Part C
Ah hoc networks

Acknowlegments

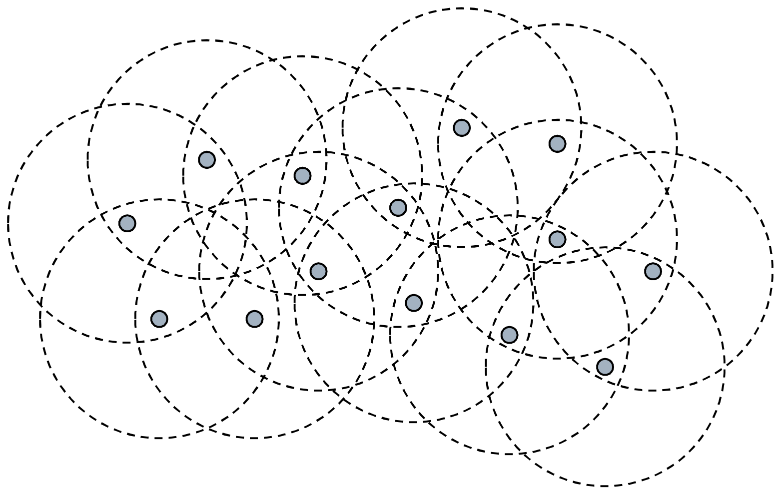
- This class notes are mostly based on the teaching material of:
  - Prof. Eylem Ekici (Ohio State University at Columbus)
  - Prof. Nitin H. Vaidya (University of Illinois at Urbana-Champaign)

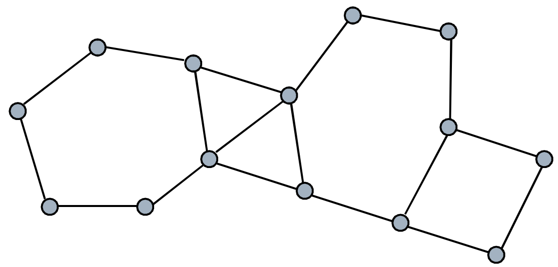
Introduction

- Mobile Ad Hoc Networks (MANET):
  - Networks of potentially *mobile network nodes*
  - Nodes equipped with wireless communication interfaces
  - No pre-established infrastructure
  - Communication between peers involve multiple hops
- Implications
  - Nodes act both as *hosts* as well as *routers*
  - Dynamic network topology

Ad Hoc Network Abstractions

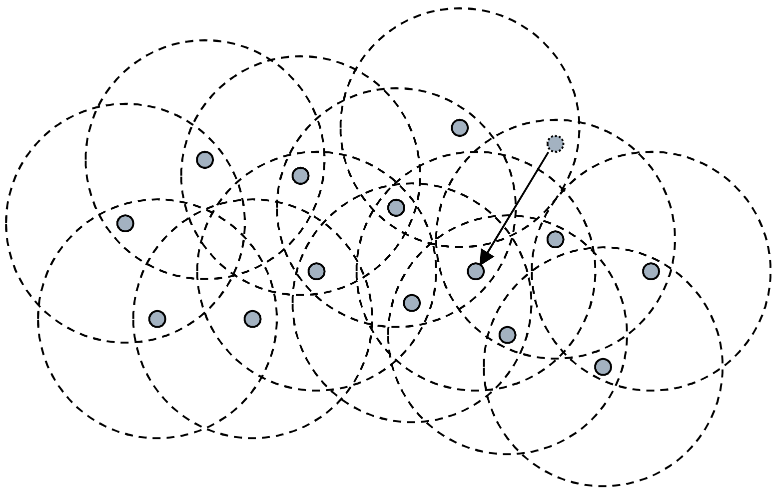
- Every node can communicate directly with a subset of mobile nodes (*neighbors*)
  - Communication "range" of a node varies depending on physical changes
  - Communication range abstracted as circles

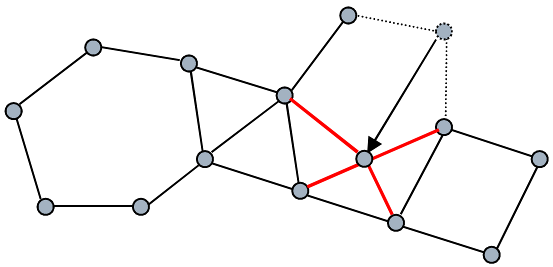




Mobile Ad Hoc Networks

- Mobility causes topology changes
  - Topology changes lead to changes in data delivery decisions
  - Introduces real-time adaptation requirements





Example Applications

- Disaster recovery, emergency, security applications
  - Law enforcement
  - Natural and man-made disaster recovery
- Civilian applications
  - Conference room networks
  - Networking in large vessels
  - Personal area networks
  - Vehicular networks
- Military applications
  - Ground-based battlefield networks
  - Hybrid platform networks (land, air, and sea based)

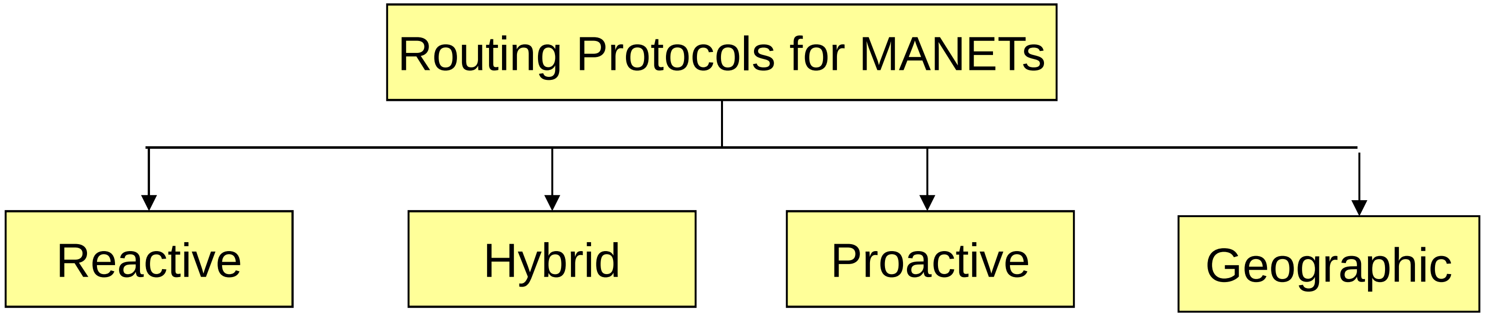
Problems to Address

- Physical layer
  - Range, symmetry, power control…
- MAC layer
  - Hidden terminal problem, asymmetrical links, error control, energy efficiency, fairness
- Network layer
  - Point-to-point, point-to-multi-point, flat, hierarchical, proactive, reactive, hybrid, mobility-tailored
- Transport layer
  - Packet loss discrimination, intermediate buffering

Introduction to routing

- Routing in ad hoc networks should account for host mobility, which leads to *dynamic topologies*
- Routing protocols designed for static (or slowly changing) networks
  - May not keep up with the rate of change
  - Waste limited resources
  - May not cater to specific performance criteria such as energy consumption
- As usual, no single protocol is optimal for all ad hoc network types and conditions

Protocol Classification



- Reactive Protocols
  - Determine the paths on-demand
- Proactive Protocols
  - Maintain paths regardless of traffic conditions
- Hybrid Protocols
  - Generally maintain local paths proactively, and create large scale paths reactively
- Geographic Protocols
  - Based on geographical location of nodes

Protocol Classification

- Reactive Protocols
  - Generally involve large delays between the request and first packet delivery
  - Incur low overhead in low traffic scenarios
- Proactive Protocols
  - Packets are immediately delivered as paths are already established
  - Results in high path maintenance overhead since the paths are kept regardless of traffic patterns
- Hybrid Protocols
  - Operate midway of delay and overhead performance
- Geographic Protocols
  - Can be used only when location information is available

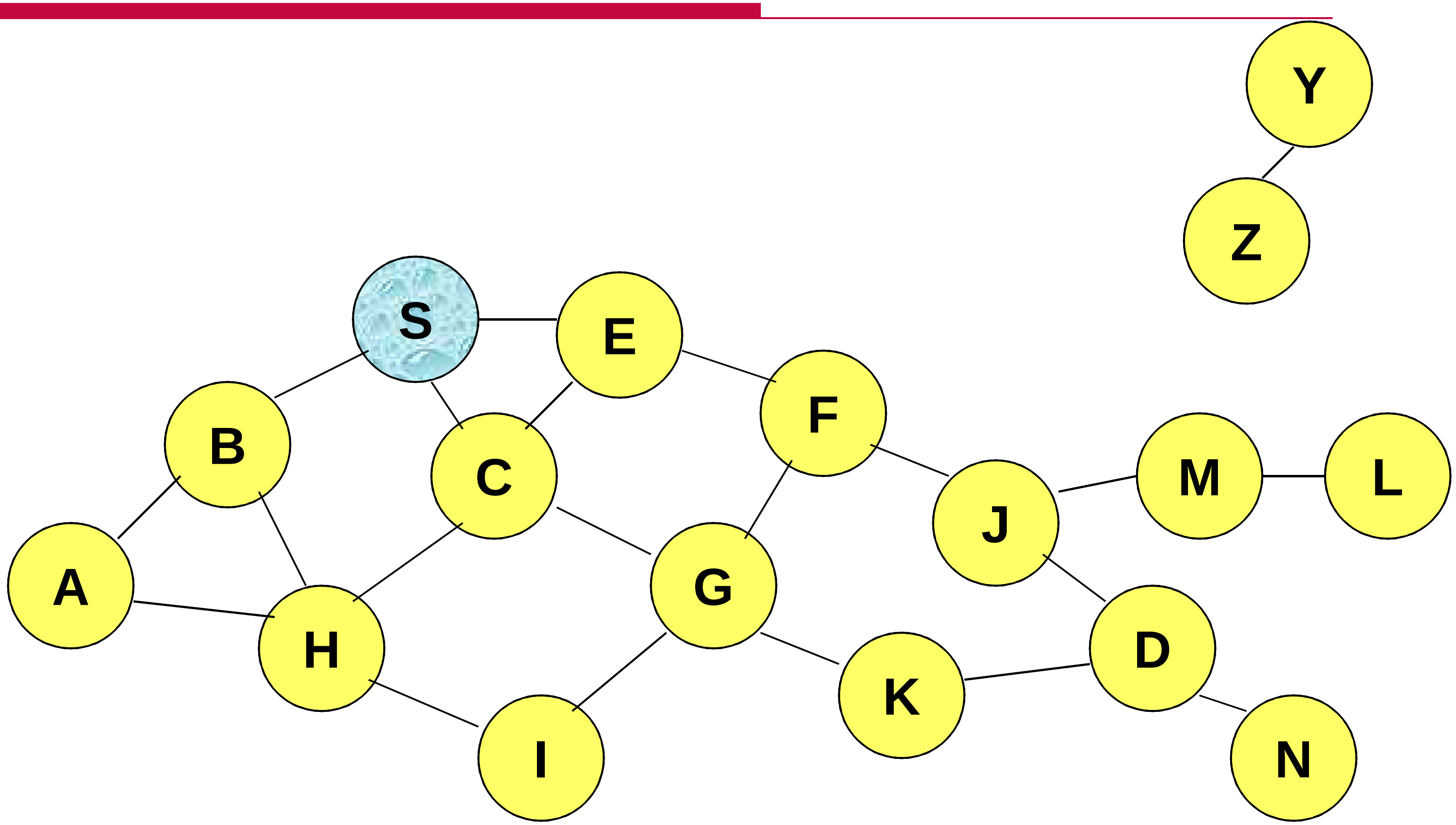
Trade-Off

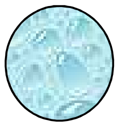
- Latency of route discovery
  - Proactive protocols may have lower latency since routes are maintained at all times
  - Reactive protocols may have higher latency because a route from X to Y will be found only when X attempts to send to Y
- Overhead of route discovery/maintenance
  - Reactive protocols 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 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

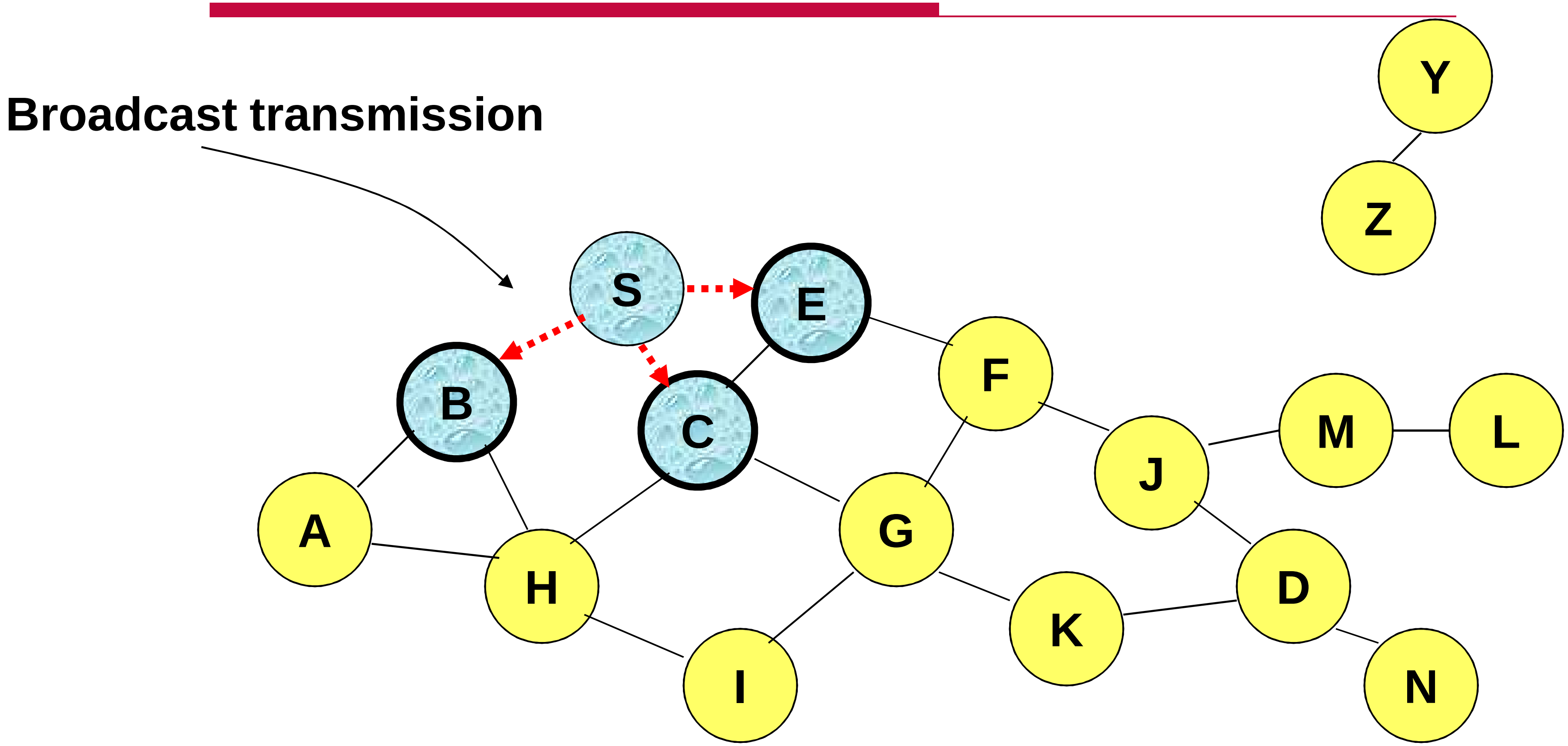


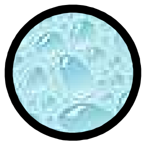


Represents a node that has received packet P

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

Flooding for Data Delivery

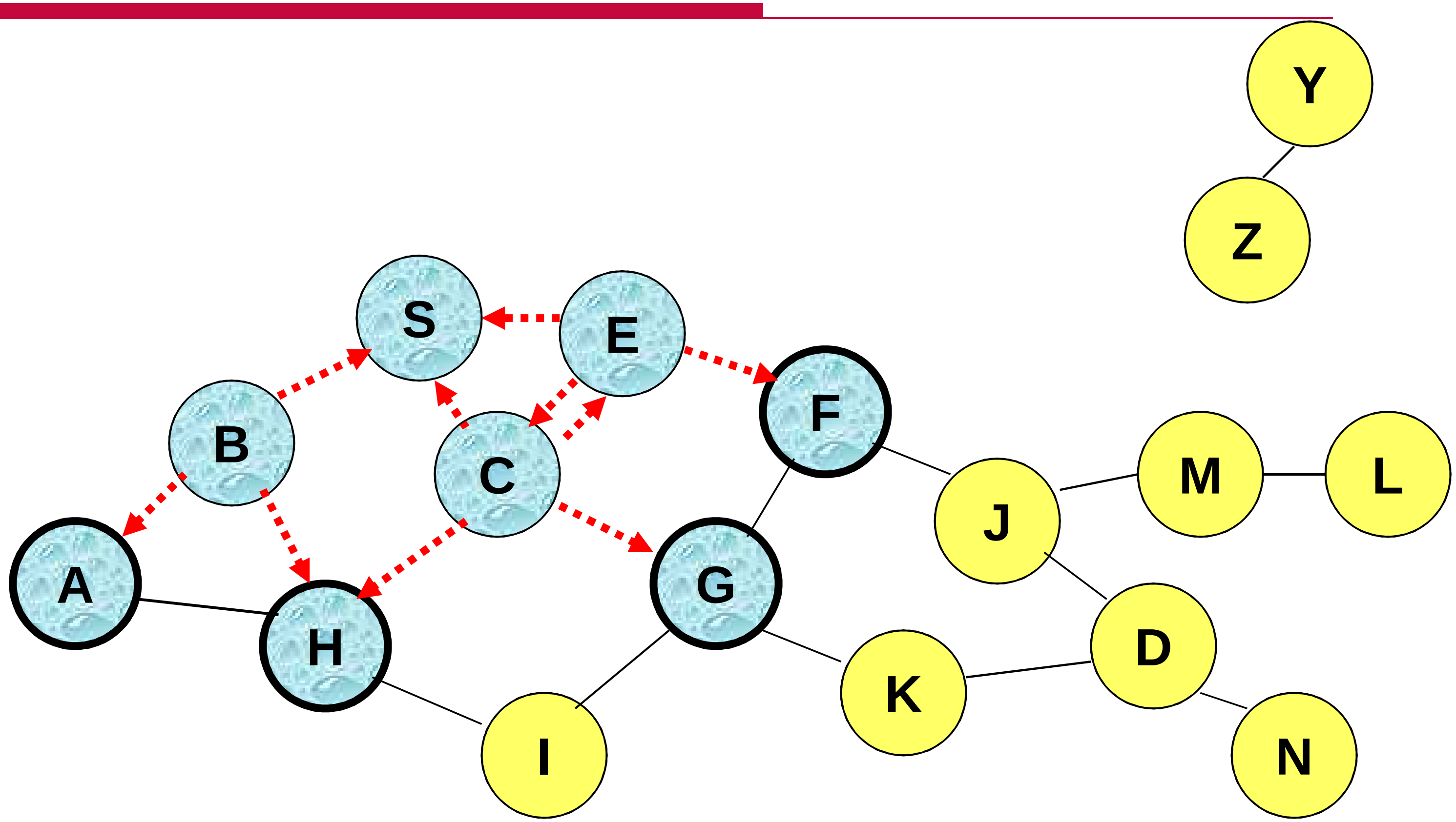




Represents a node that receives packet P for the first time

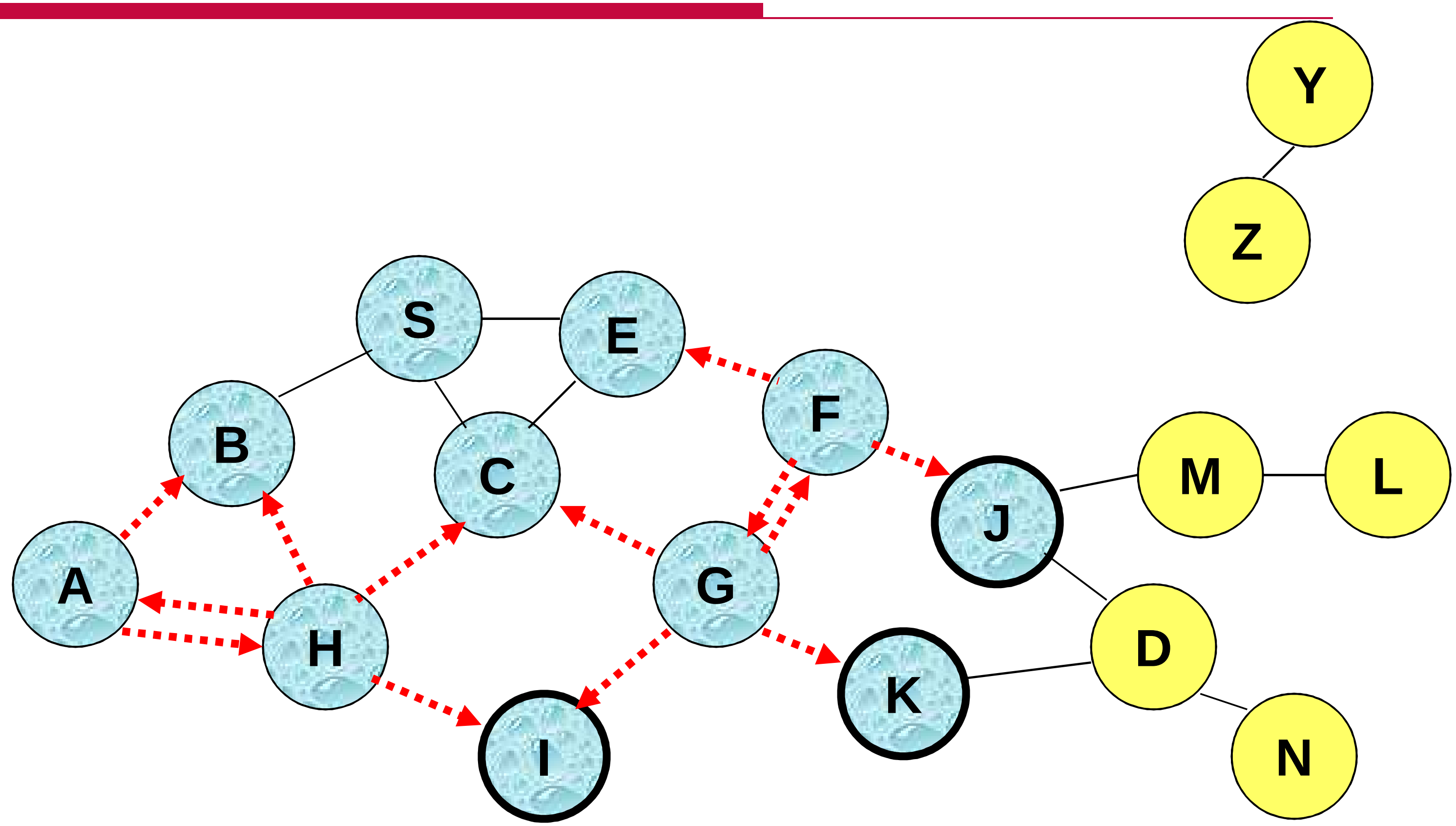
Represents transmission of packet P

Flooding for Data Delivery



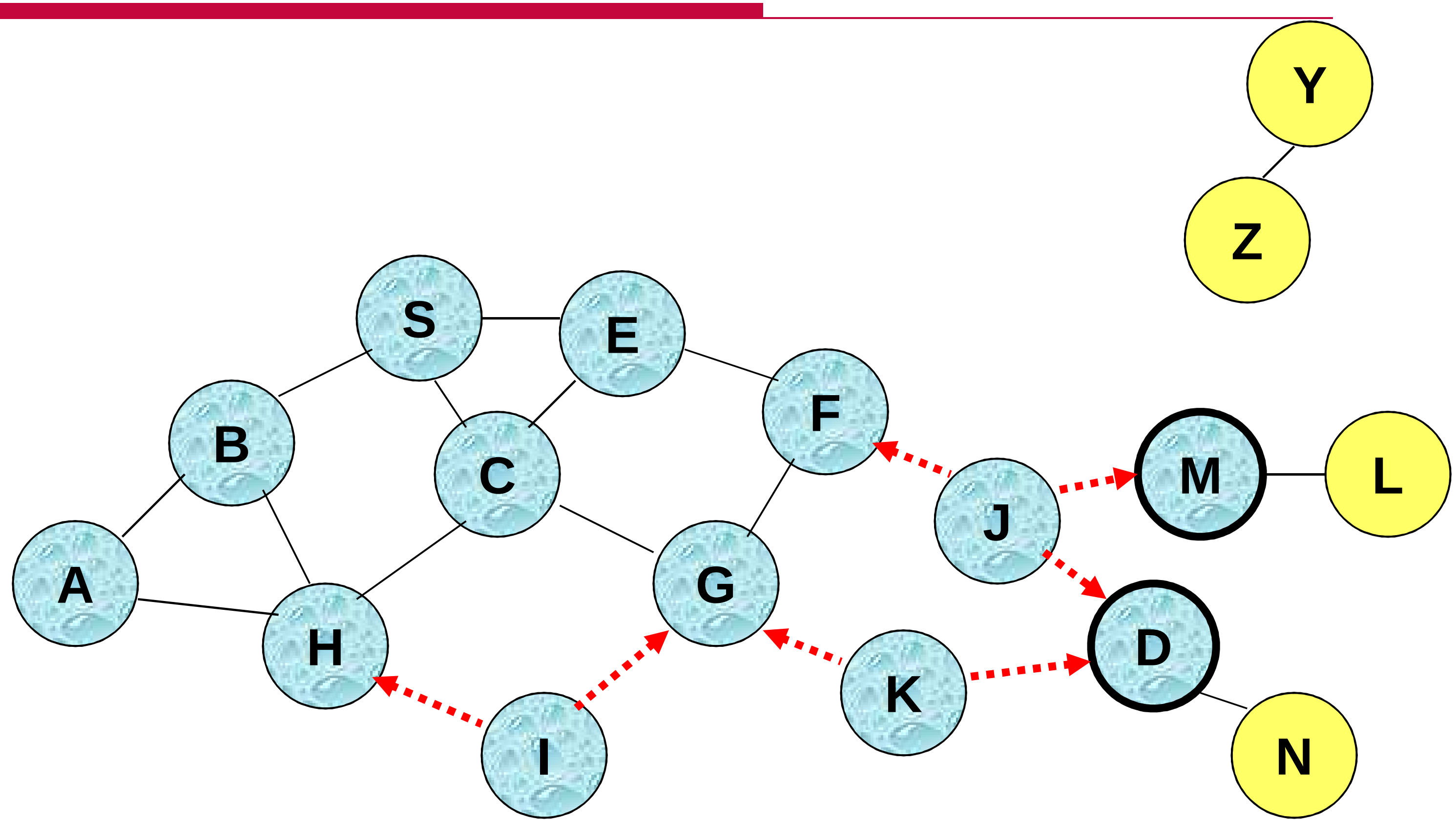
- Node H receives packet P from two neighbors: **potential for collision**

Flooding for Data Delivery



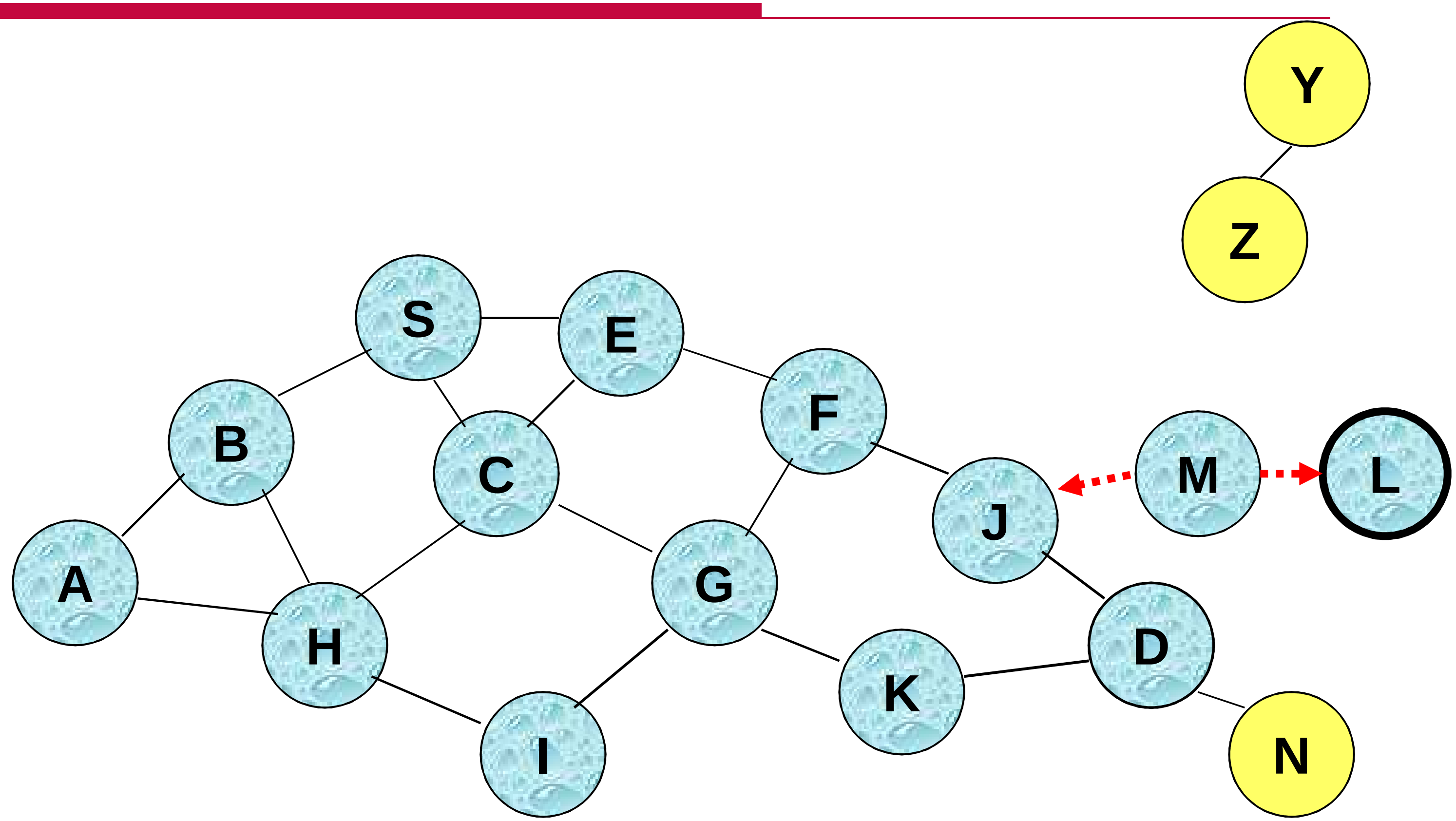
- Node C receives packet P from G and H, but does not forward it again, because node C has already forwarded packet P once

Flooding for Data Delivery



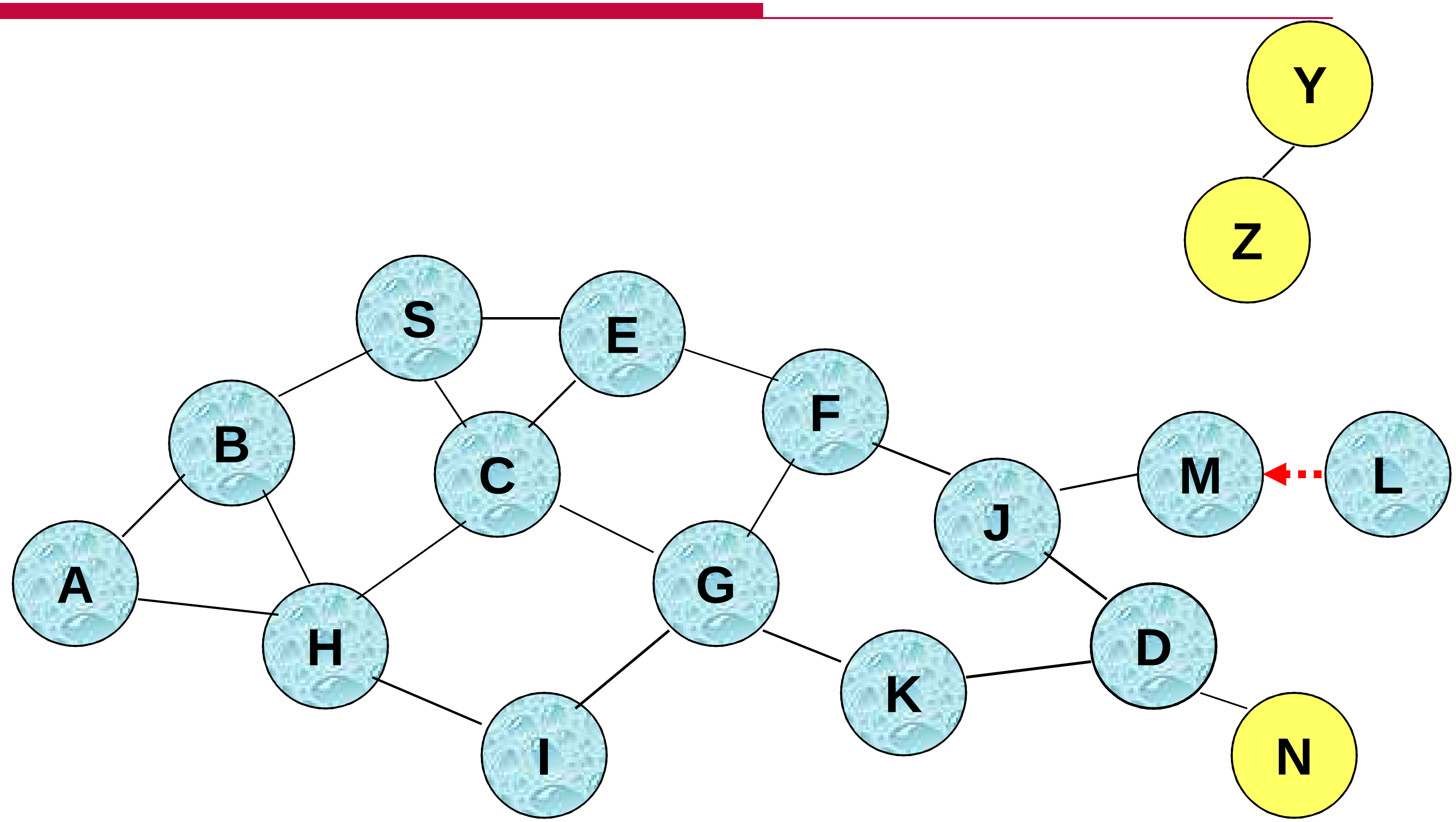
- Nodes J and K both broadcast packet P to node D
- Since nodes J and K are hidden from each other, their transmissions may collide => Packet P may not be delivered to node D at all, despite the use of flooding

Flooding for Data Delivery



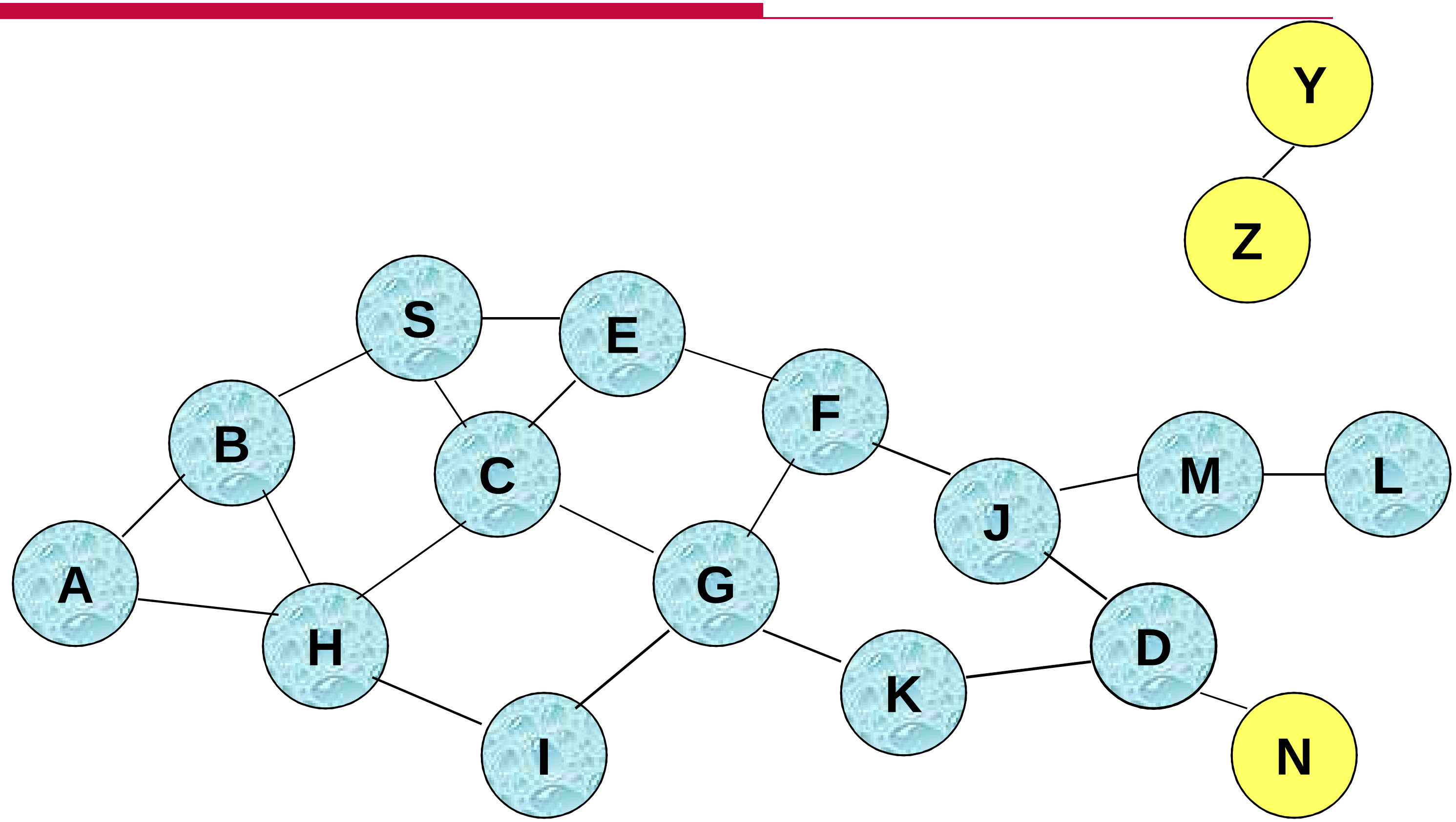
- Node D **does not forward** packet P, because node D is the intended destination of packet P

Flooding for Data Delivery



- Flooding completed
- Nodes unreachable from S do not receive packet P (e.g., node Z)
- Nodes for which all paths from S go through the destination D also do not receive packet P (example: node N)

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 for Data Delivery: Advantages

- Simplicity
- May be more efficient than other protocols when rate of information transmission is low enough that the overhead of explicit route discovery/maintenance incurred by other protocols is relatively higher
  - this scenario may occur, for instance, when nodes transmit small data packets relatively infrequently, and many topology changes occur between consecutive packet transmissions
- Potentially higher reliability of data delivery
  - Because packets may be delivered to the destination on multiple paths

Flooding for Data Delivery: 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
  - In our example, nodes J and K may transmit to node D simultaneously, resulting in loss of the packet
    - in this case, destination would not receive the packet at all

Flooding of Control Packets

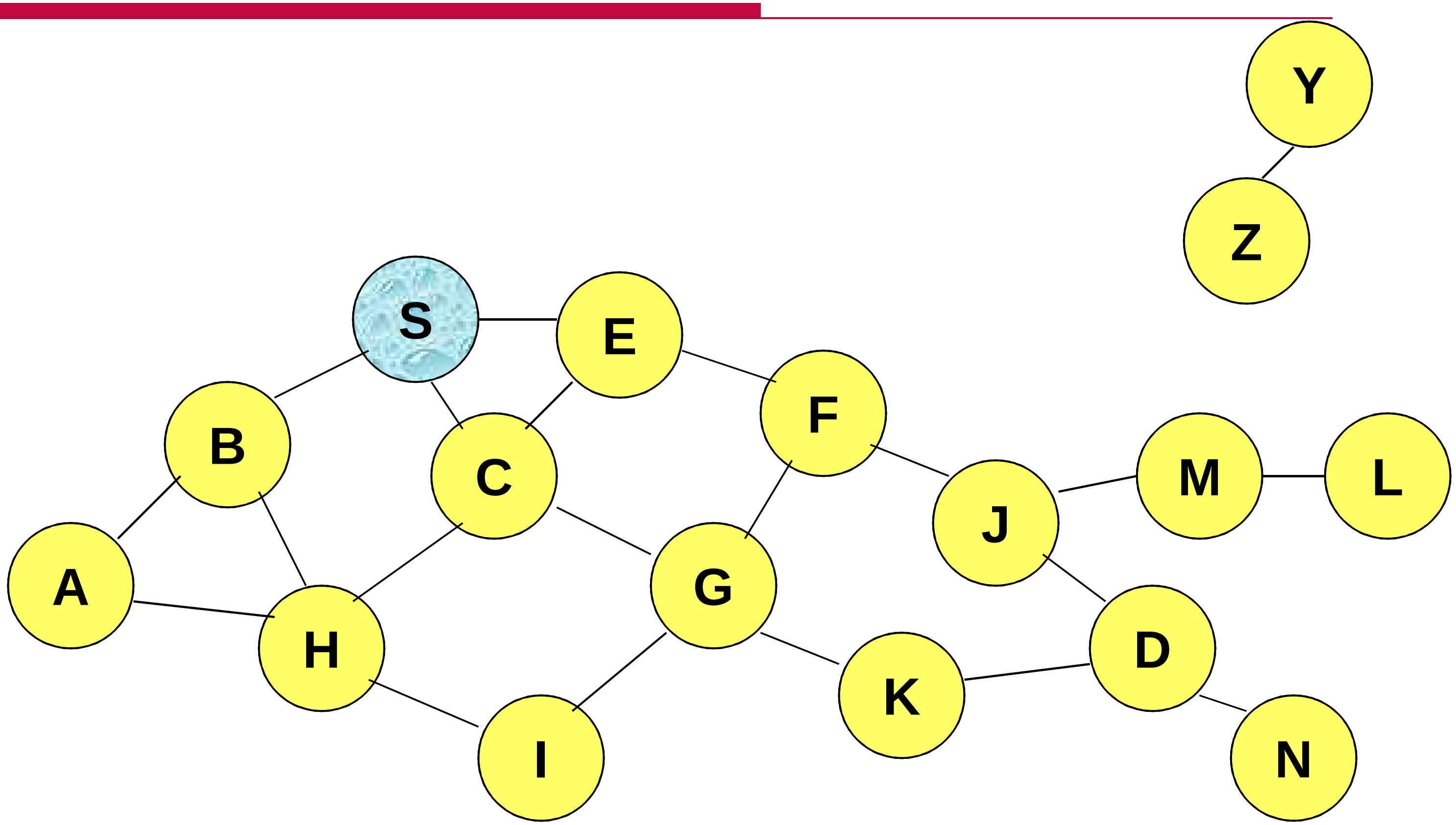
- Many protocols perform (potentially *limited*) flooding of control packets, instead of data packets
- The control packets are used to discover routes
- Discovered routes are subsequently used to send data packet(s)
- Overhead of control packet flooding is amortized over data packets transmitted between consecutive control packet floods

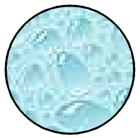
Reactive Protocols

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

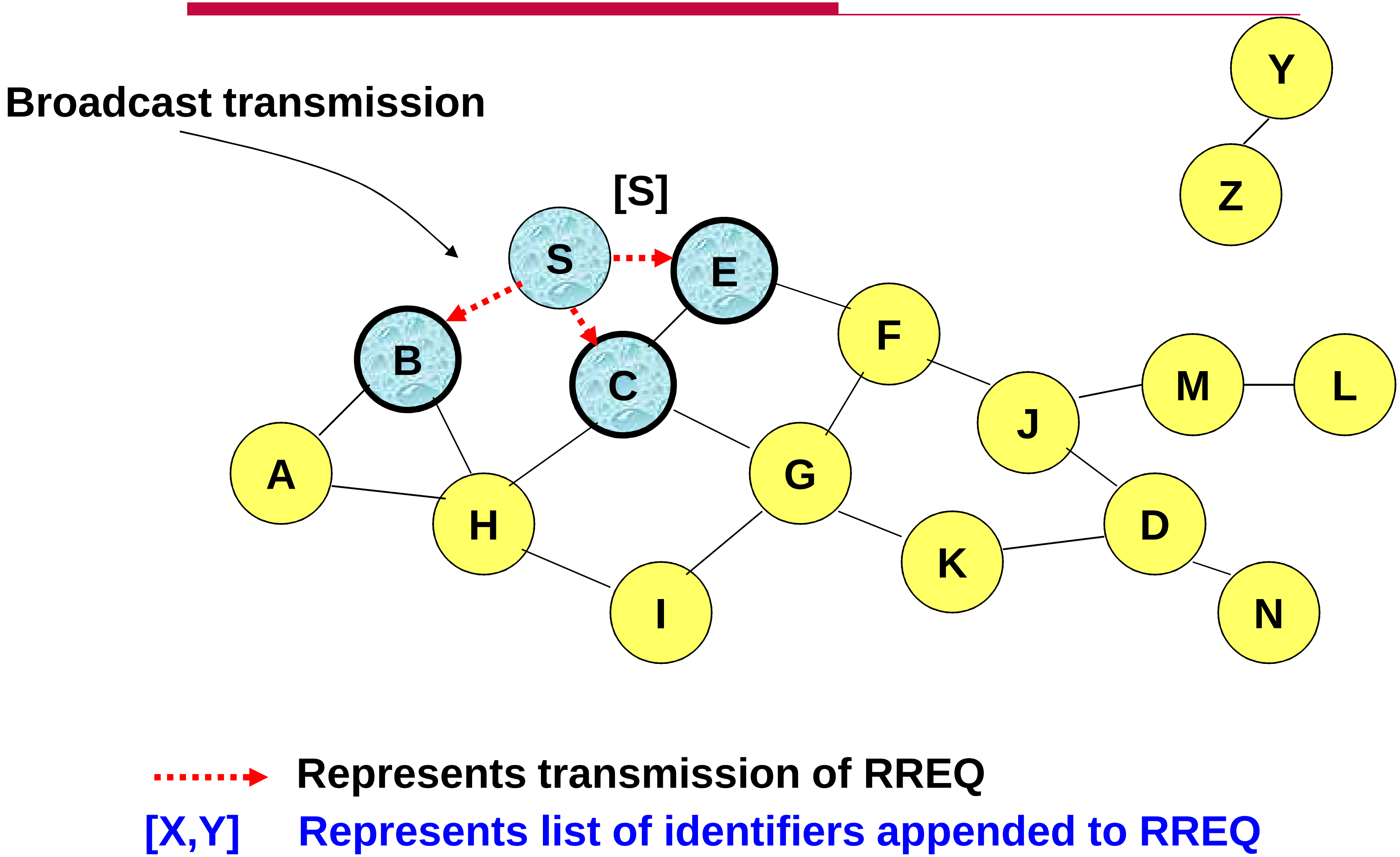
Route Discovery in DSR



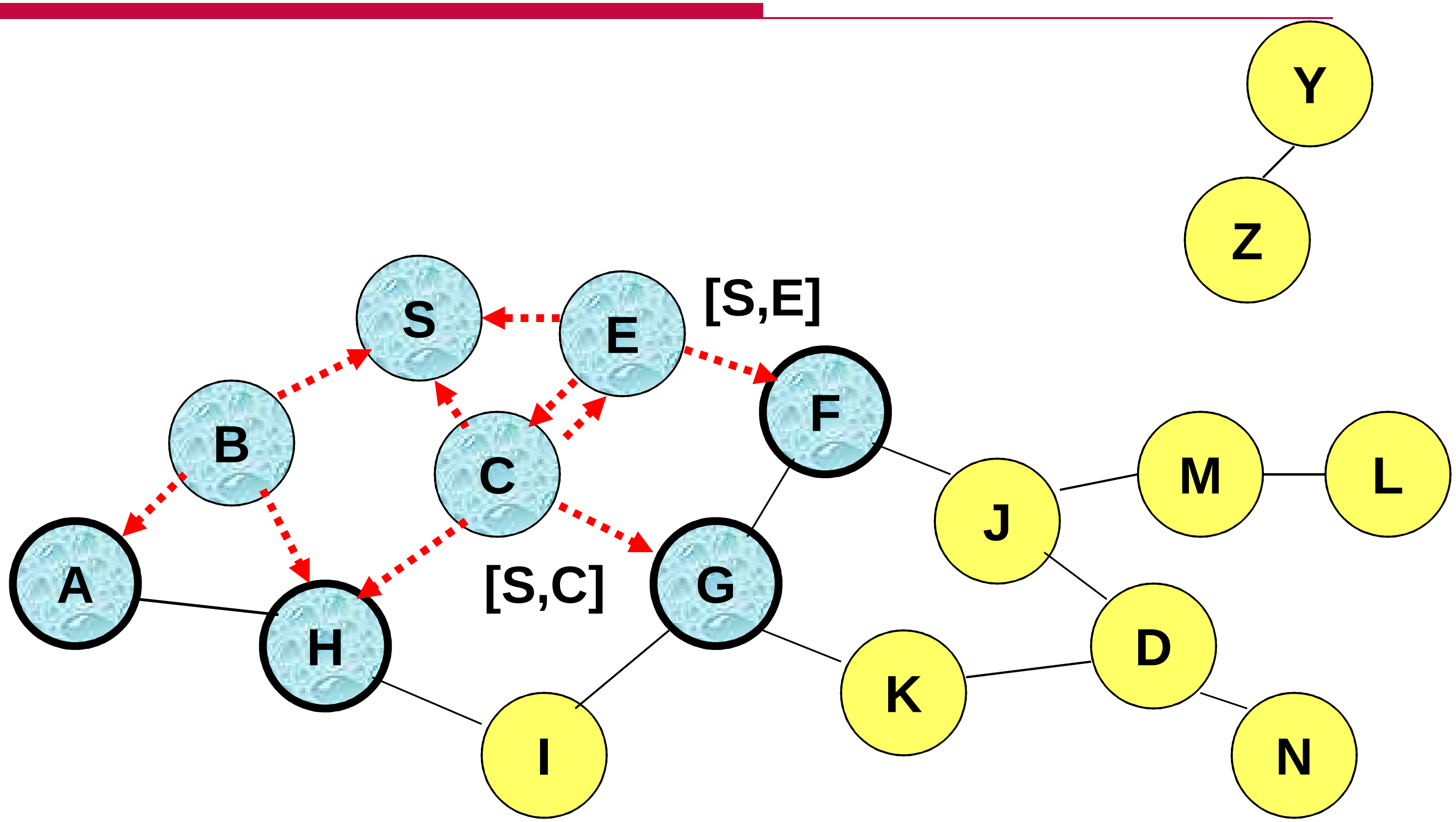


Represents a node that has received RREQ for D from S

Route Discovery in DSR

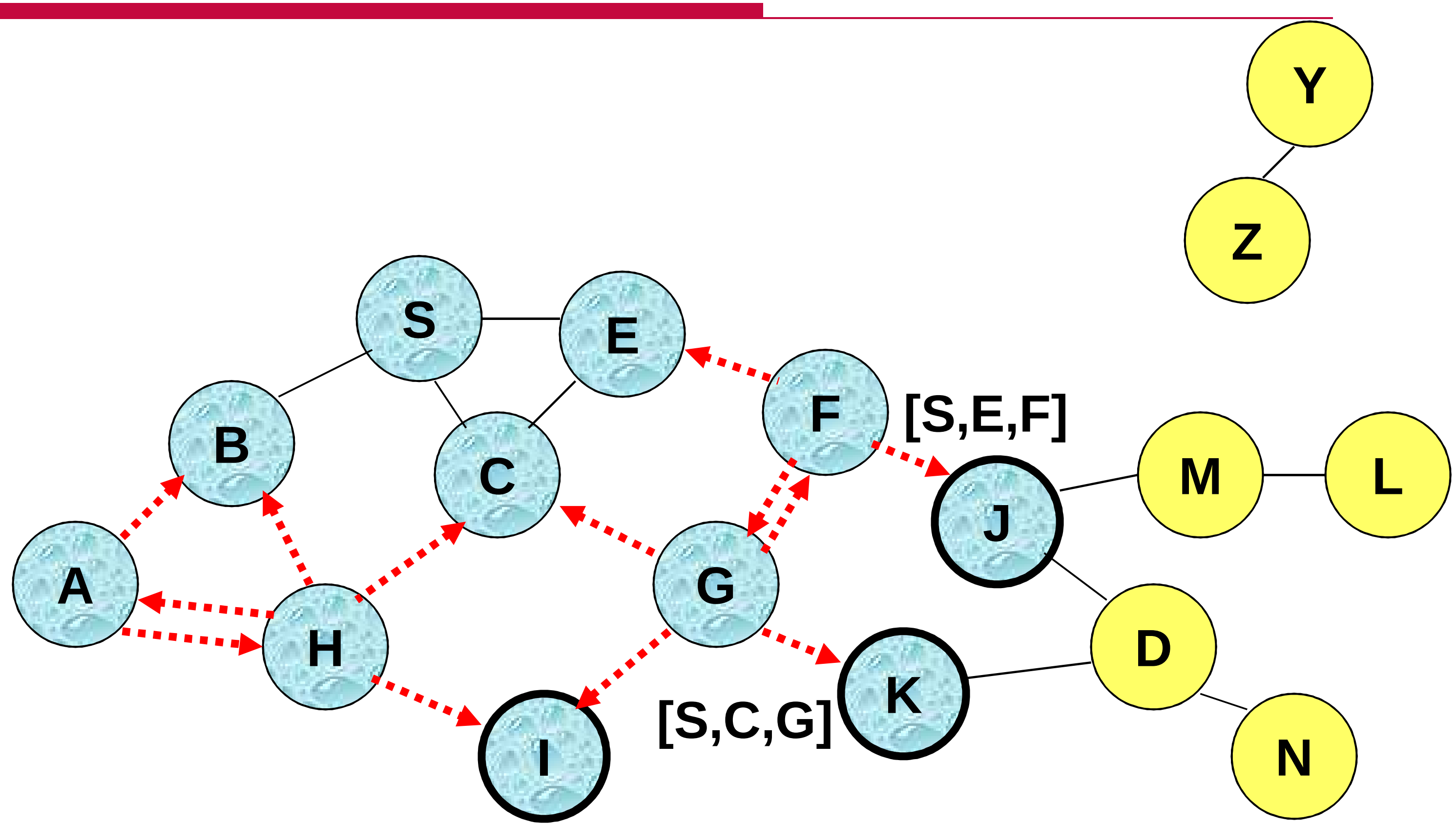


Route Discovery in DSR



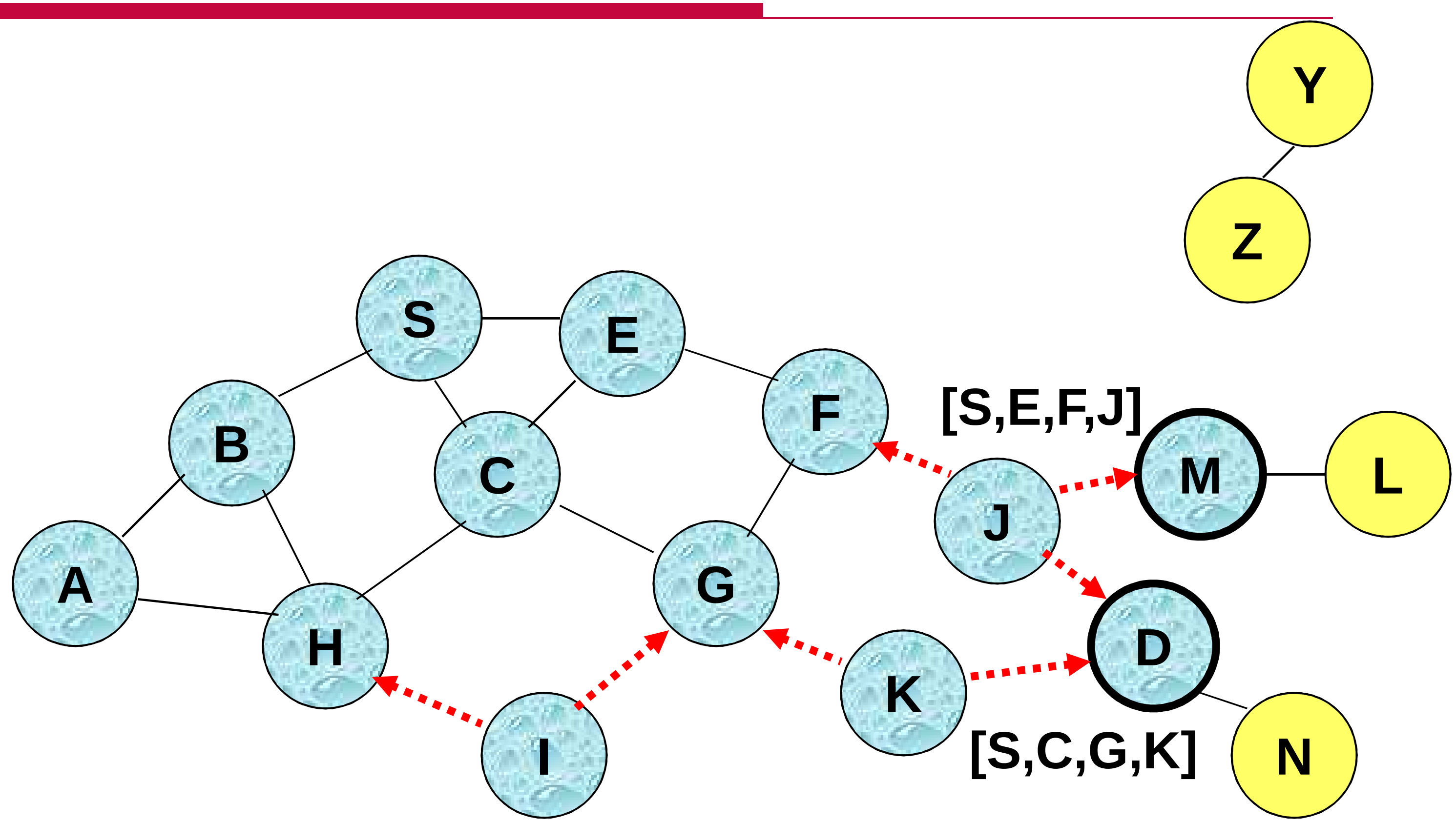
- Node H receives packet RREQ from two neighbors: potential for collision

Route Discovery in DSR



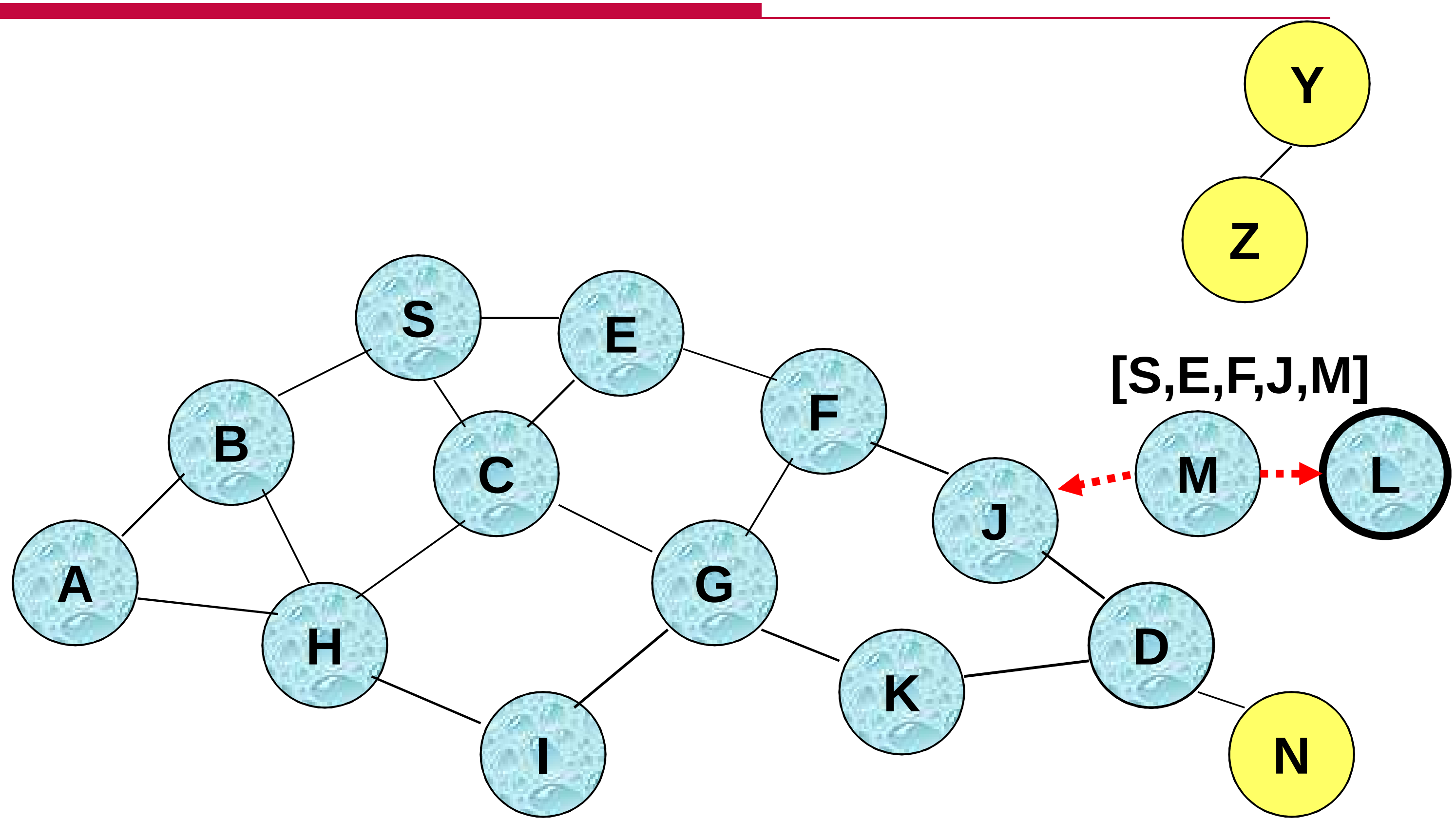
• Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

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

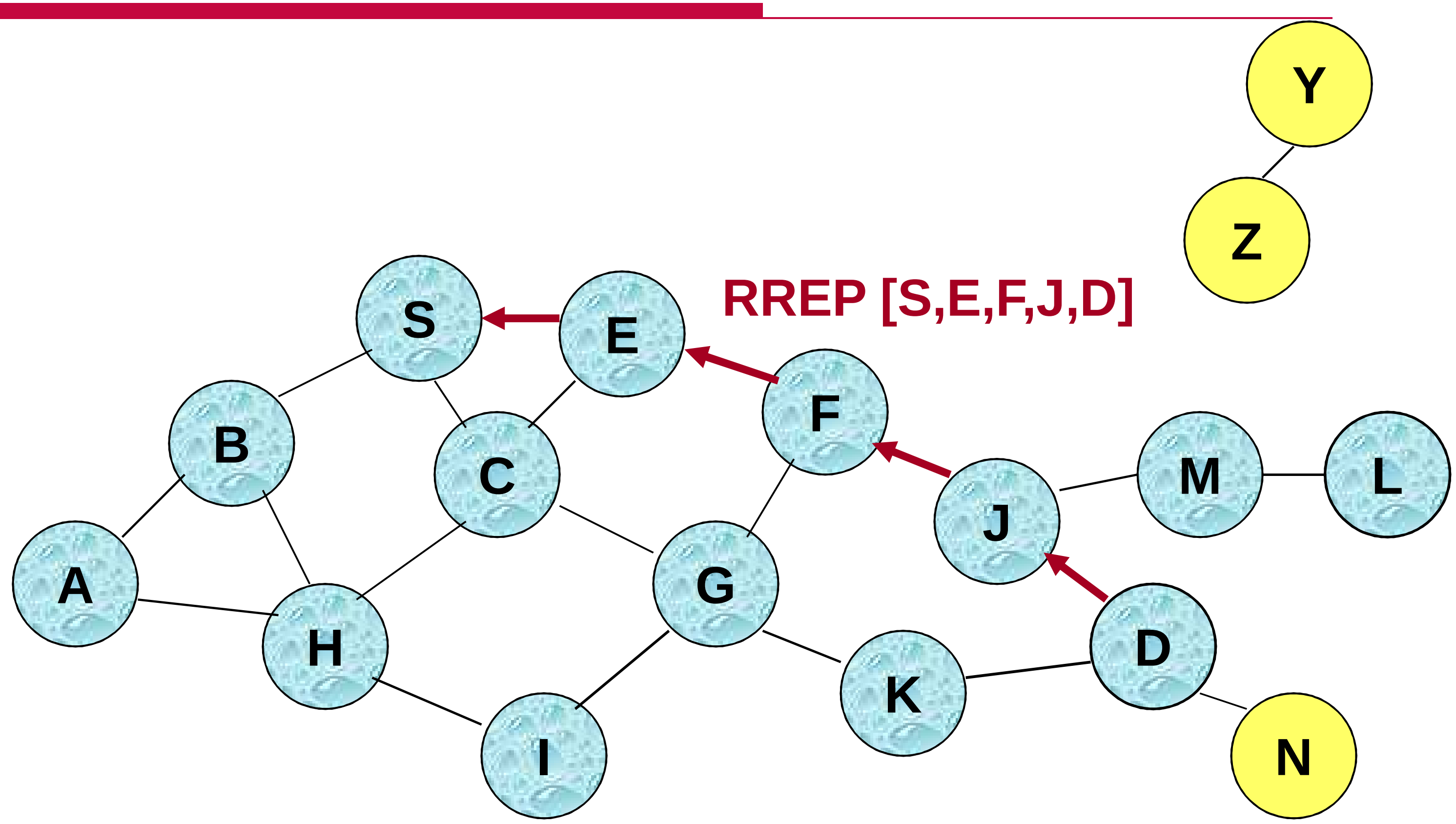


• Node D **does not forward** RREQ, because node D is the **intended target** of the route discovery

Route Discovery in DSR

- 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

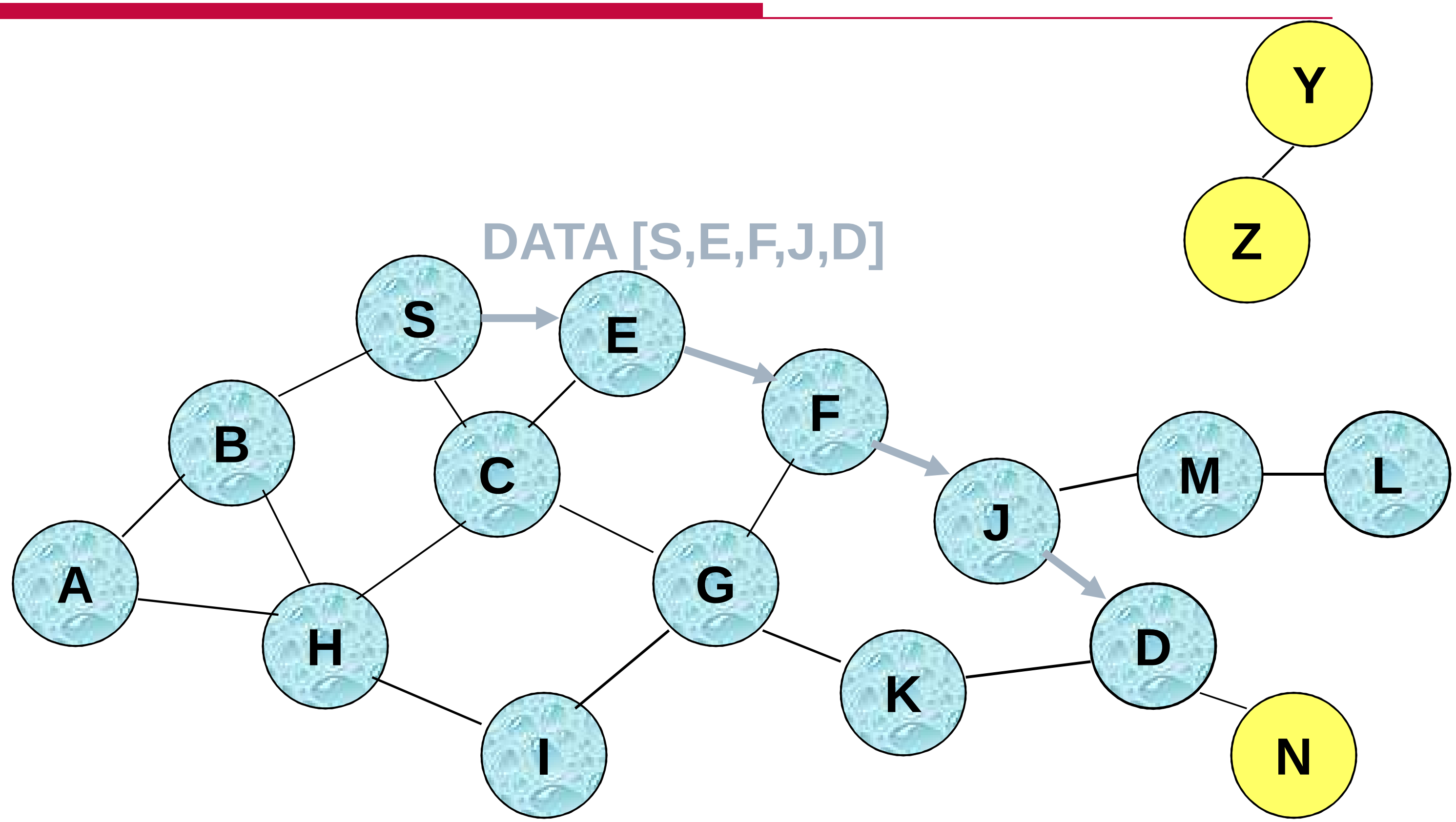
Route Reply in DSR

- 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 was 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)

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

Data Delivery in DSR



Packet <u>header</u> size grows with route length

When to Perform a Route Discovery

- When node S wants to send data to node D, but does not know a valid route node D

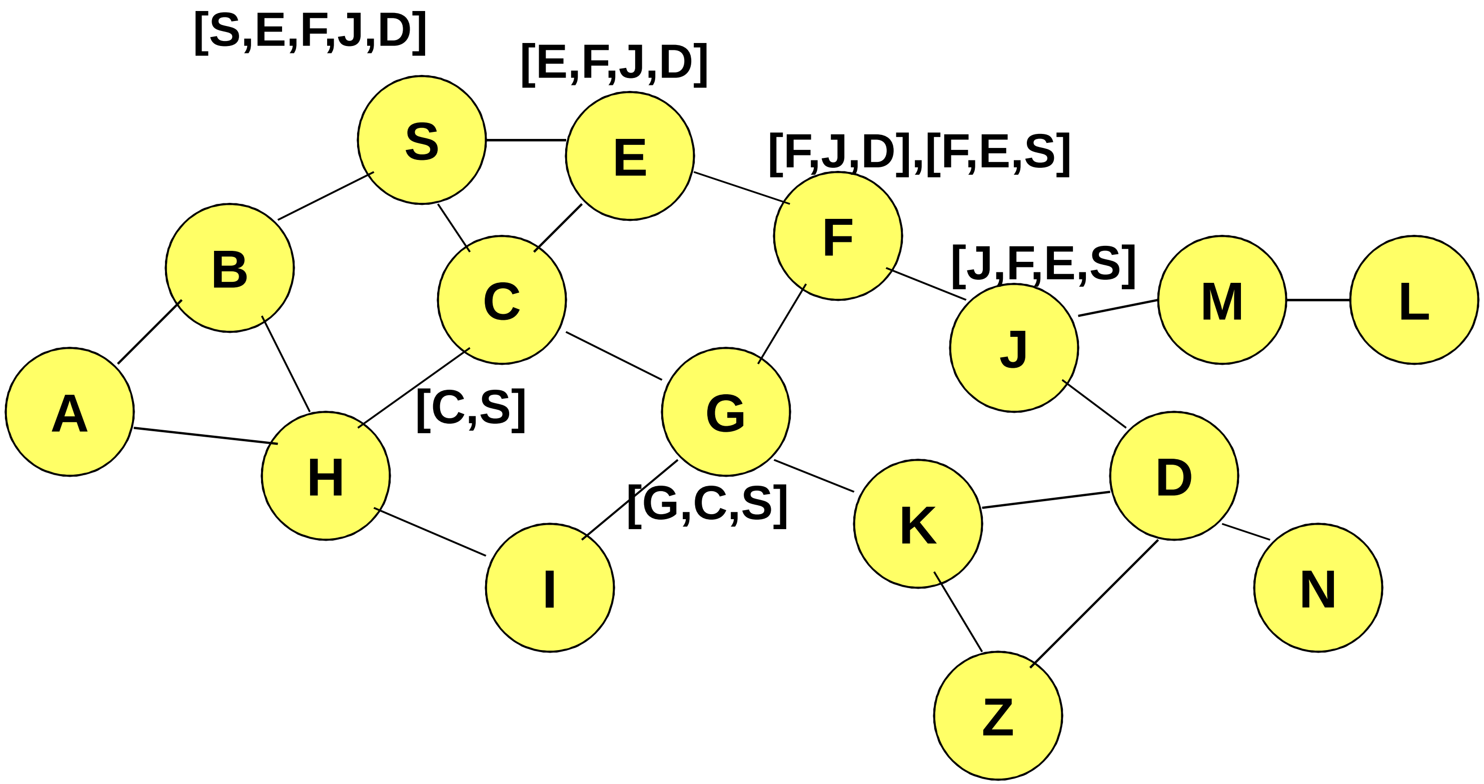
DSR Optimization: Route Caching

- 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 D, node K learns route [K,G,C,S] to node S
- When node F forwards Route Reply RREP [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

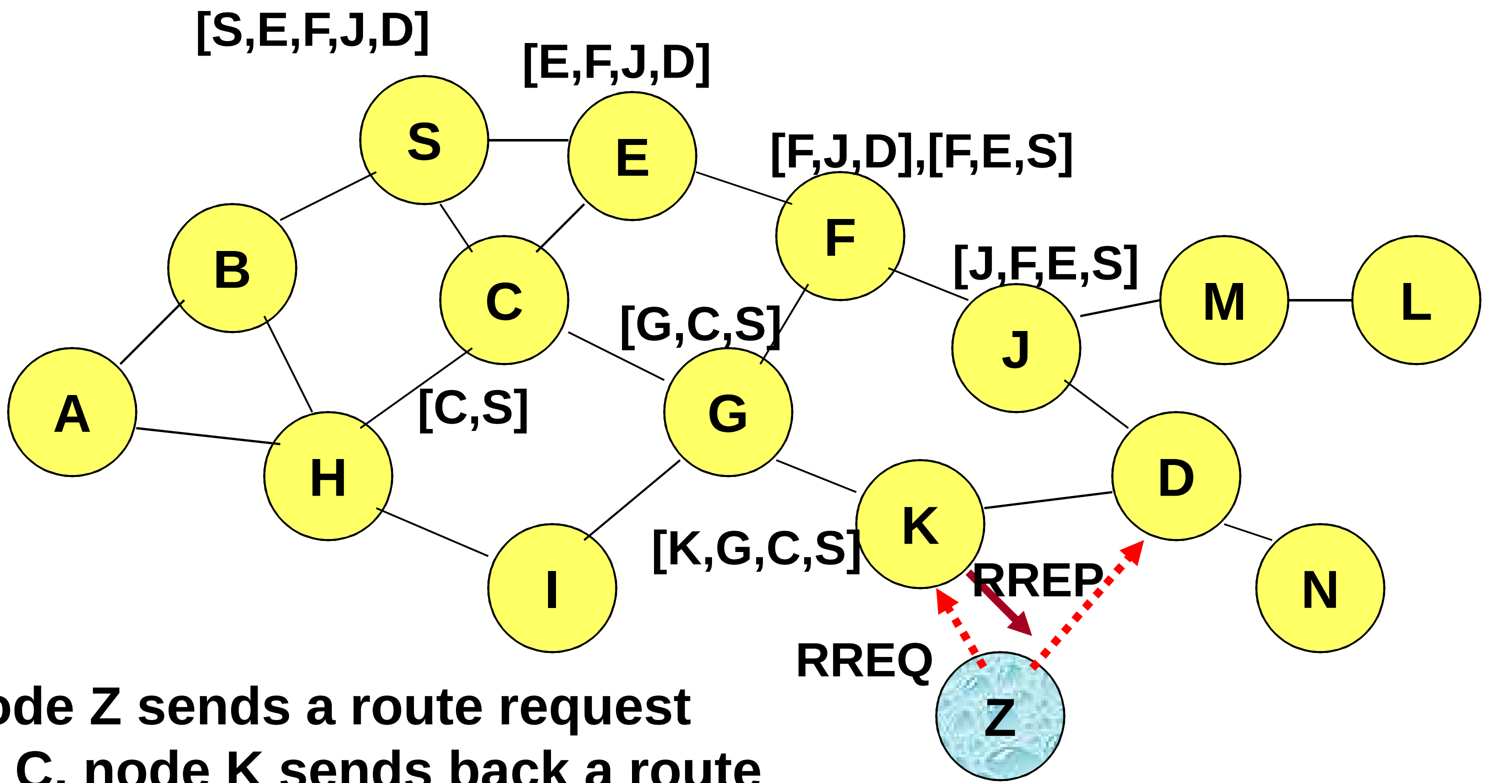
- When node S learns that a route to node D is broken, it uses another route from its local cache, if such a route to D exists in its cache. Otherwise, node S initiates route discovery by sending a route request
- Node X, on receiving a Route Request for some node D, can send a Route Reply if node X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



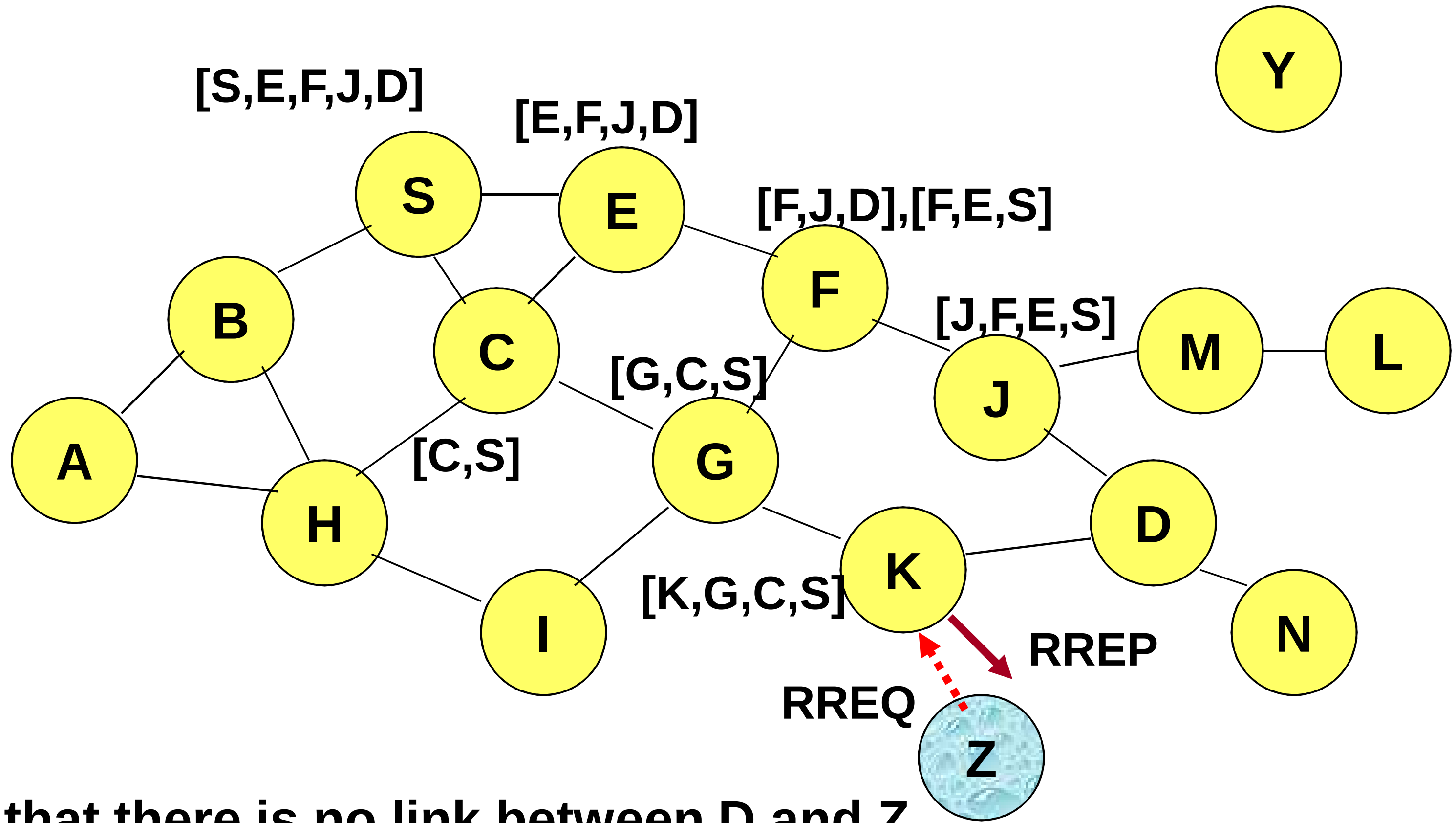
[P,Q,R] Represents cached route at a node
(DSR maintains the cached routes in a tree format)

Route Caching: Can Speed up Route Discovery



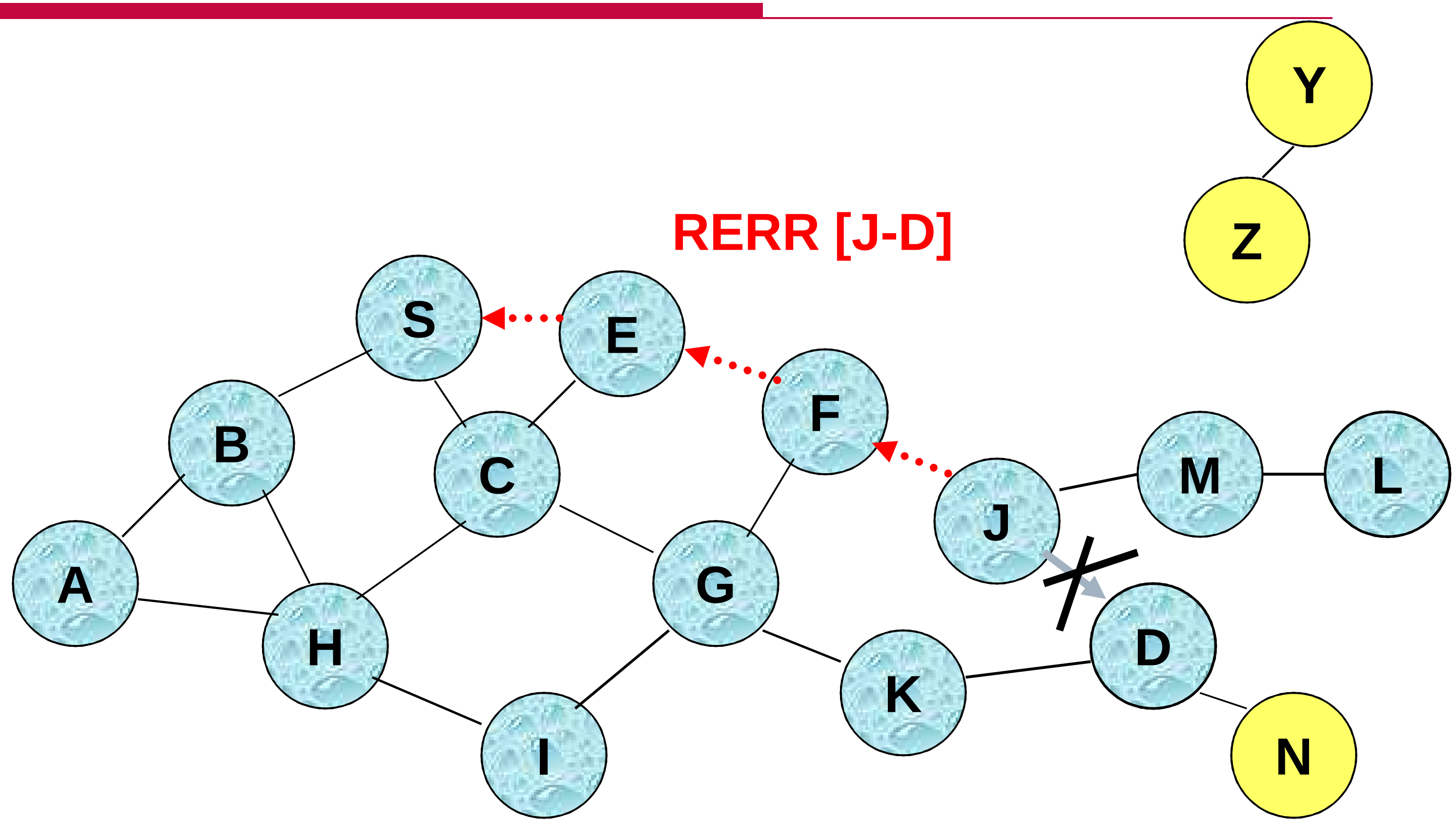
When node Z sends a route request for node C, node K sends back a route reply [Z,K,G,C] to node Z using a locally cached route

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

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

Ad Hoc On-Demand Distance Vector Routing (AODV)

- 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

Proactive Protocols

Link State Routing

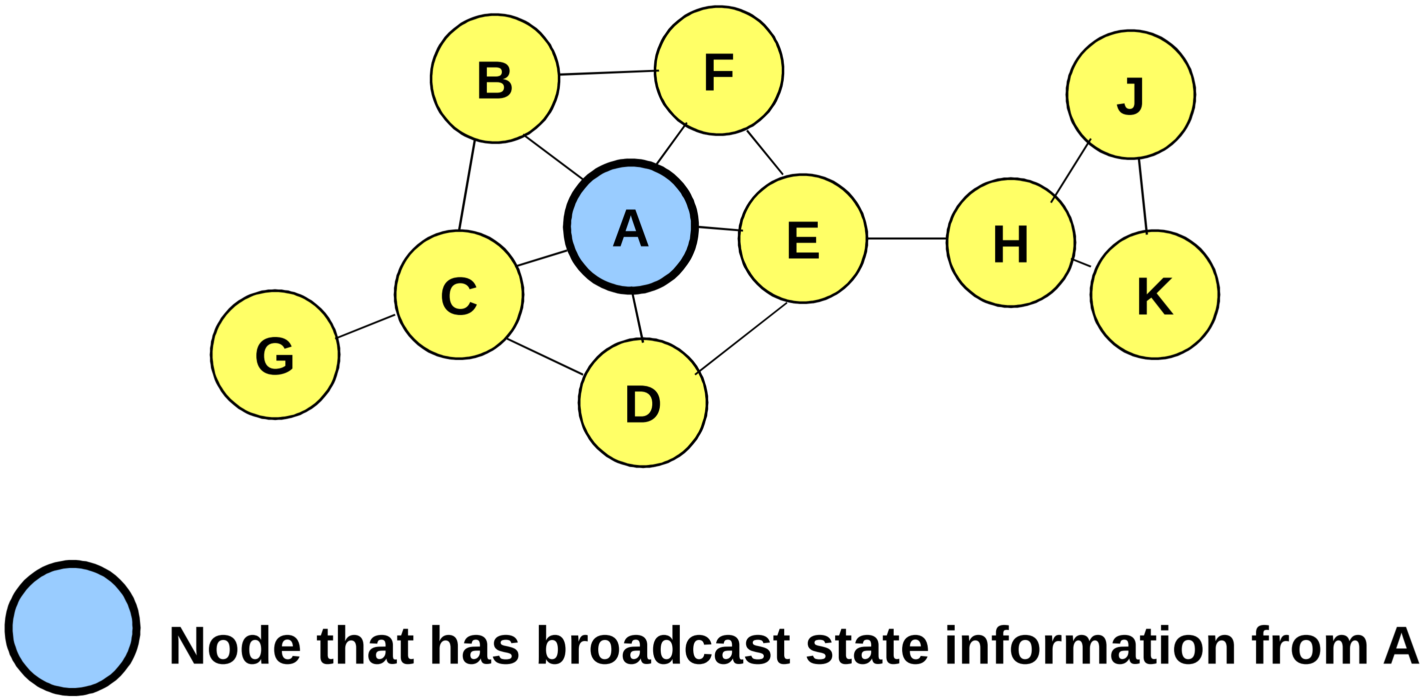
- Each node periodically floods status of its links
- Each node re-broadcasts link state information received from its neighbor
- Each node keeps track of link state information received from other nodes
- Each node uses above information to determine next hop to each destination

Optimized Link State Routing (OLSR)

- The overhead of flooding link state information is reduced by requiring fewer nodes to forward the information
- A broadcast from node X is only forwarded by its *multipoint relays*
- Multipoint relays of node X are its neighbors such that each two-hop neighbor of X is a one-hop neighbor of at least one multipoint relay of X
  - Each node transmits its neighbor list in periodic beacons, so that all nodes can know their 2-hop neighbors, in order to choose the multipoint relays

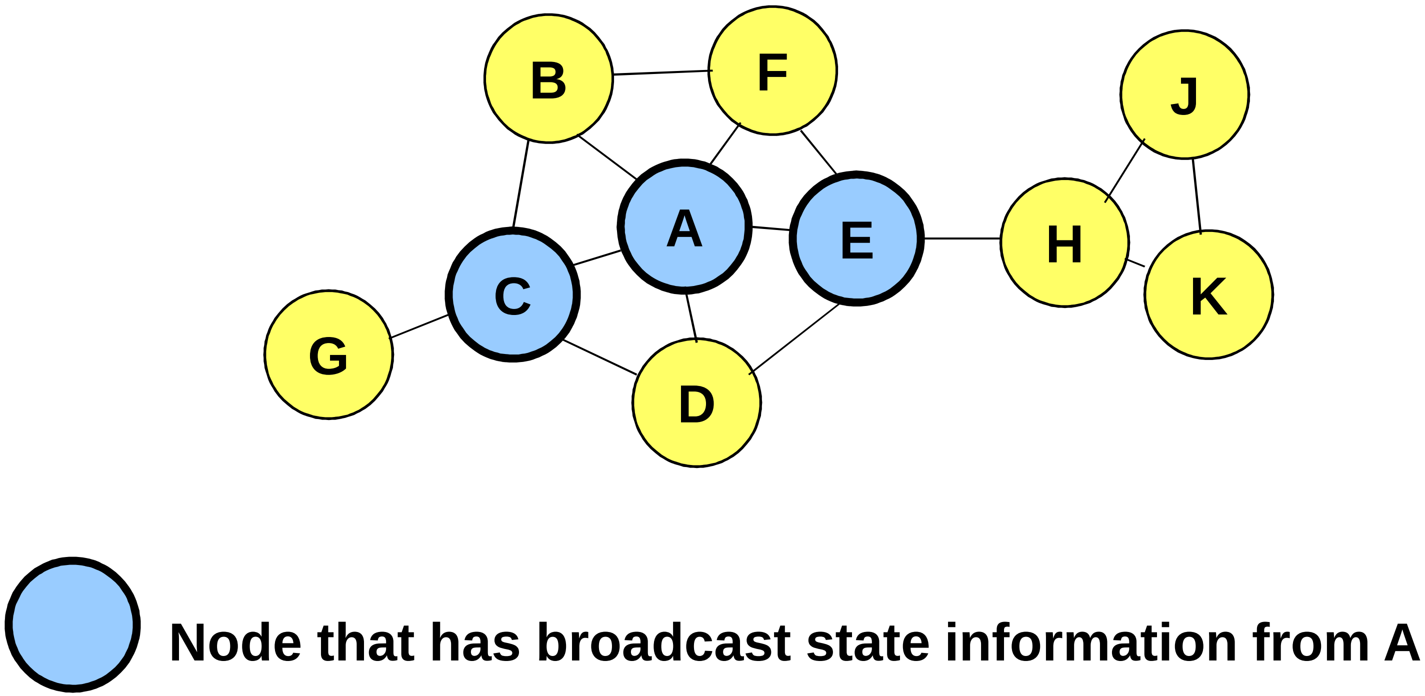
Optimized Link State Routing (OLSR)

- Nodes C and E are multipoint relays of node A



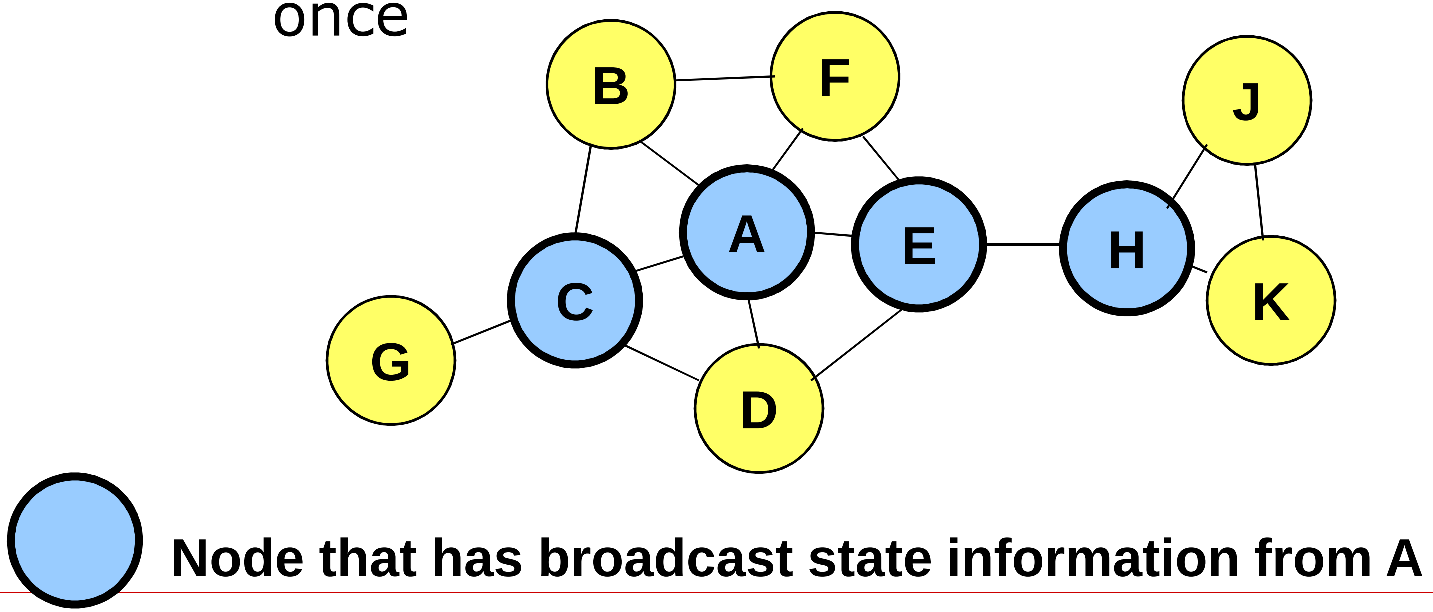
Optimized Link State Routing (OLSR)

- Nodes C and E forward information received from A



Optimized Link State Routing (OLSR)

- Nodes E and K are multipoint relays for node H
- Node K forwards information received from H
  - E has already forwarded the same information once



OLSR

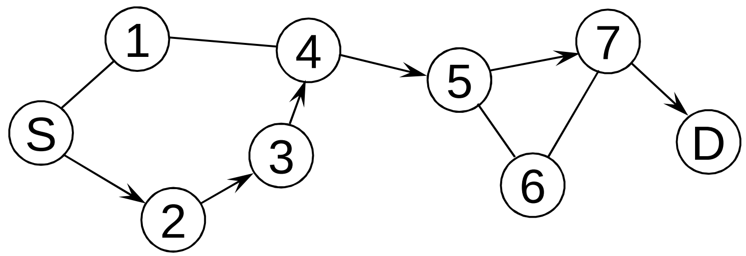
- OLSR floods information through the multipoint relays
- The flooded information itself is for links connecting nodes to respective multipoint relays
- Routes used by OLSR only include multipoint relays as intermediate nodes

Geographic routing

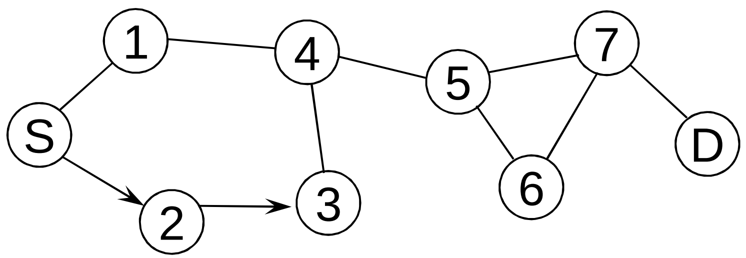
Geographic Distance Routing (GEDIR)

- Rather than maintaining routing tables and discovering paths, one can also use the geographic location of nodes
  - Requires that each node knows it own location (e.g., using GPS)
  - Requires knowledge of all neighbor locations
- It is based on sending the packet to the neighbor that is closest to the destination
  - Works only if nodes are located densely
  - Obstacles and low node density may lead to routing failures

GEDIR – Example



Regular Operation
(not necessarily minimum hop)

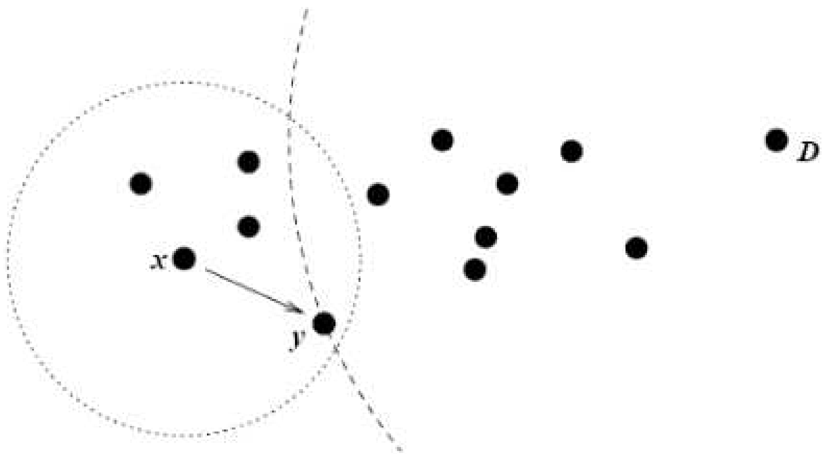


Routing fails because 3 has no neighbors closer to D than itself

- To overcome the problem of not finding closer neighbors, expanded local search algorithms are also proposed
  - When stuck, broadcast a path discovery request with small TTL, use discovered path for forwarding data

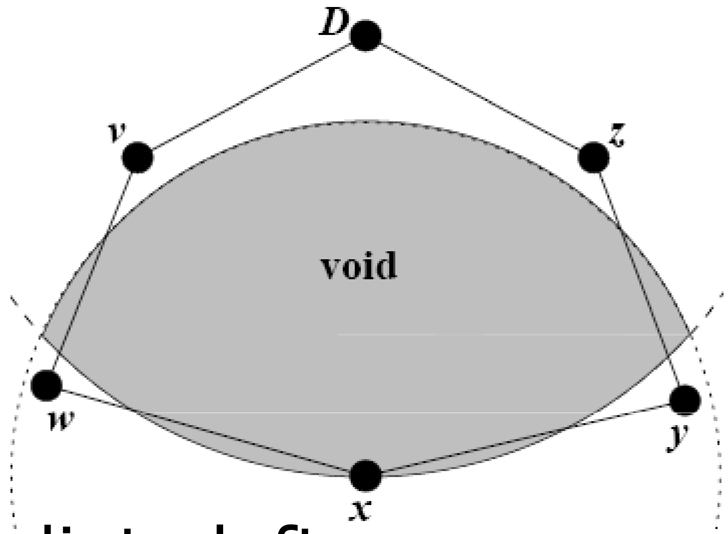
Greedy Perimeter Stateless Routing (GPSR)

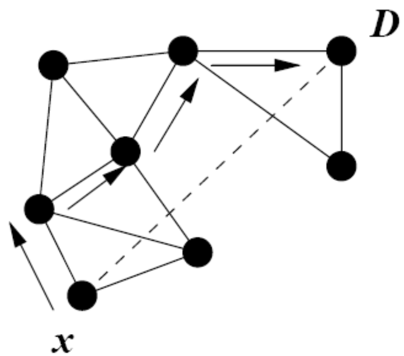
- Another geographic routing algorithm
- Like GEDIR, it is also based on greedy forwarding
  - Maintain a list of neighbors with their locations
  - Send the packet to the node nearest to the destination (Most Forward within Radiu – MFR)
  - Avoid routing loops

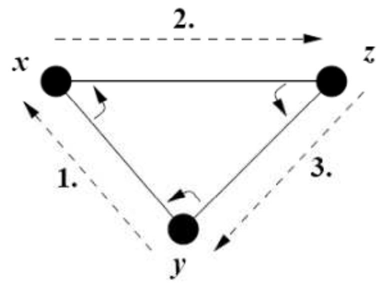


GPSR

- Avoiding routing gaps:
  - Use perimeter routing
  - Mark the line connecting the intermediate node with destination
  - Take the hop to its immediate left (counter-clockwise)
  - Right hand rule!

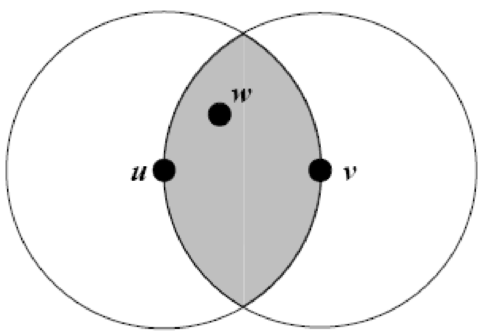




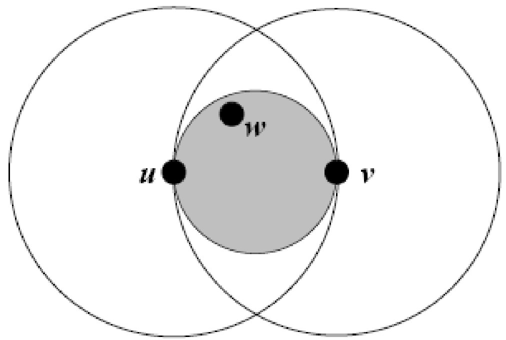


GPSR

- Perimeter routing requires that graphs are planar
  - No edge in the graph crosses another edge
- Planarization algorithms



Relative Neighbor Graph



Gabriel Graph

In both cases, eliminate link uv

Thank you!