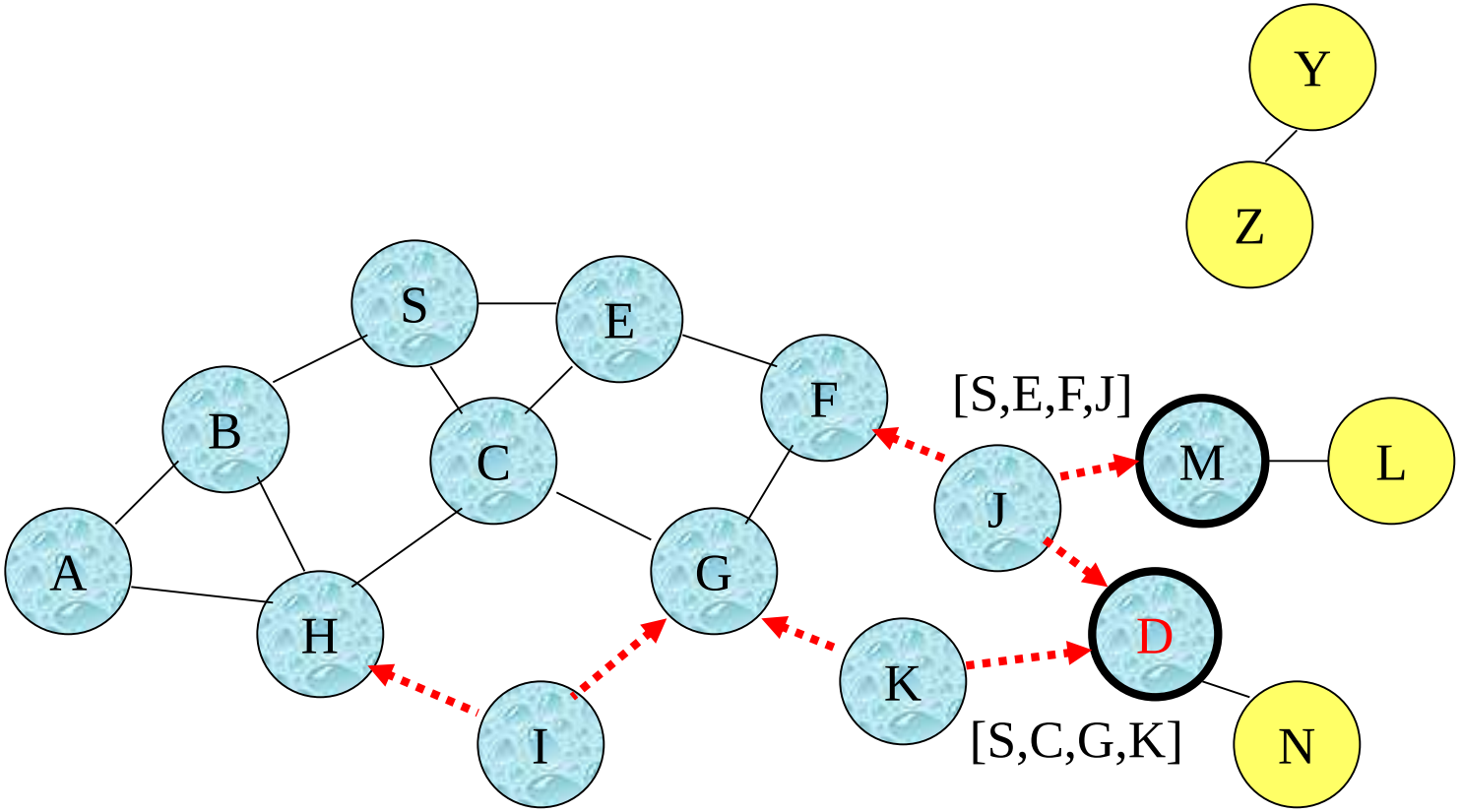
- Node H receives packet RREQ from two neighbors:
  potential for collision

Route Discovery in DSR



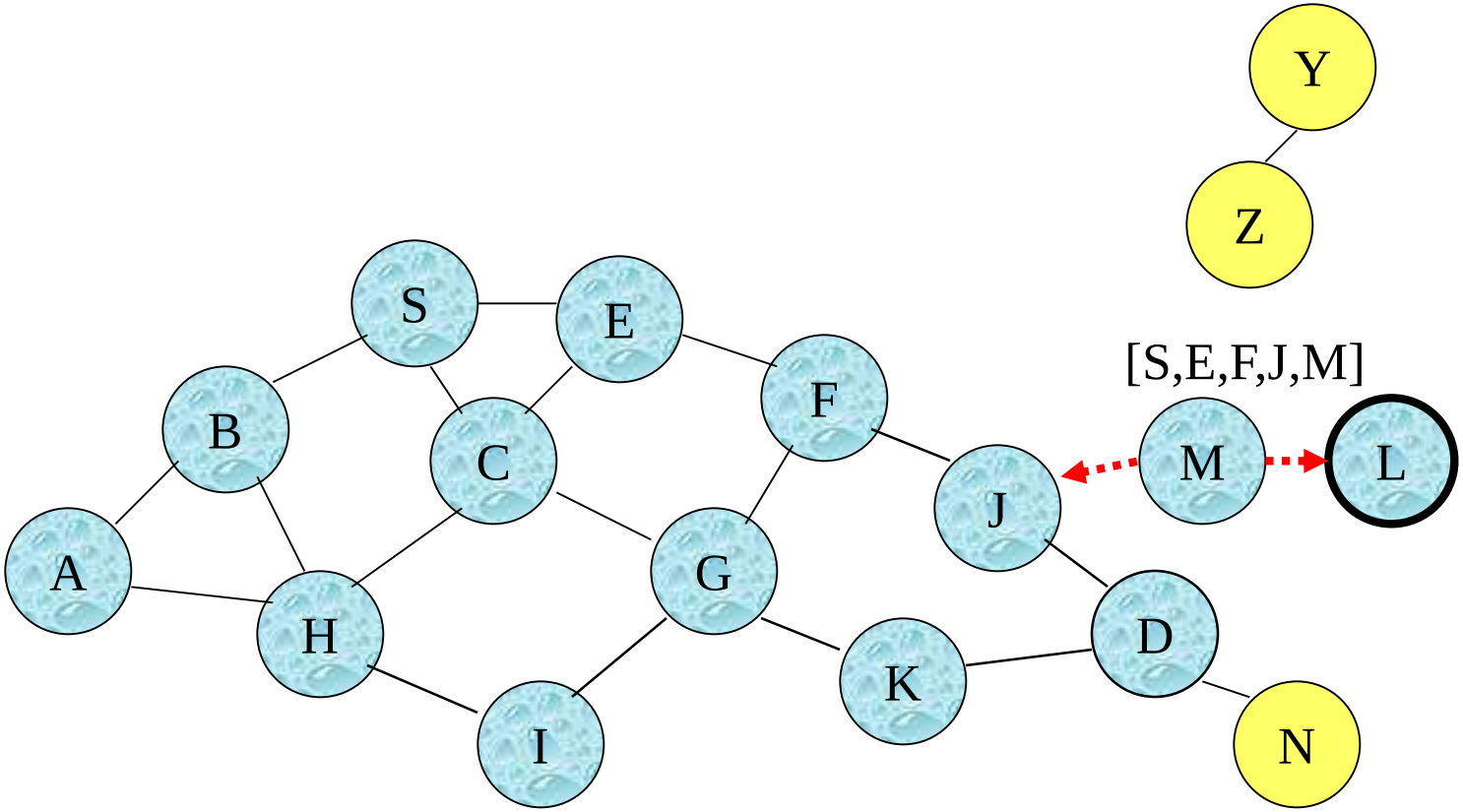
- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

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

NUST

Route Discovery in DSR

- 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

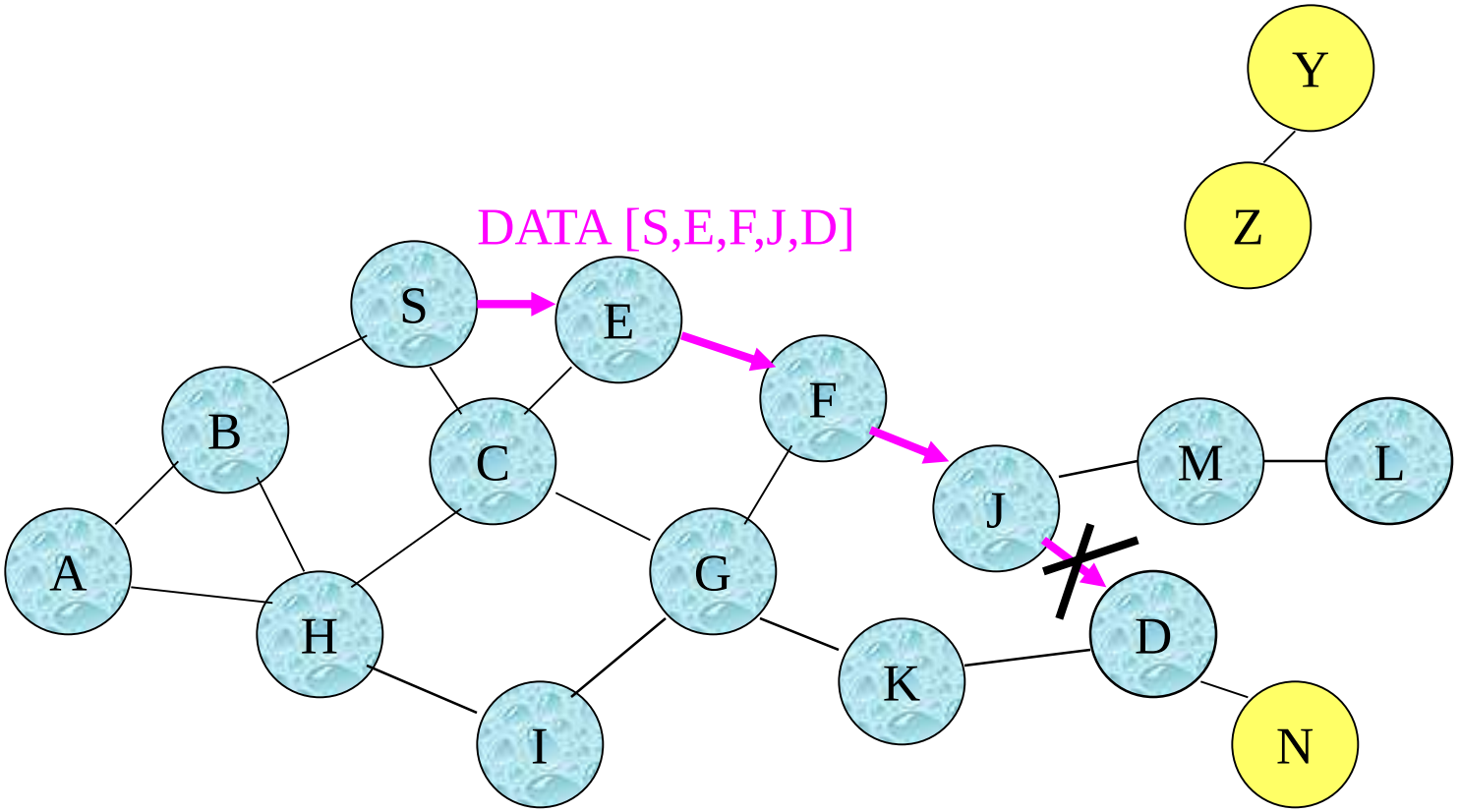
Route Reply in DSR

- 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 this is reliable?? If the path maintained is node/edge disjoint??? How can we make it reliable?? Does the reliability have any impact on overhead?? What happens to reliability if we, instead of node-disjoint, we discover partially-disjoint paths?
- 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)

Dynamic Source Routing (DSR)

- Three steps in DSR
  - Route Discovery
  - Data Delivery
  - Route maintenance
- Data delivery
  - 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

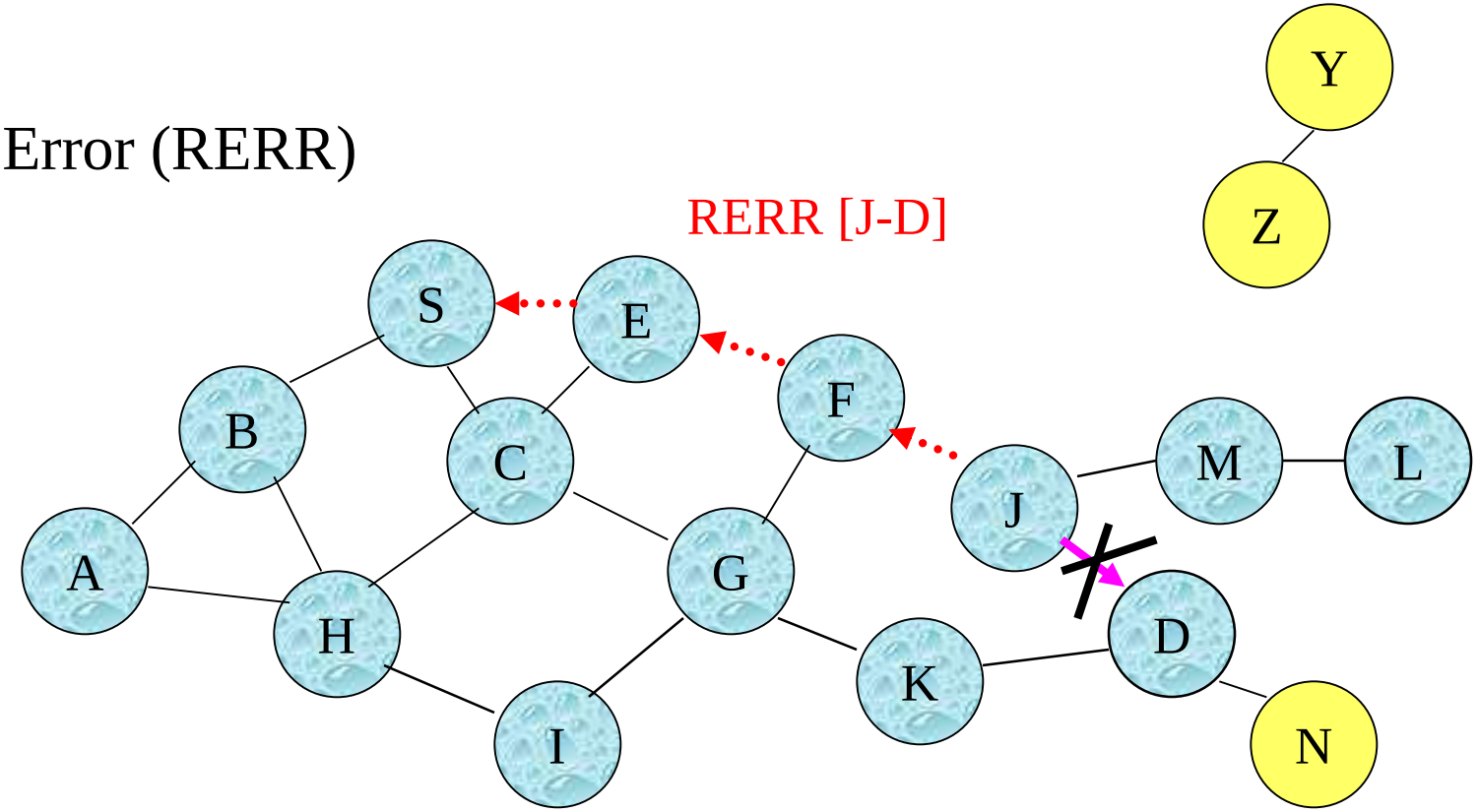
Data Delivery in DSR



- **Any problem?**
  - **Packet header size grows with route length**
  - **Route failure may occur**
    - **Who should recover the failure?**

NUST

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