KuVS Summer School 2002
Introduction to Mobile Ad Hoc Networks

Christian Maihöfer
DaimlerChrysler

Slides compiled from **Nitin H. Vaidya**'s tutorial at MobiCom 2000

http://www.crhc.uiuc.edu/~nhv

Tutorial Outline

- Introduction, Definition
- Motivation
- Protocols
  - Flooding
  - Dynamic Source Routing (DSR)
  - Location Aided Routing (LAR)
  - DREAM, GEDIR
- Query Localisation
- Broadcast Storm Problem
- Summary

Mobile Ad Hoc Networks (MANET)

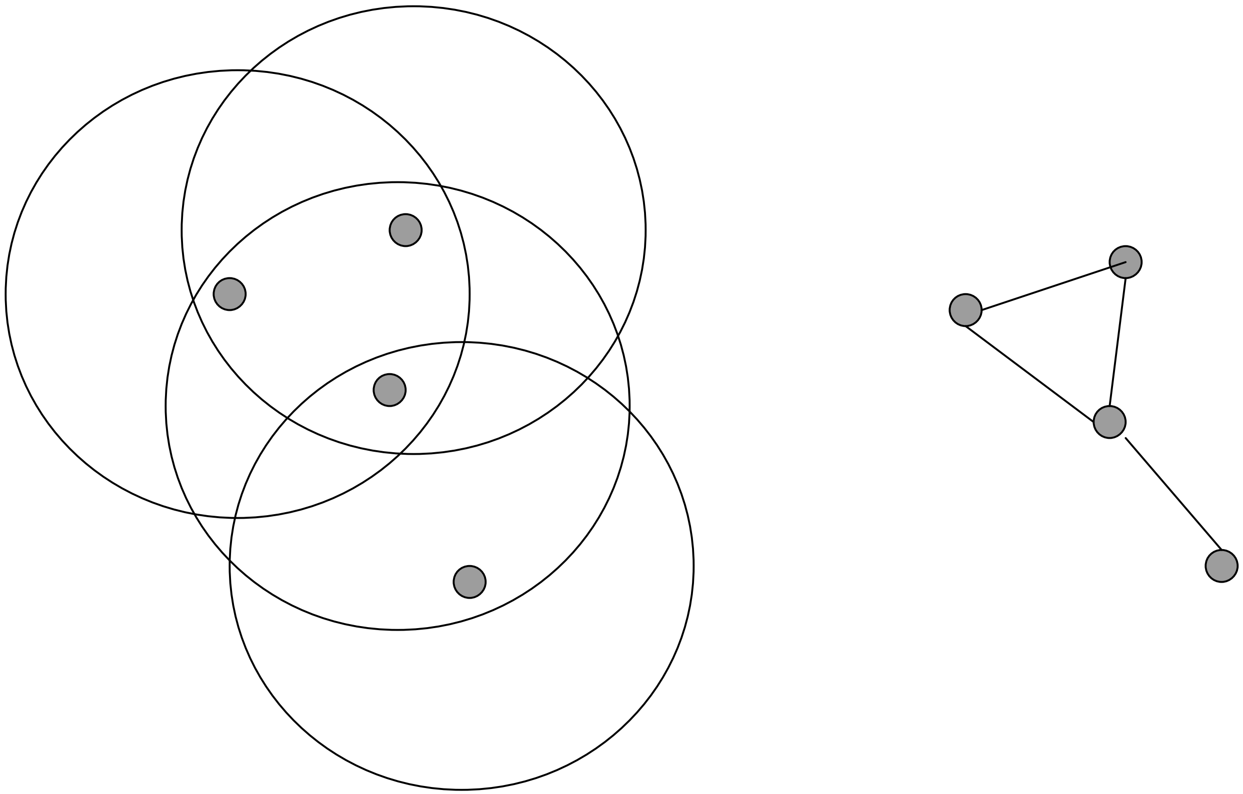
Introduction and Generalities

Mobile Ad Hoc Networks

- Formed by wireless hosts which may be mobile
- Without (necessarily) using a pre-existing infrastructure
- Routes between nodes may potentially contain multiple hops
- Self organizing
- Often hosts act as routers

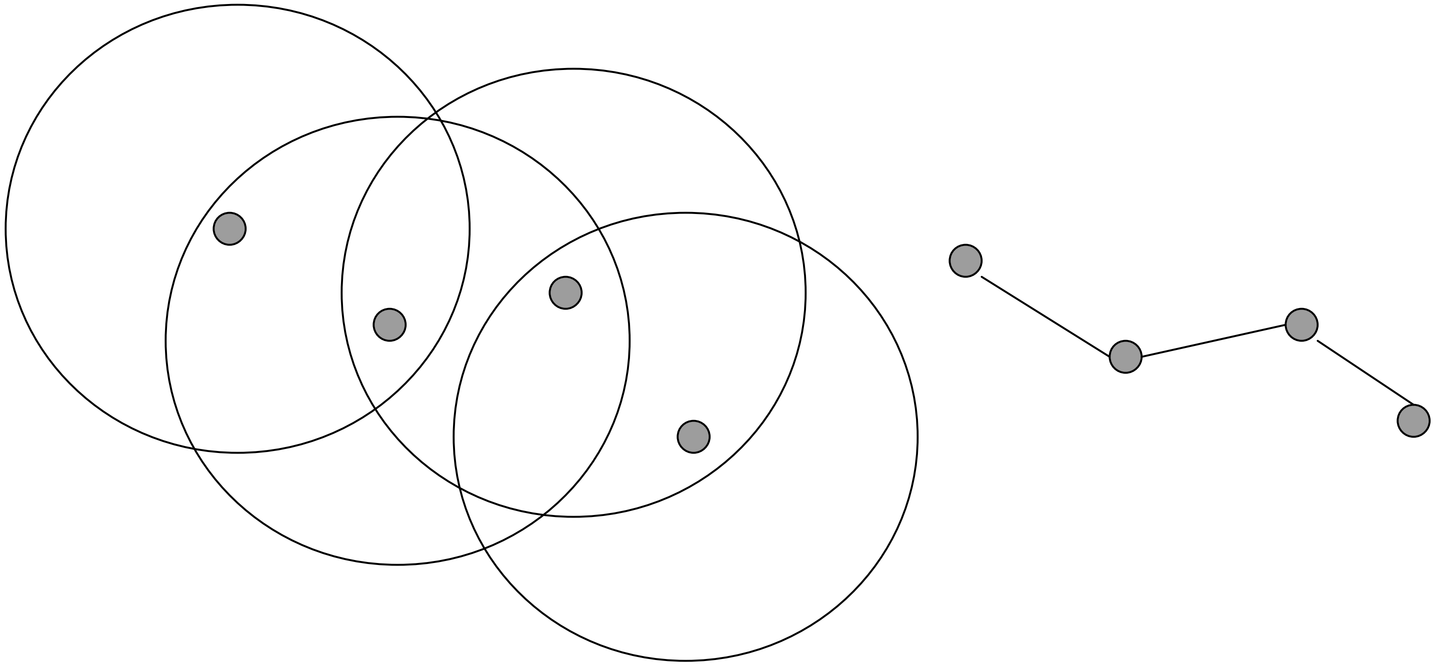
Mobile Ad Hoc Networks

- May need to traverse multiple links to reach a destination



Mobile Ad Hoc Networks (MANET)

- Mobility causes route changes



Why Ad Hoc Networks ?

- Ease of deployment
- Speed of deployment
- Decreased dependence on infrastructure
- Located, where they are required
- Cheaper, no costs for usage (vehicle scenario)
- More robust ?

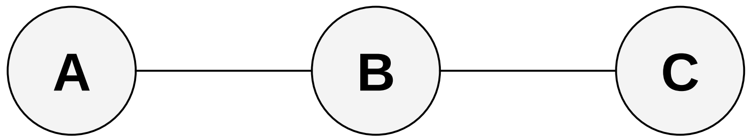
Many Applications

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

Challenges

- Limited wireless transmission range
- Broadcast nature of the wireless medium
  - Hidden terminal problem (see next slide)
- Packet losses due to transmission errors
- Mobility-induced route changes
- Mobility-induced packet losses
- Battery constraints
- Potentially frequent network partitions
- Ease of snooping on wireless transmissions (security hazard)

Hidden Terminal Problem



Nodes A and C cannot hear each other

Transmissions by nodes A and C can collide at node B

Nodes A and C are hidden from each other

Unicast Routing
in
Mobile Ad Hoc Networks

Why is Routing in MANET different ?

- Host mobility
  - link failure/repair due to mobility may have different characteristics than those due to other causes
- Rate of link failure/repair may be high when nodes move fast
- New performance criteria may be used
  - route stability despite mobility
  - energy consumption

Routing Protocols - Classification

- Proactive protocols
  - Determine routes independent of traffic pattern
  - Traditional link-state and distance-vector routing protocols are proactive
- Reactive protocols
  - Maintain routes only if needed
- Hybrid protocols
- Further classifications possible (e.g. position-based)

Trade-Off

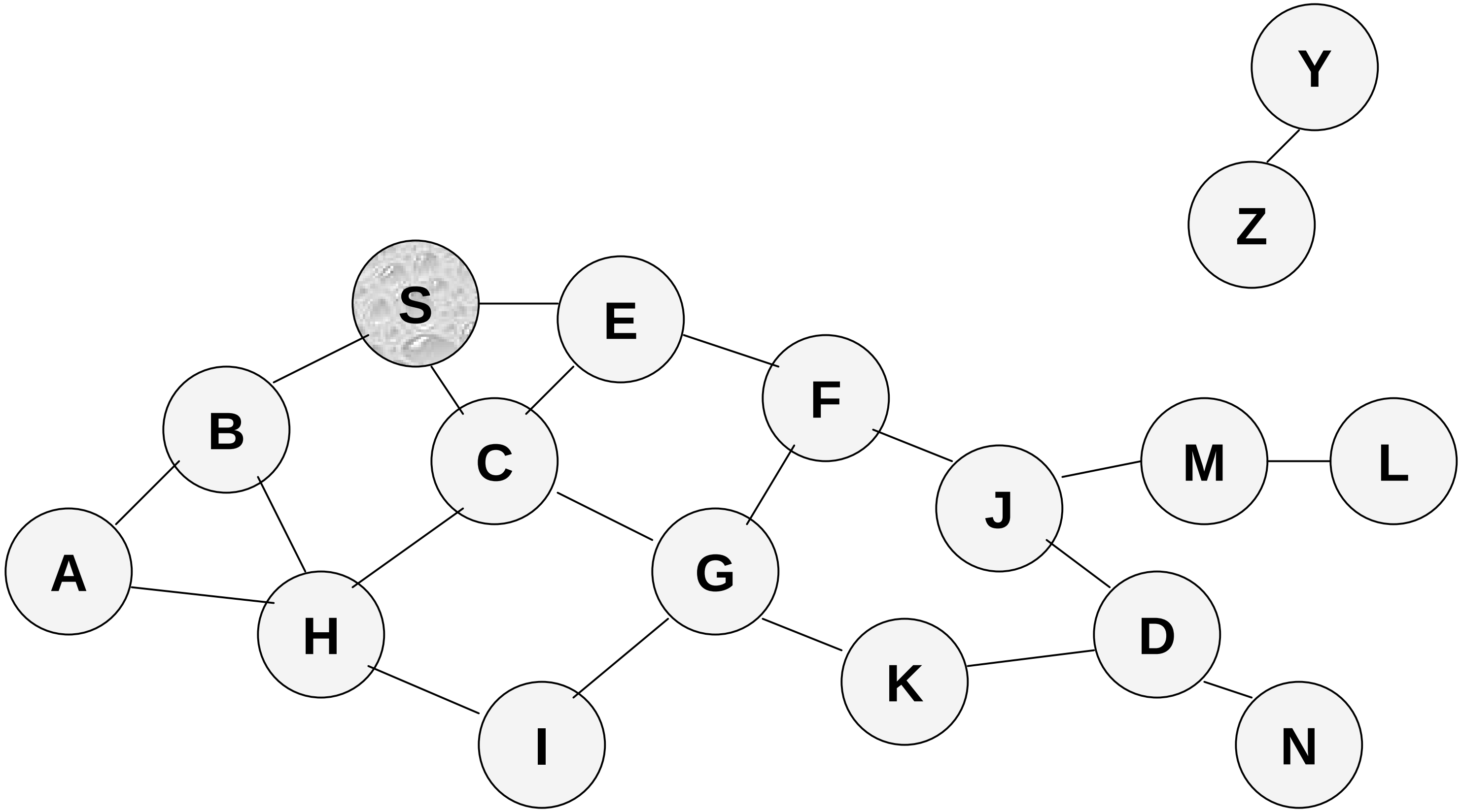
- Latency of route discovery
  - Proactive protocols may have lower latency since routes are maintained at all times
  - Reactive protocols may have higher latency because a route from X to Y will be found only when X attempts to send to Y
- Overhead of route discovery/maintenance
  - Reactive protocols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

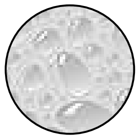
Overview of Unicast Routing Protocols

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

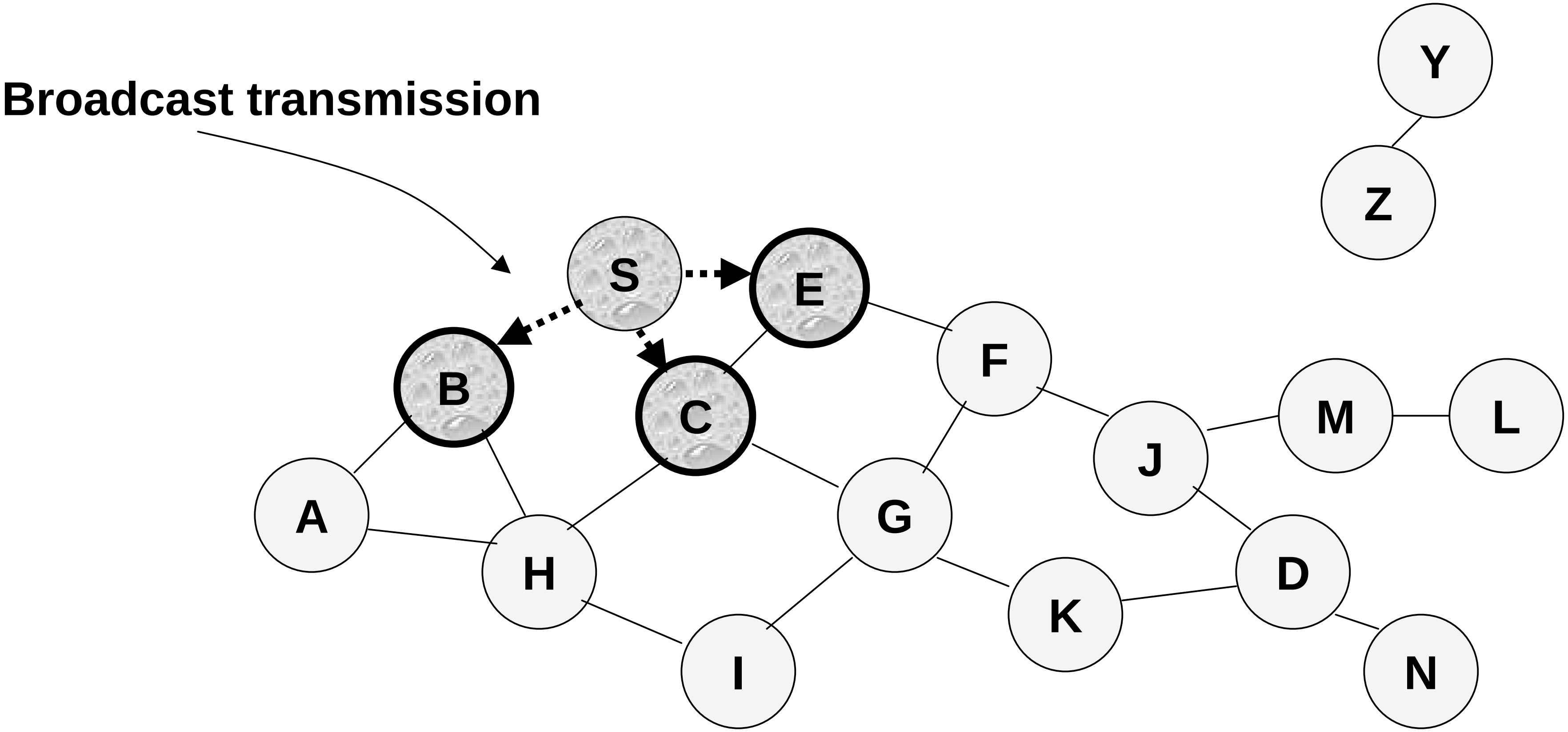




Represents a node that has received packet P

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

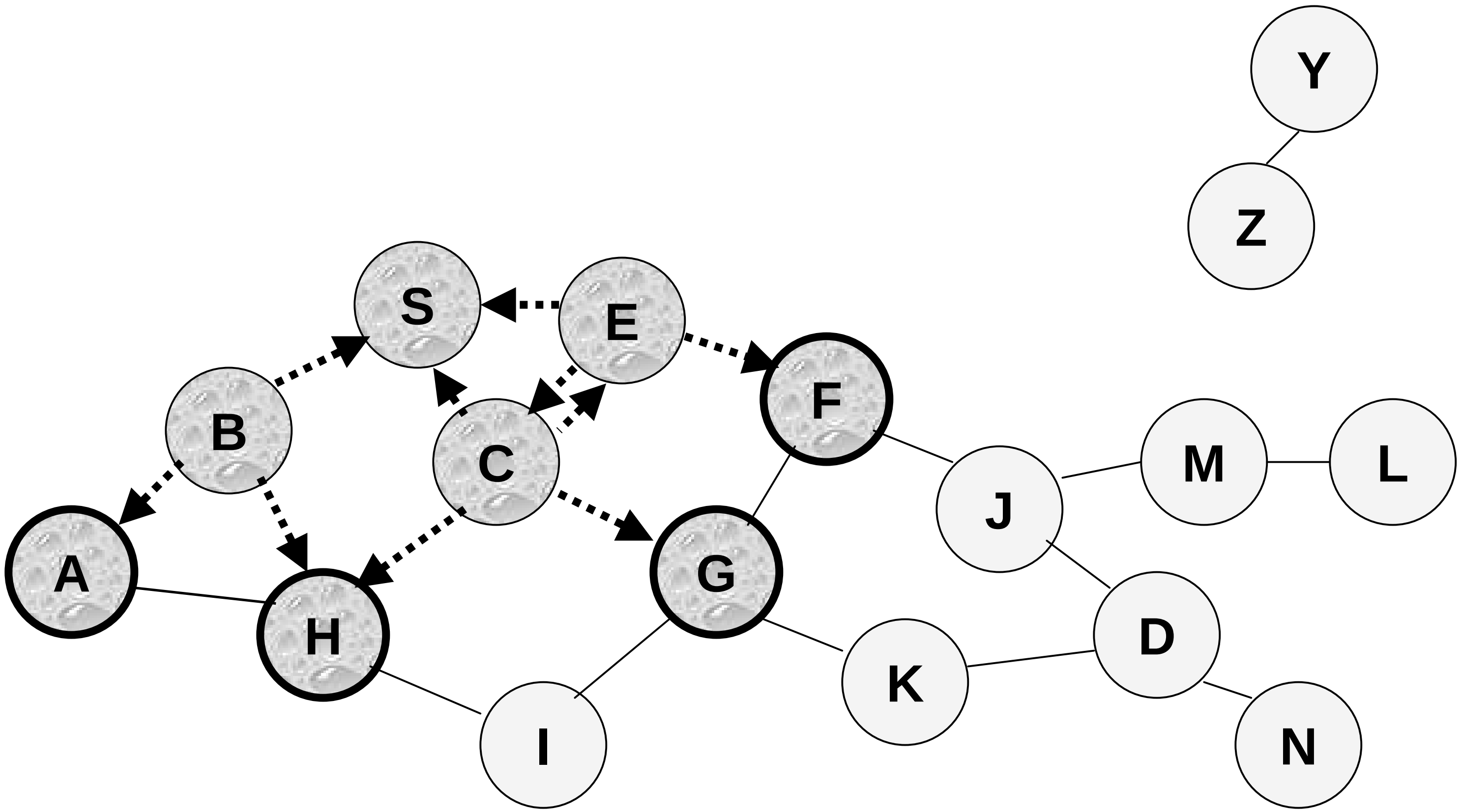
Flooding for Data Delivery



Represents a node that receives packet P for the first time

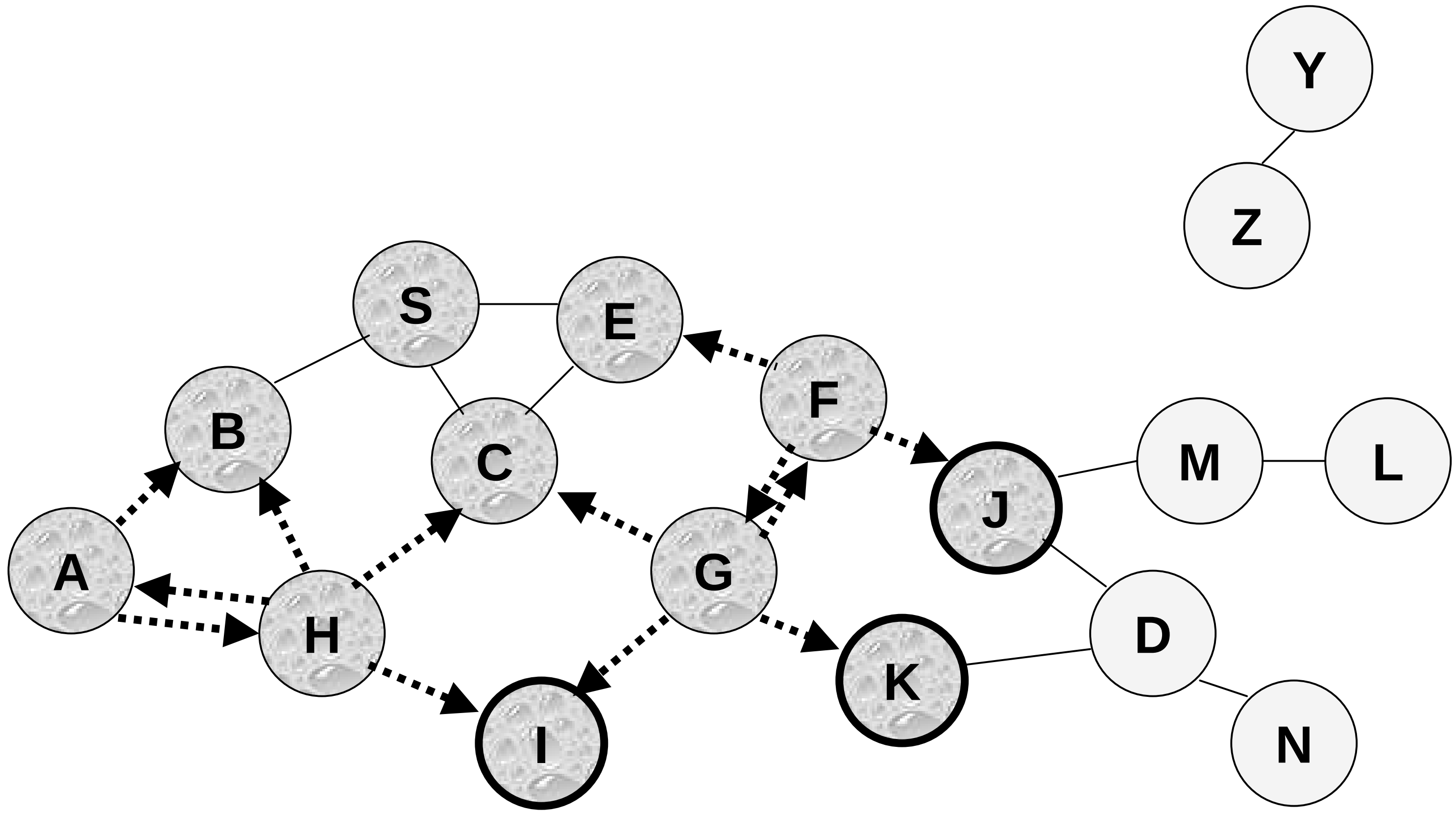
Represents transmission of packet P

Flooding for Data Delivery



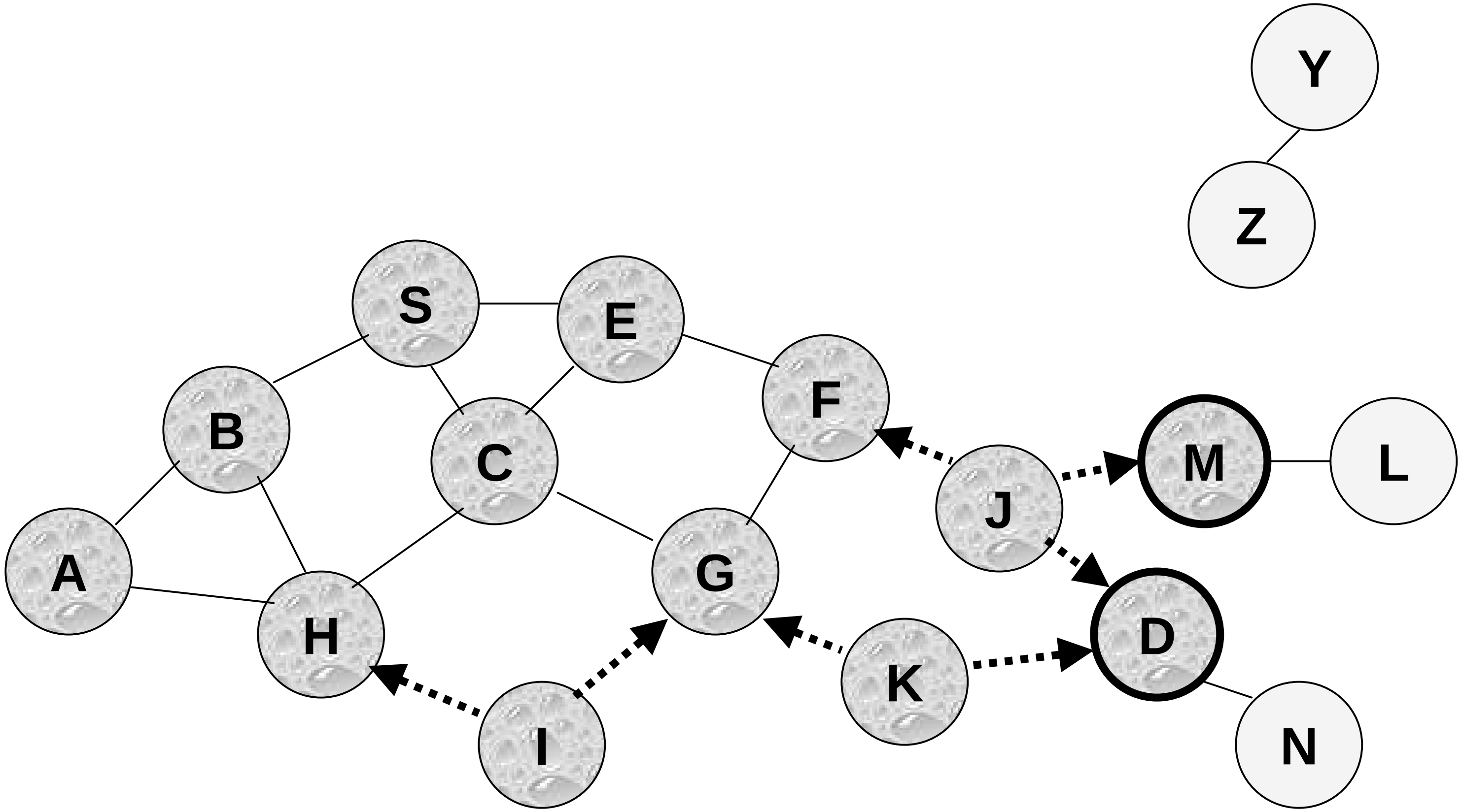
• **Node H receives packet P from two neighbors: potential for collision**

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**

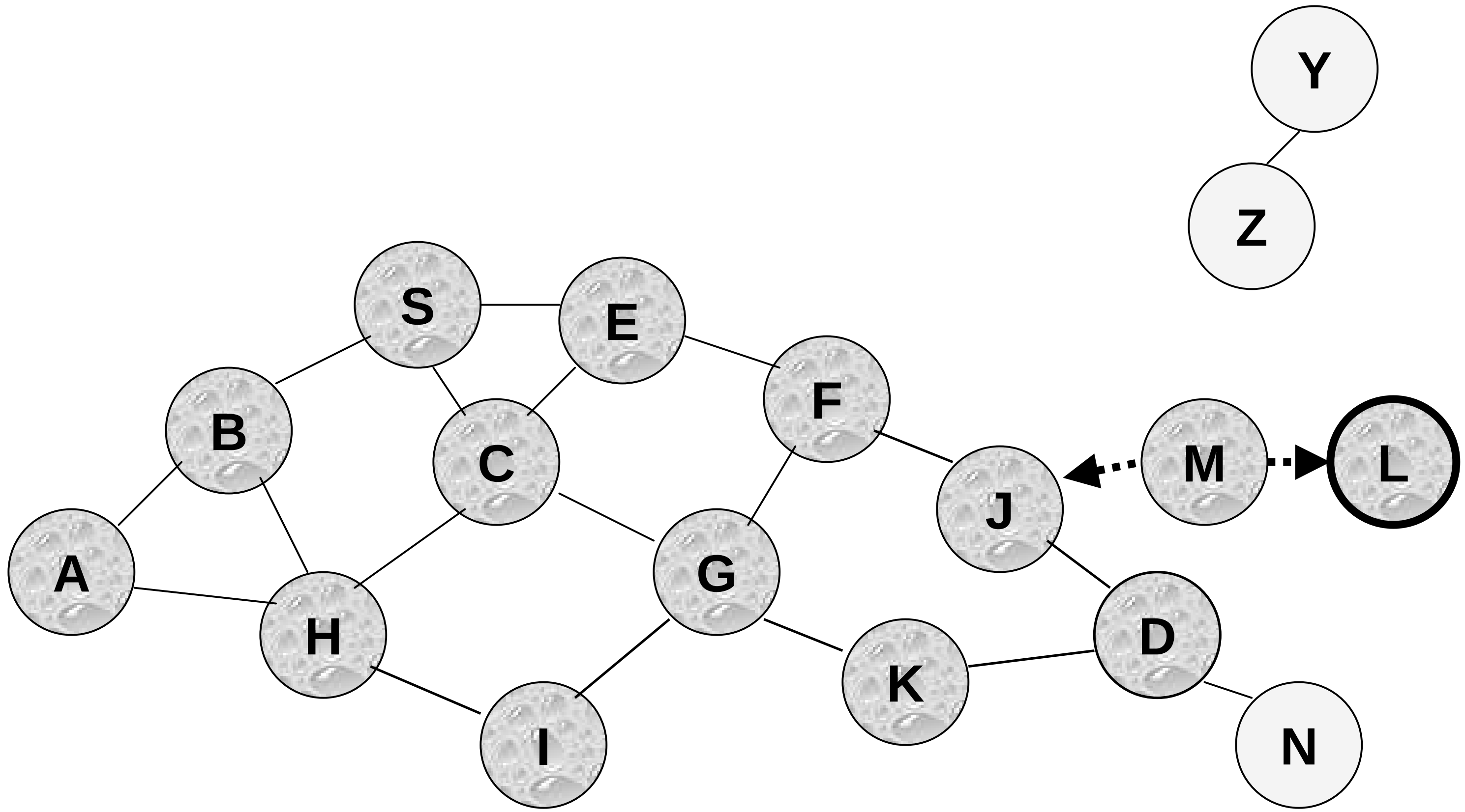
Flooding for Data Delivery



- **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**

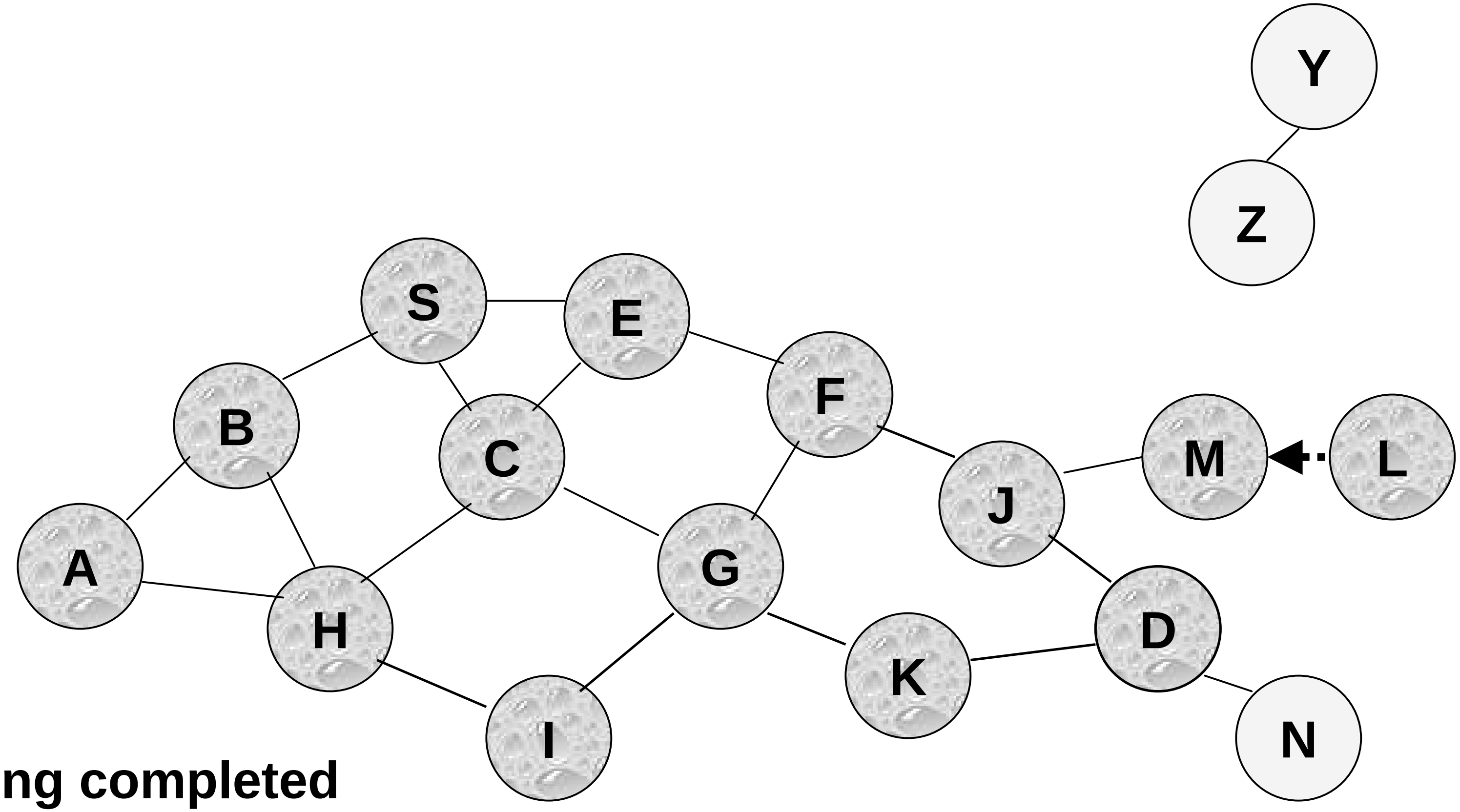
  => Packet P may not be delivered to node D at all, despite the use of flooding

Flooding for Data Delivery



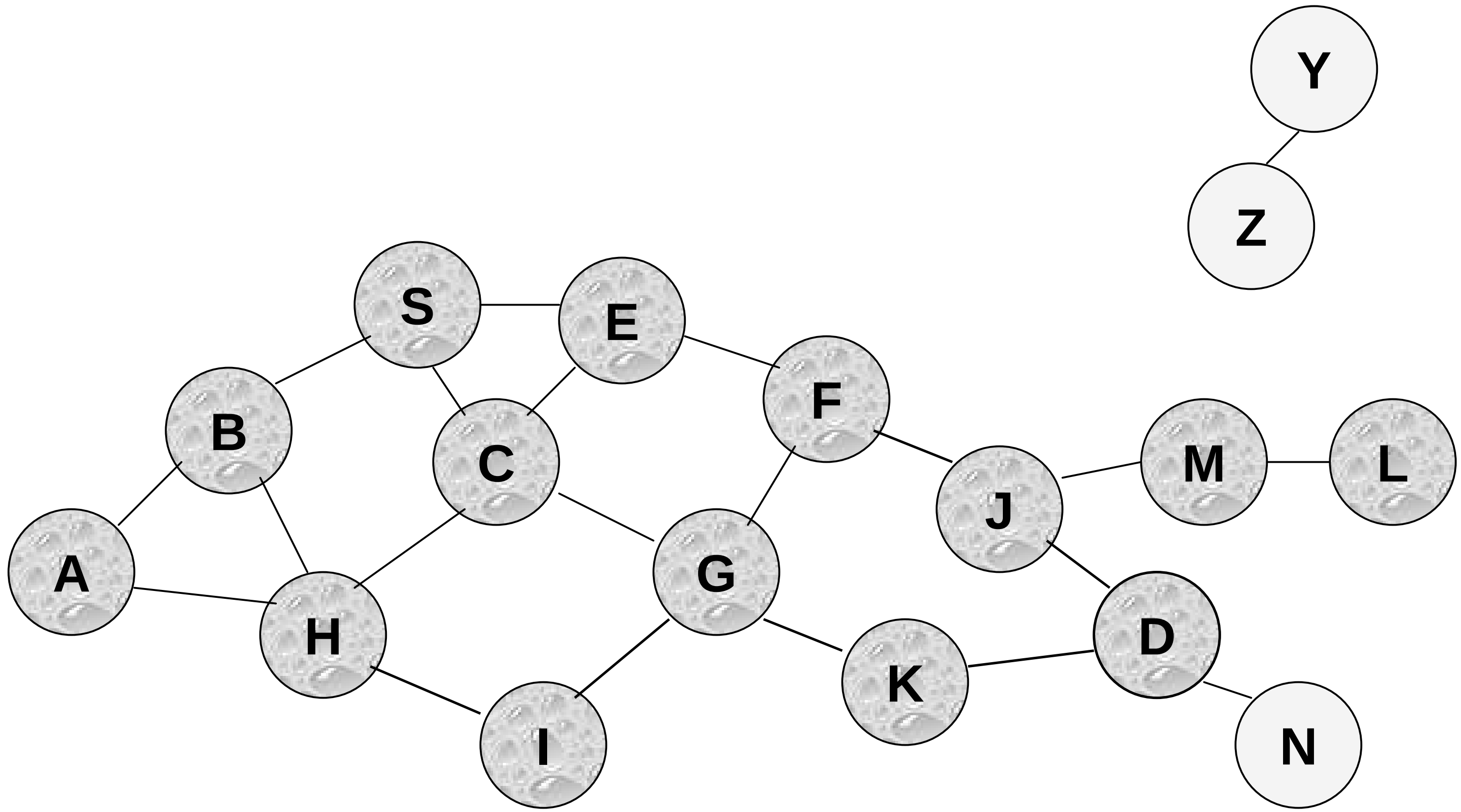
- **Node D does not forward packet P, because node D is the intended destination of packet P**

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

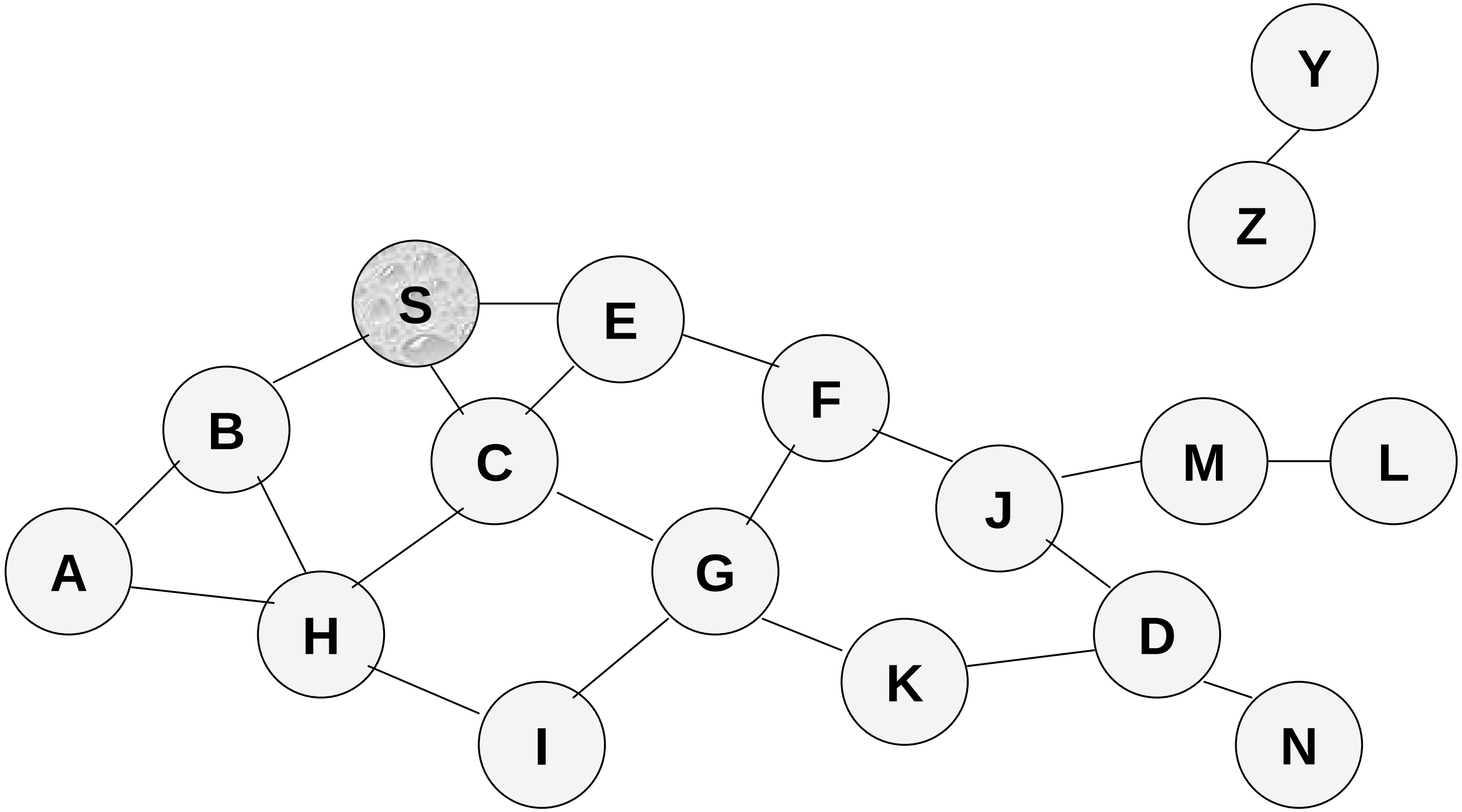
Flooding of Control Packets

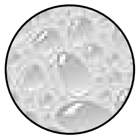
- Many protocols perform (potentially *limited*) flooding of control packets, instead of data packets
- The control packets are used to discover routes
- Discovered routes are subsequently used to send data packet(s)
- Overhead of control packet flooding is amortized over data packets transmitted between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

Dynamic Source Routing (DSR) [Johnson96]

- 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

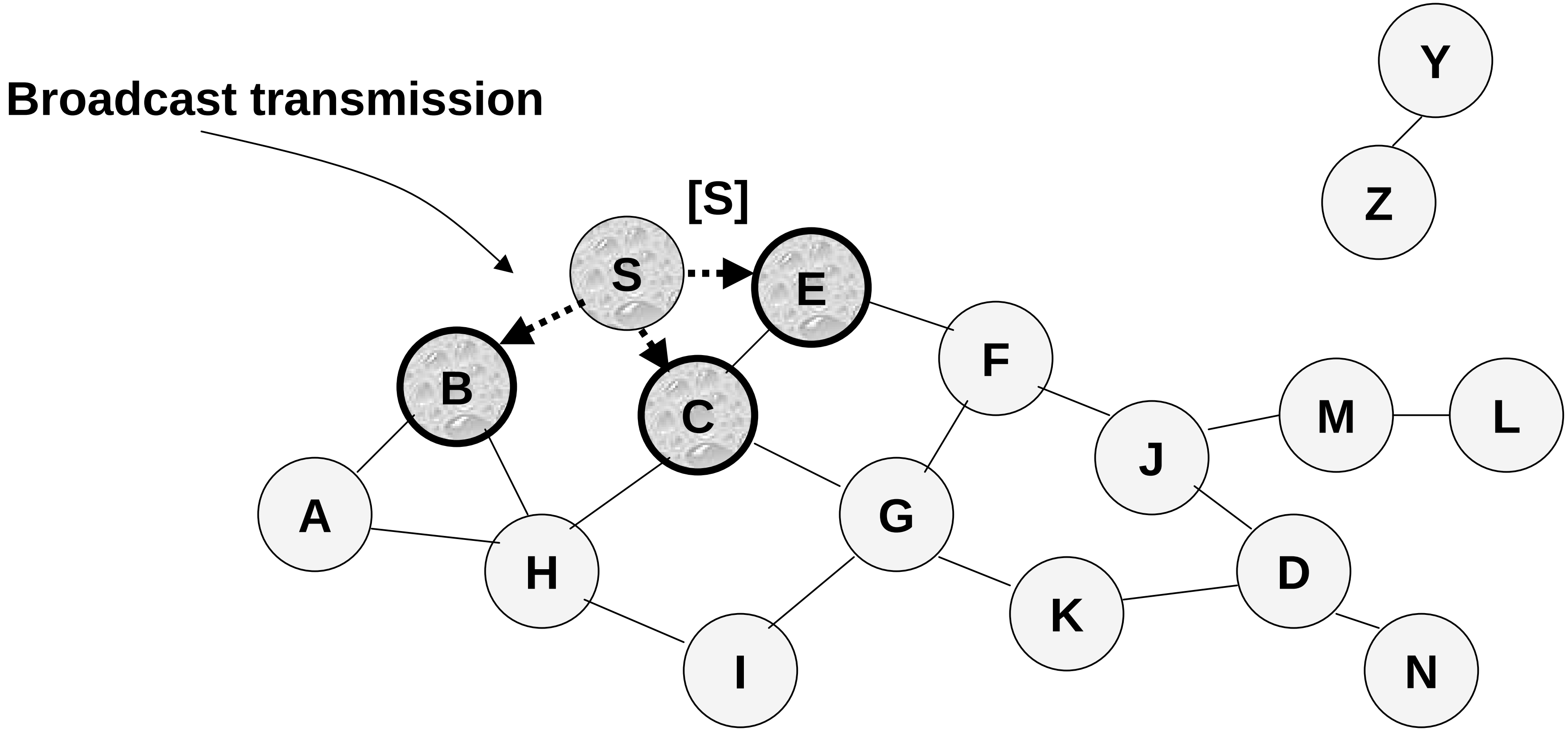
Route Discovery in DSR





Represents a node that has received RREQ for D from S

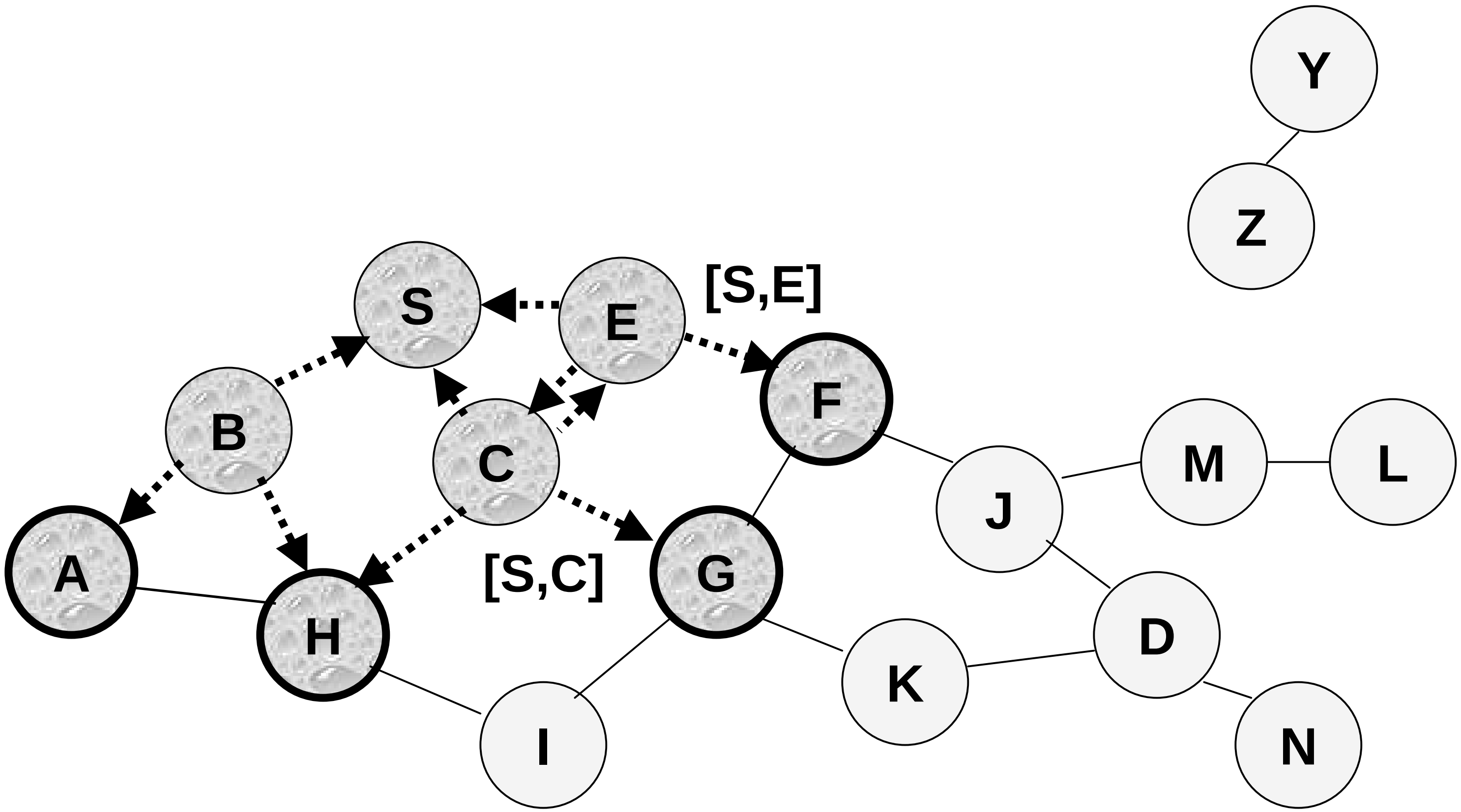
Route Discovery in DSR



······▶ Represents transmission of RREQ

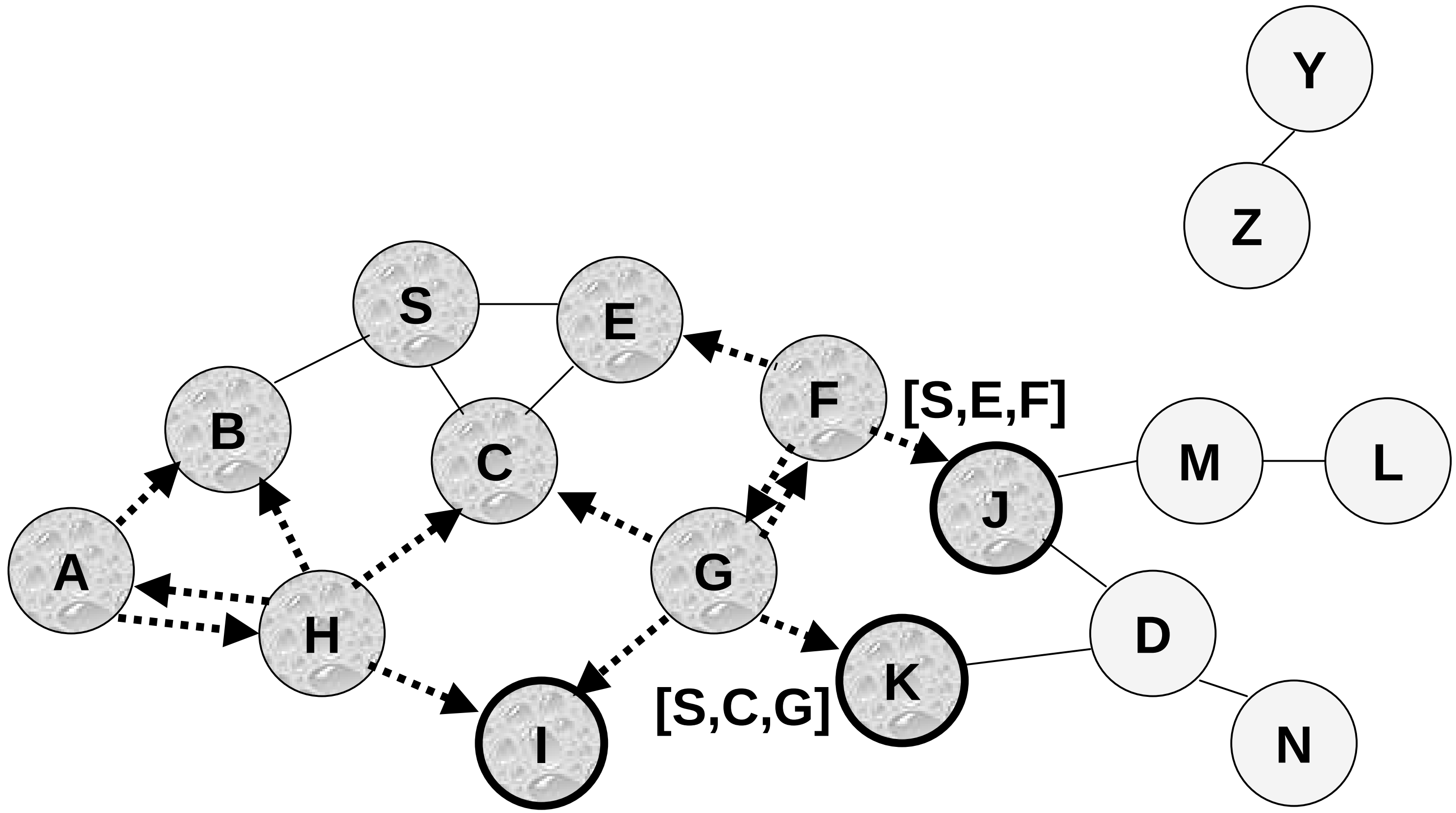
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



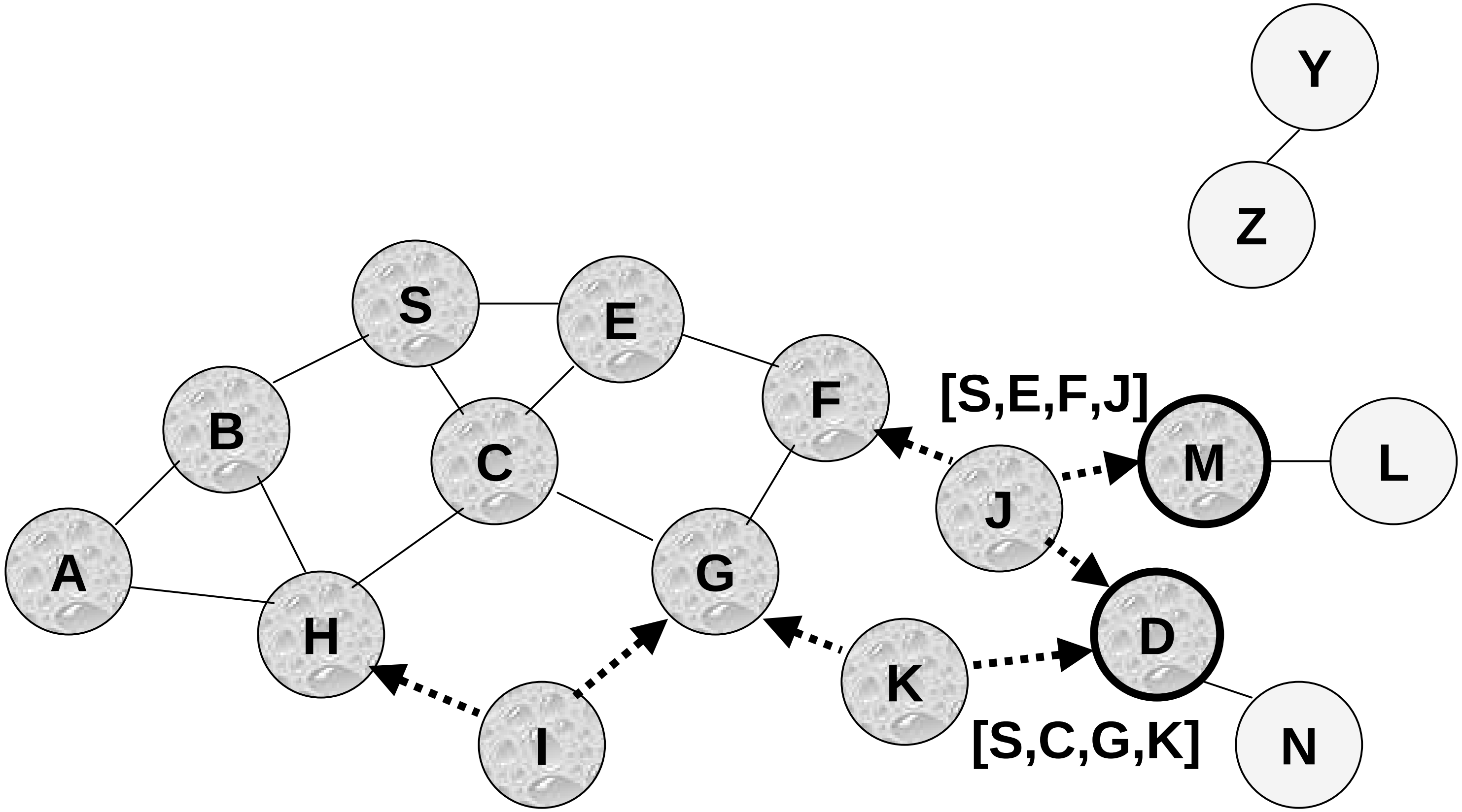
- **Node H receives packet RREQ from two neighbors: potential for collision**

Route Discovery in DSR



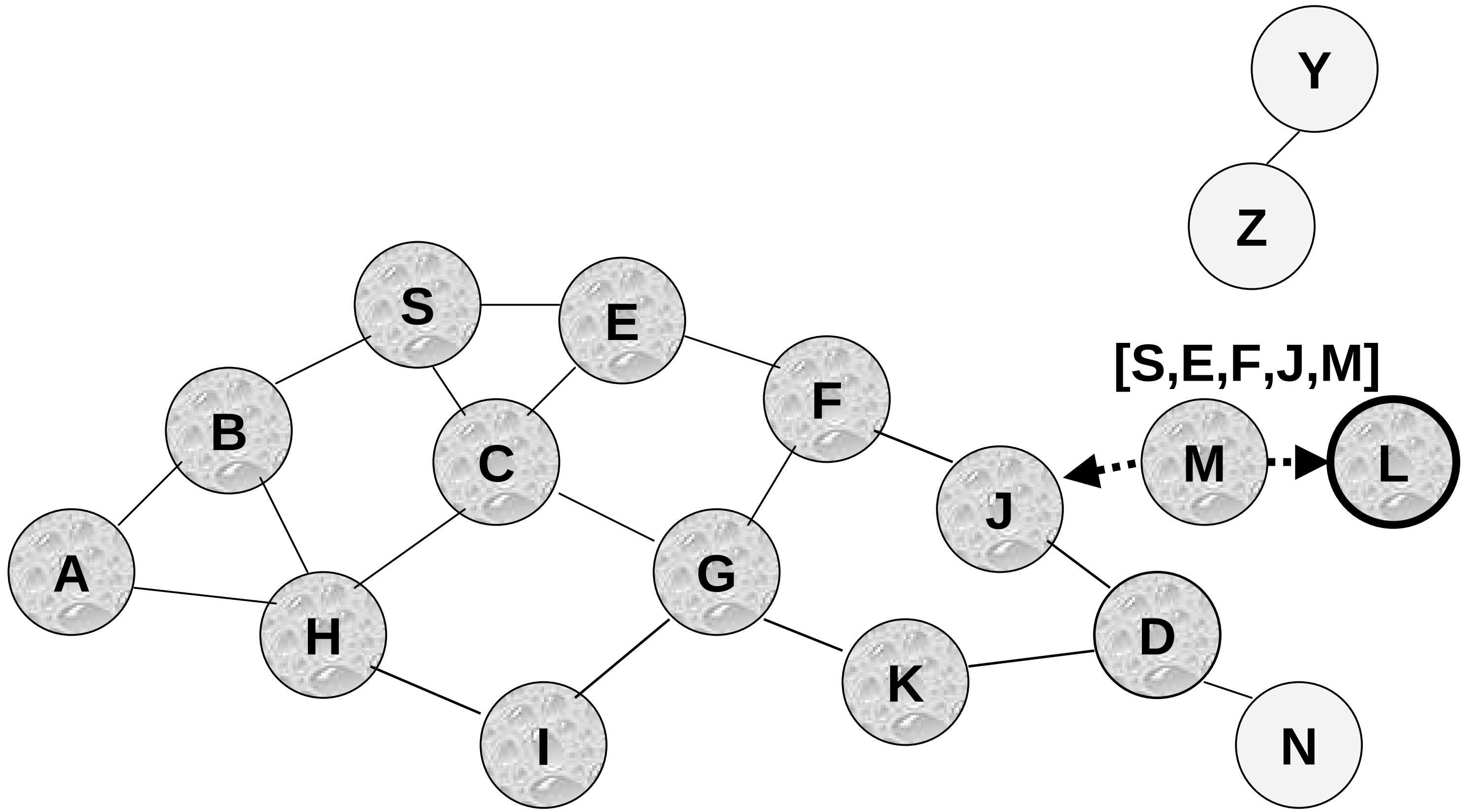
- **Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once**

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

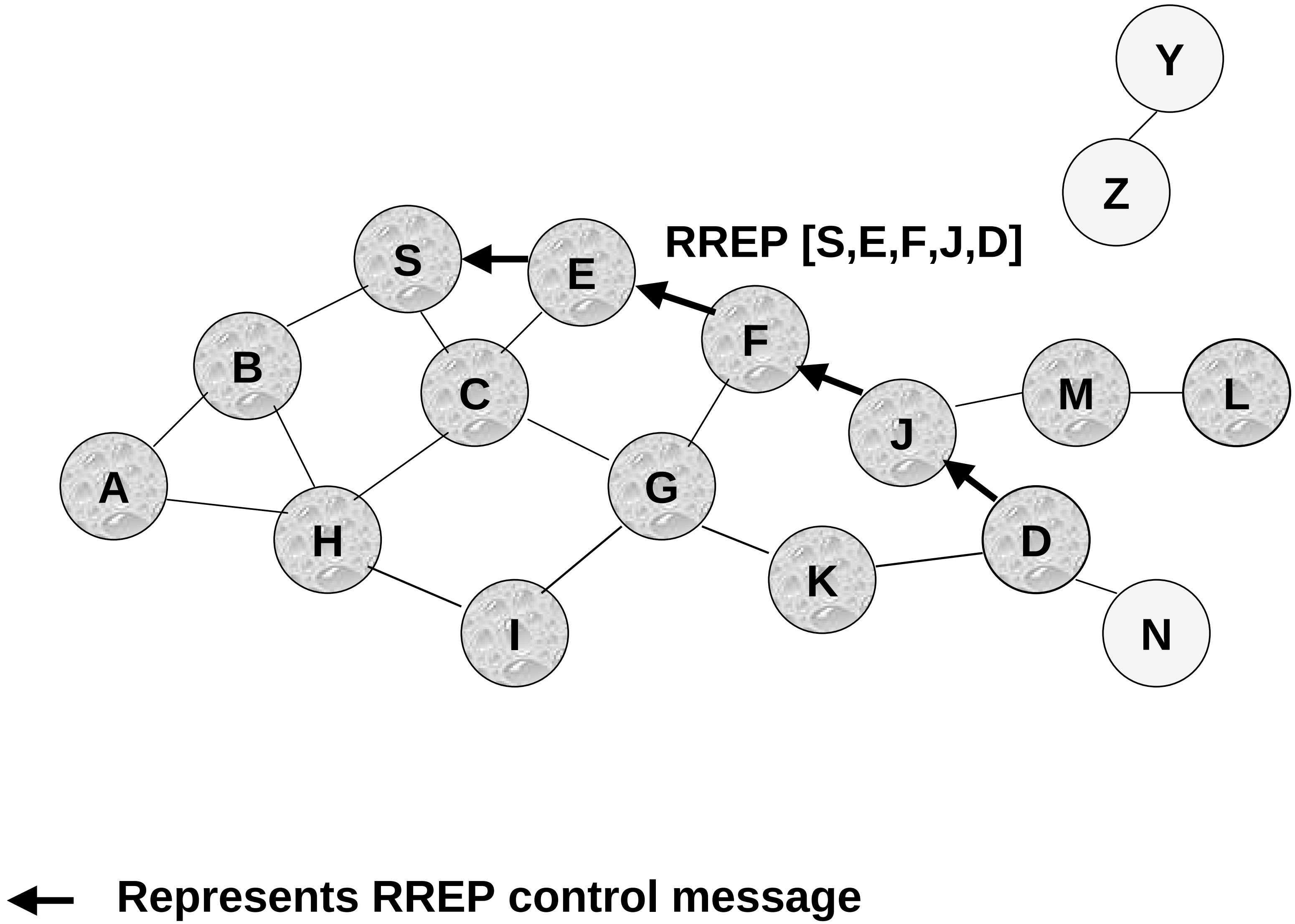


• **Node D does not forward RREQ, because node D is the intended target of the route discovery**

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



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

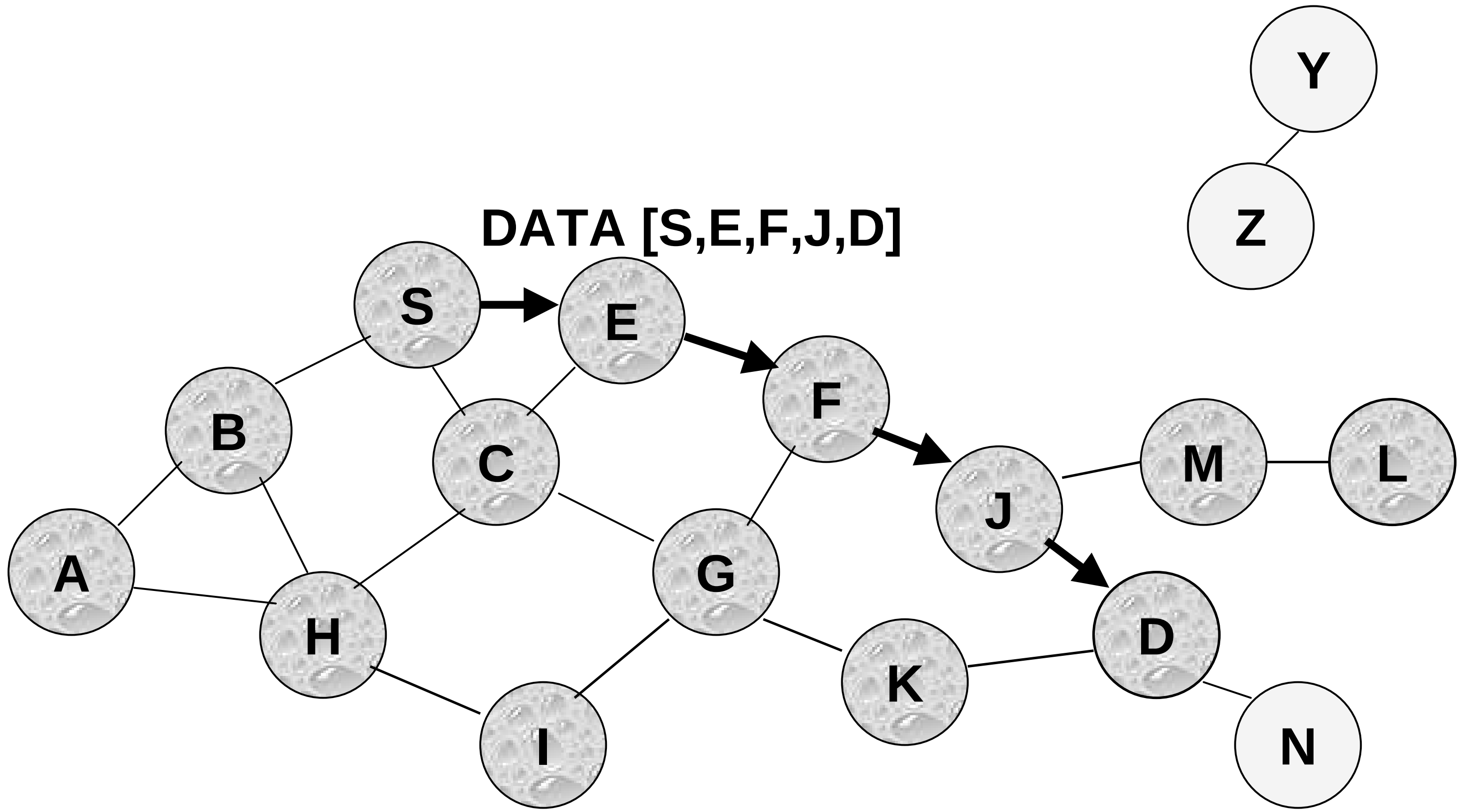
- If unidirectional (asymmetric) links are allowed, then RREP may need a route discovery for S from node D
  - Unless node D already knows a route to node S
  - If a route discovery is initiated by D for a route to S, then the Route Reply is piggybacked on the Route Request from D.

- 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 a packet should be forwarded

Data Delivery in DSR



Packet header 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

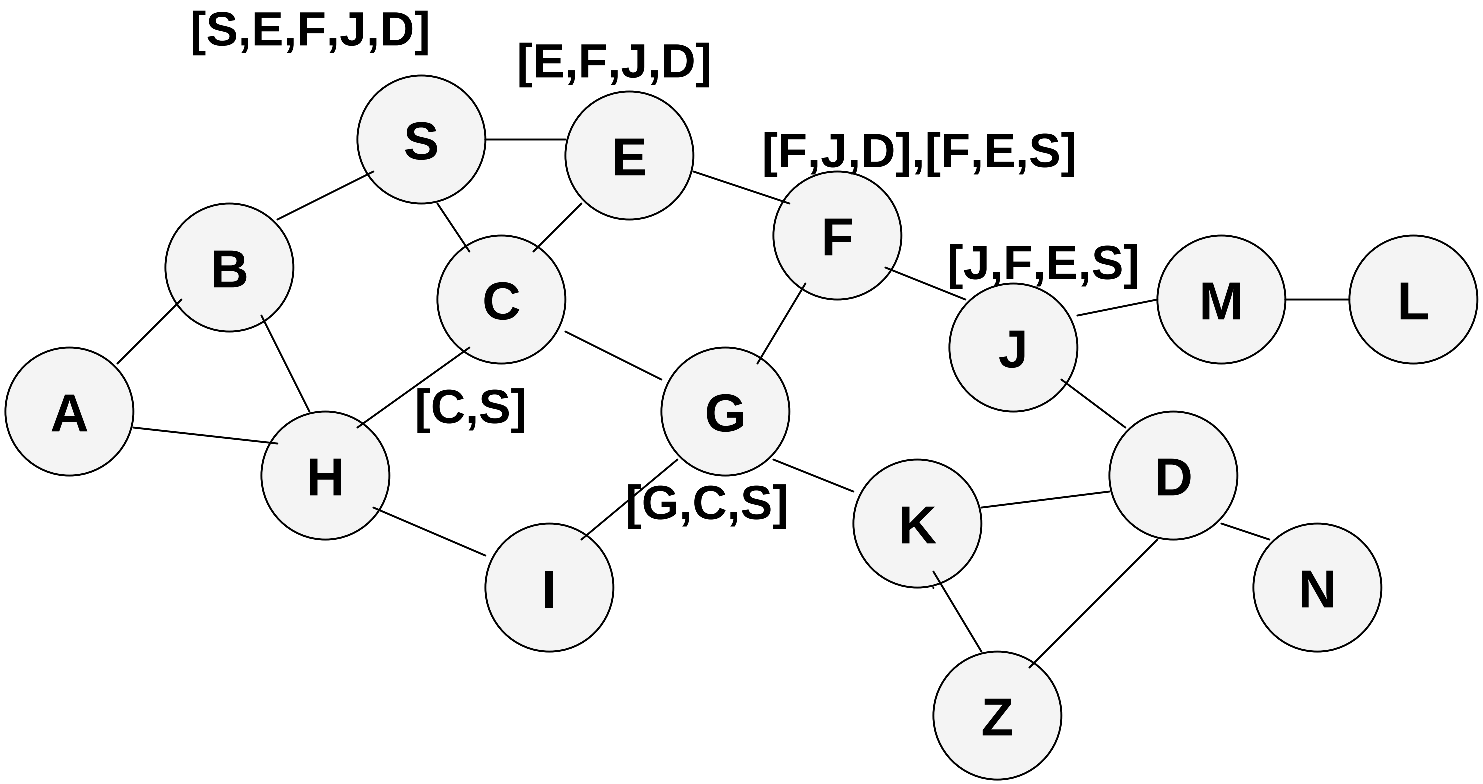
DSR Optimization: Route Caching

- 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, 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

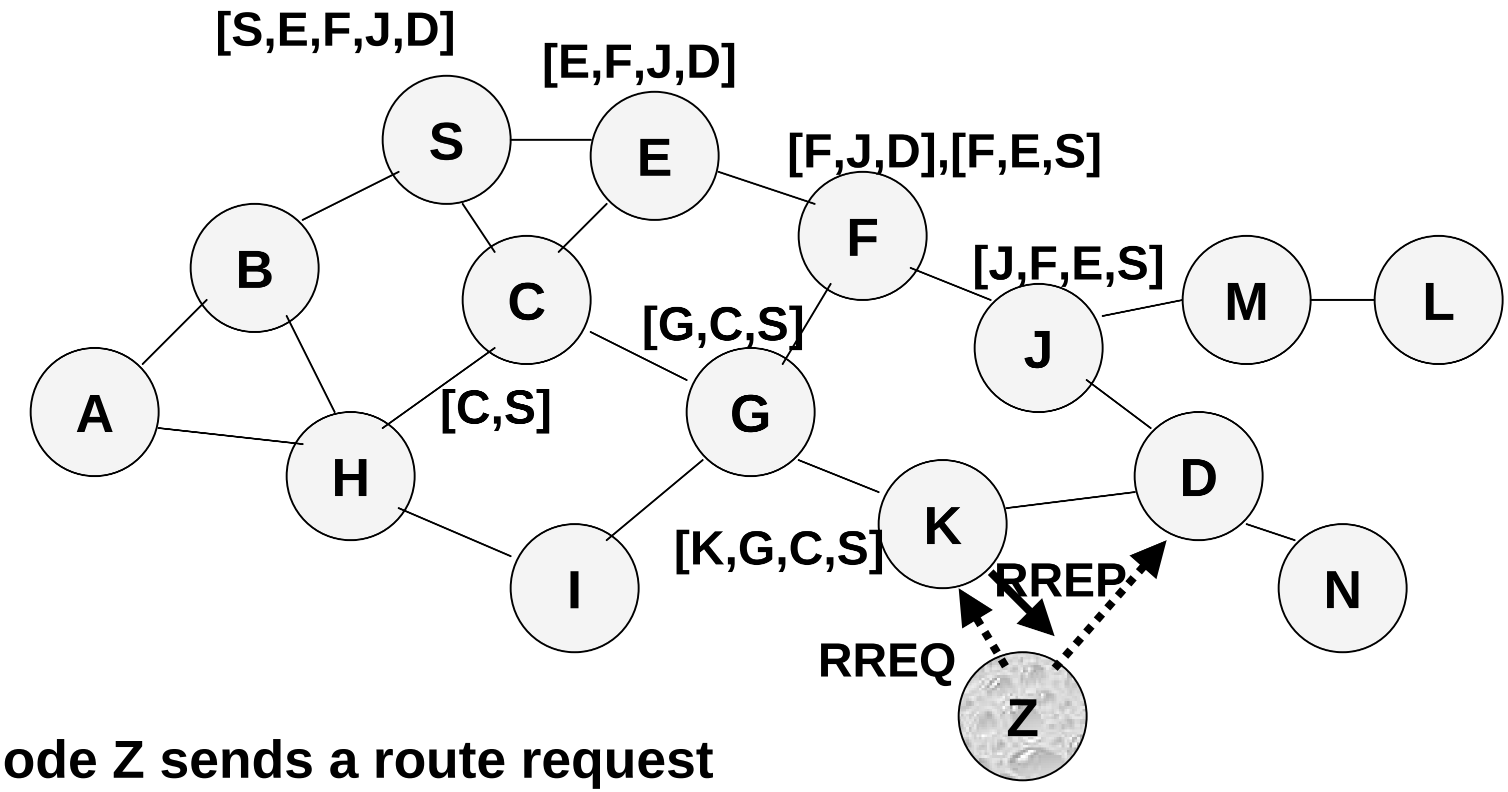
- When node S learns that a route to node D is broken, it uses another route from its local cache, if such a route to D exists in its cache. Otherwise, node S initiates route discovery by sending a route request
- Node X on receiving a Route Request for some node D can send a Route Reply if node X knows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

Use of Route Caching



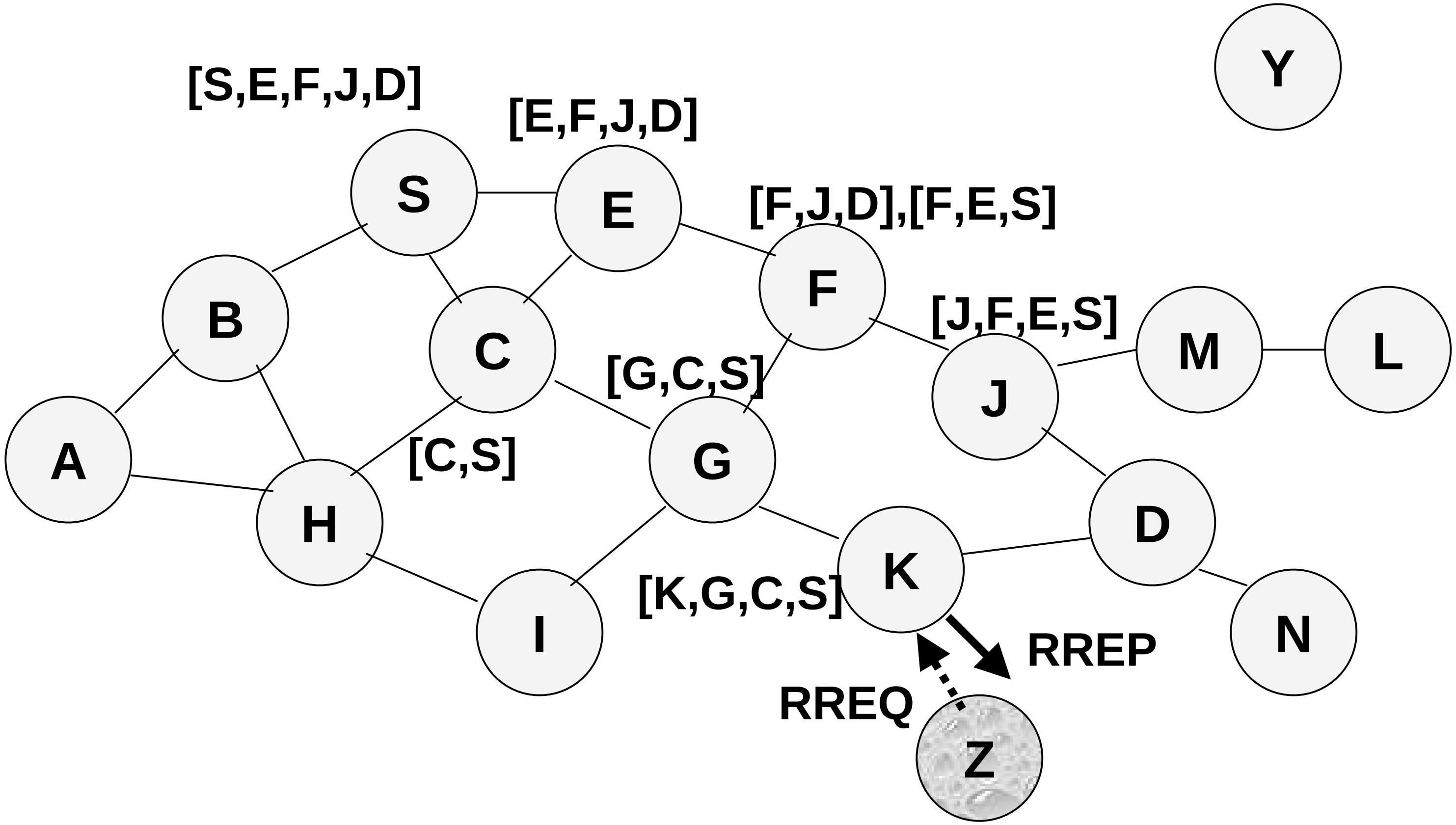
[P,Q,R]   Represents cached route at a node
(DSR maintains the cached routes in a tree format)

Use of Route Caching: Can Speed up Route Discovery



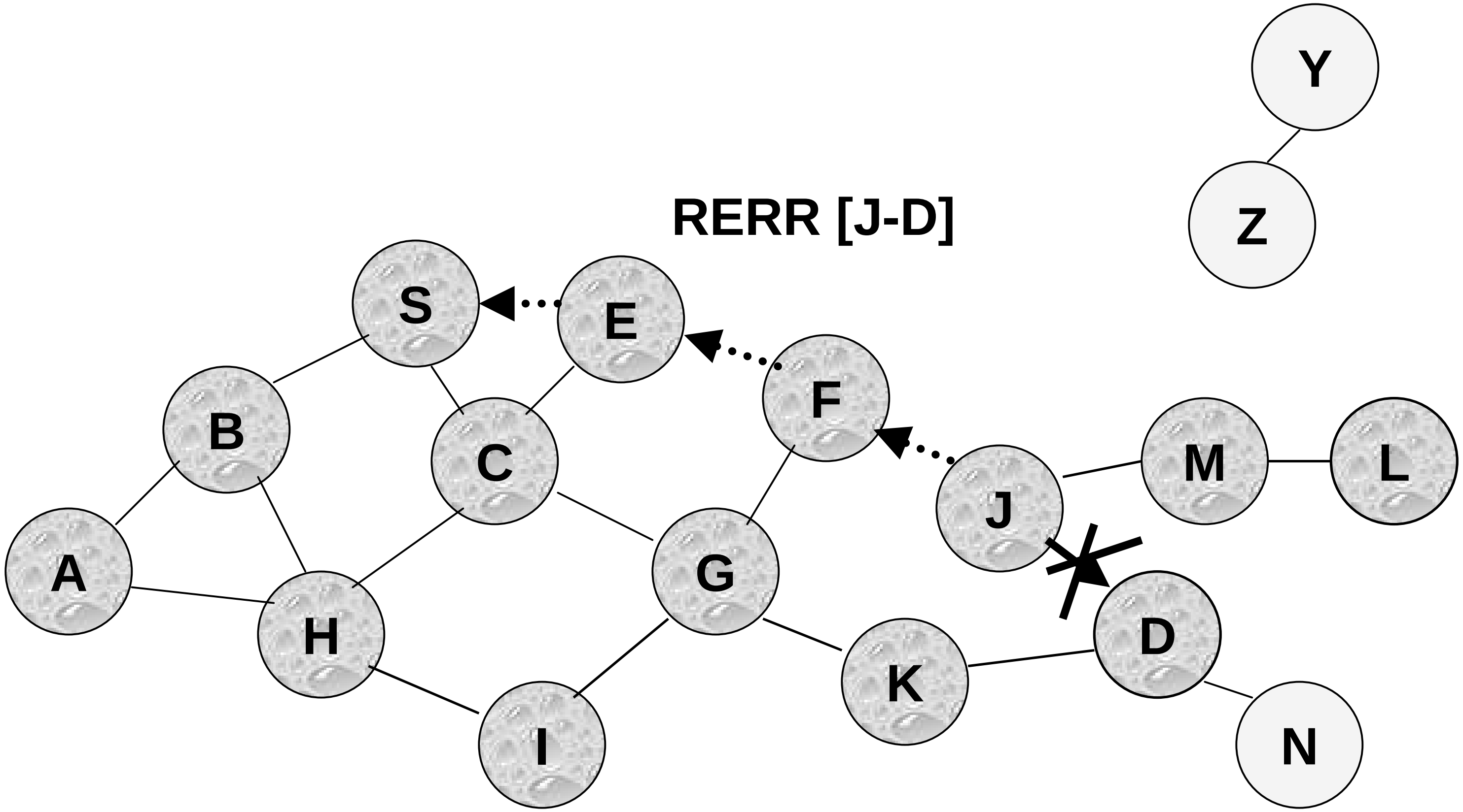
When node Z sends a route request for node C, node K sends back a route reply [Z,K,G,C] to node Z using a locally cached route

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

- 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.
  - Static timeouts
  - Adaptive timeouts based on link stability

Flooding of Control Packets

- How to reduce the scope of the route request flood ?
  - LAR [Ko98Mobicom]
  - Query localization [Castaneda99Mobicom]

- How to reduce redundant broadcasts ?
  - The Broadcast Storm Problem [Ni99Mobicom]

Location-Aided Routing (LAR) [Ko98Mobicom]

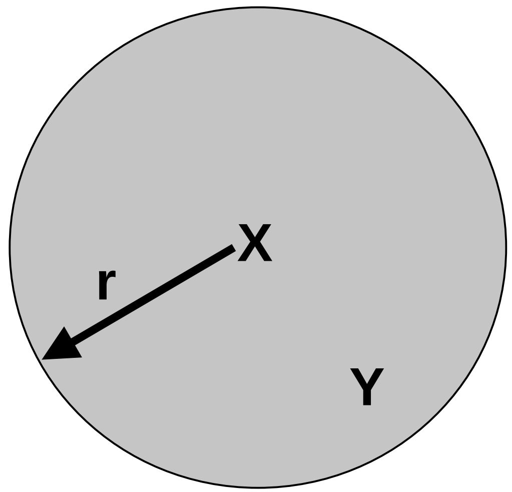
- Exploits location information to limit scope of route request flood
  - Location information may be obtained using GPS
- *Expected Zone* is determined as a region that is expected to hold the current location of the destination
  - Expected zone determined based on potentially old location information, and knowledge of the destination's speed
- Route requests limited to a *Request Zone* that contains the Expected Zone and location of the sender node

Expected Zone in LAR

X = last known location of node D, at time t0

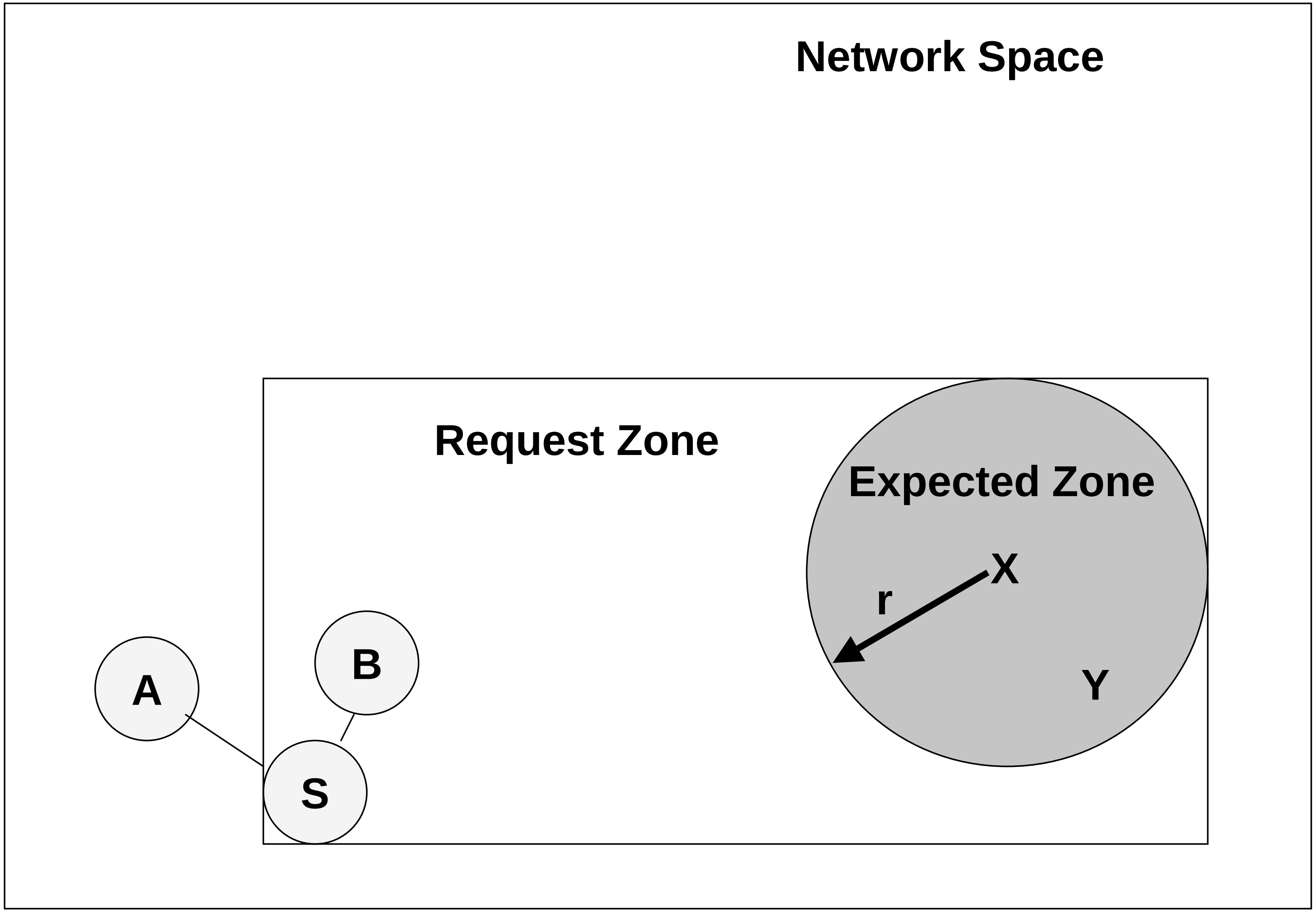
Y = location of node D at current time t1, unknown to node S

r = (t1 - t0) * estimate of D's speed



Expected Zone

Request Zone in LAR



LAR

- Only nodes within the request zone forward route requests
  - Node A does not forward RREQ, but node B does (see previous slide)
- Request zone explicitly specified in the route request
- Each node must know its physical location to determine whether it is within the request zone

LAR

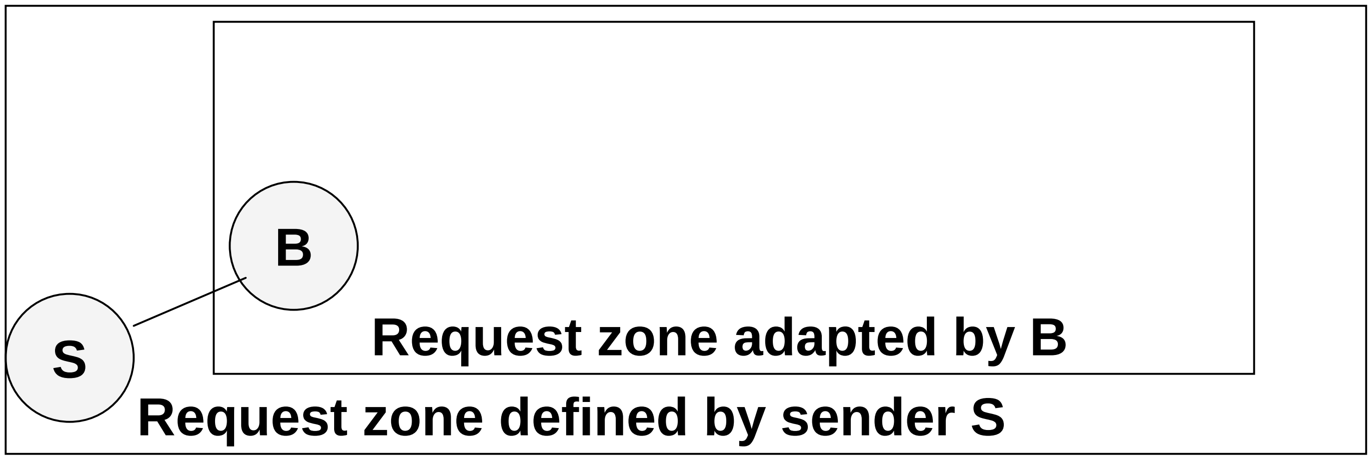
- Only nodes within the request zone forward route requests

- If route discovery using the smaller request zone fails to find a route, the sender initiates another route discovery (after a timeout) using a larger request zone
  - the larger request zone may be the entire network

- Rest of route discovery protocol similar to DSR

LAR Variations: Adaptive Request Zone

- Each node may modify the request zone included in the forwarded request
- Modified request zone may be determined using more recent/accurate information, and may be smaller than the original request zone



LAR Variations: Implicit Request Zone

- In the previous scheme, a route request explicitly specified a request zone
- Alternative approach: A node X forwards a route request received from Y if node X is deemed to be closer to the expected zone as compared to Y
- The motivation is to attempt to bring the route request physically closer to the destination node after each forwarding

Location-Aided Routing

- The basic proposal assumes that, *initially,* location information for node X becomes known to Y only during a route discovery
- This location information is used for a future route discovery
  - Each route discovery yields more updated information which is used for the next discovery

Variations

- Location information can also be piggybacked on any message from Y to X
- Y may also proactively distribute its location information
  - Similar to other protocols discussed later (e.g., DREAM)

Location Aided Routing (LAR)

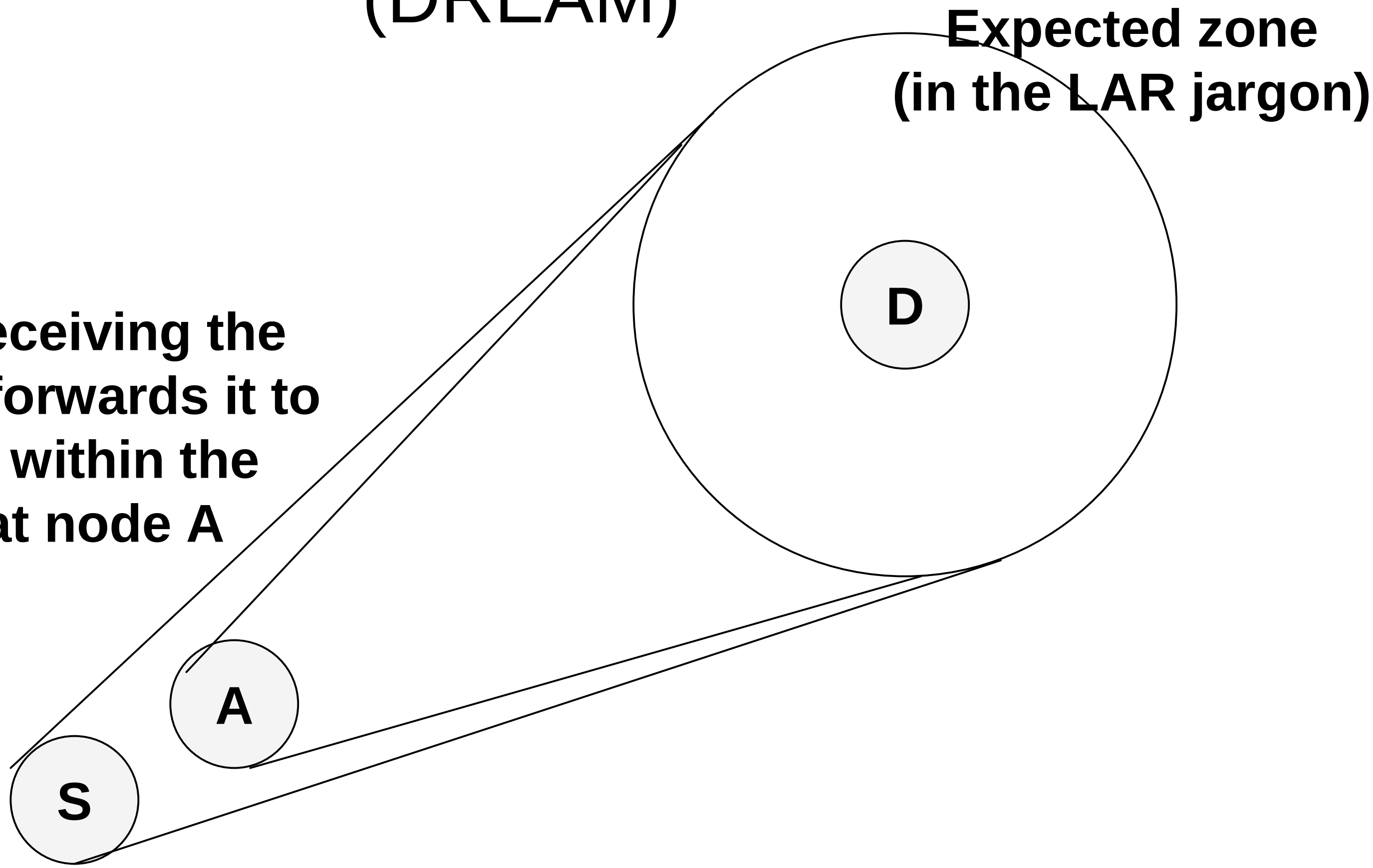
- Advantages
  - reduces the scope of route request flood
  - reduces overhead of route discovery

- Disadvantages
  - Nodes need to know their physical locations
  - Request zone may be partitioned

Distance Routing Effect Algorithm for Mobility (DREAM) [Basagni98Mobicom]

- Uses location and speed information (like LAR)
- DREAM uses flooding of *data packets* as the routing mechanism (unlike LAR)
  - DREAM uses location information to limit the flood of data packets to a small region

Distance Routing Effect Algorithm for Mobility (DREAM)



Node A, on receiving the data packet, forwards it to its neighbors within the cone rooted at node A

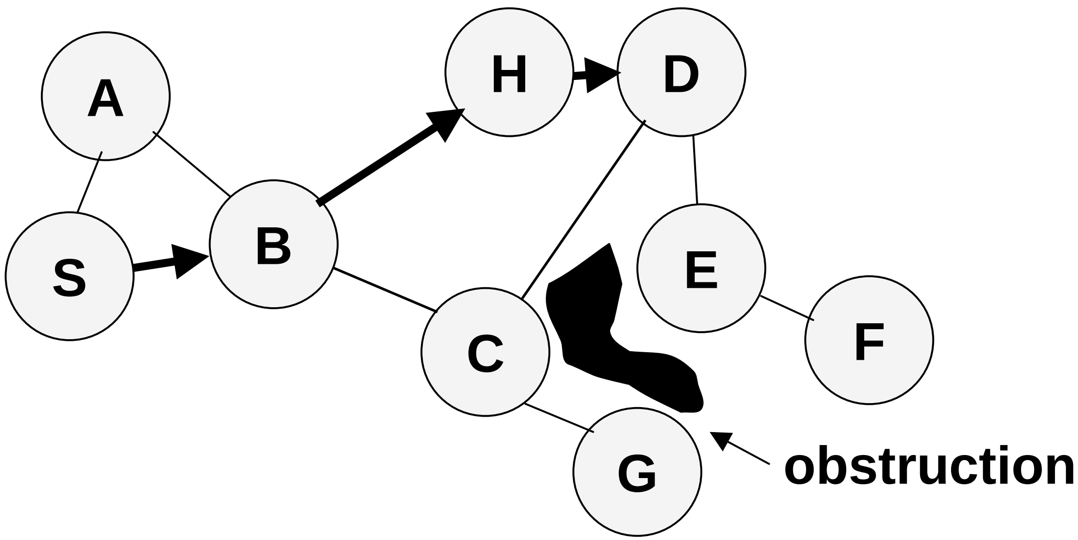
S sends *data packet* to all neighbors in the cone rooted at node S

Distance Routing Effect Algorithm for Mobility (DREAM)

- Nodes periodically broadcast their physical location
- Nearby nodes are updated more frequently, far away nodes less frequently
- Distance effect: Far away nodes seem to move at a lower angular speed as compared to nearby nodes
- Location update's time-to-live field used to control how far the information is propagated

Geographic Distance Routing (GEDIR) [Lin98]

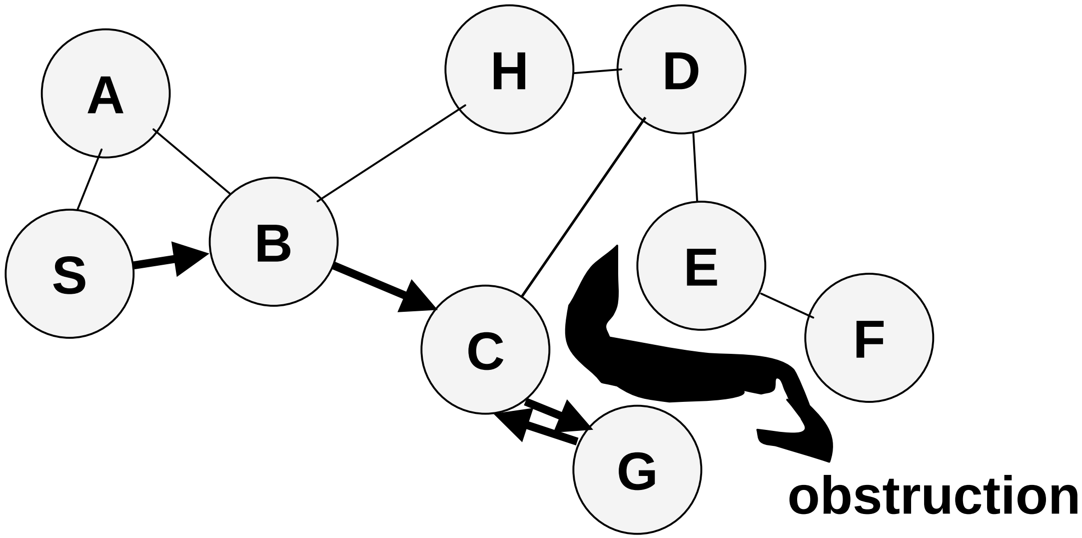
- Location of the destination node is assumed known
- Each node knows location of its neighbors
- Each node forwards a packet to its neighbor closest to the destination
- Route taken from S to D shown below



Geographic Distance Routing (GEDIR) [Stojmenovic99]

- The algorithm terminates when same edge traversed twice consecutively

- Algorithm fails to route from S to E
  - Node G is the neighbor of C who is closest from destination E, but C does not have a route to E



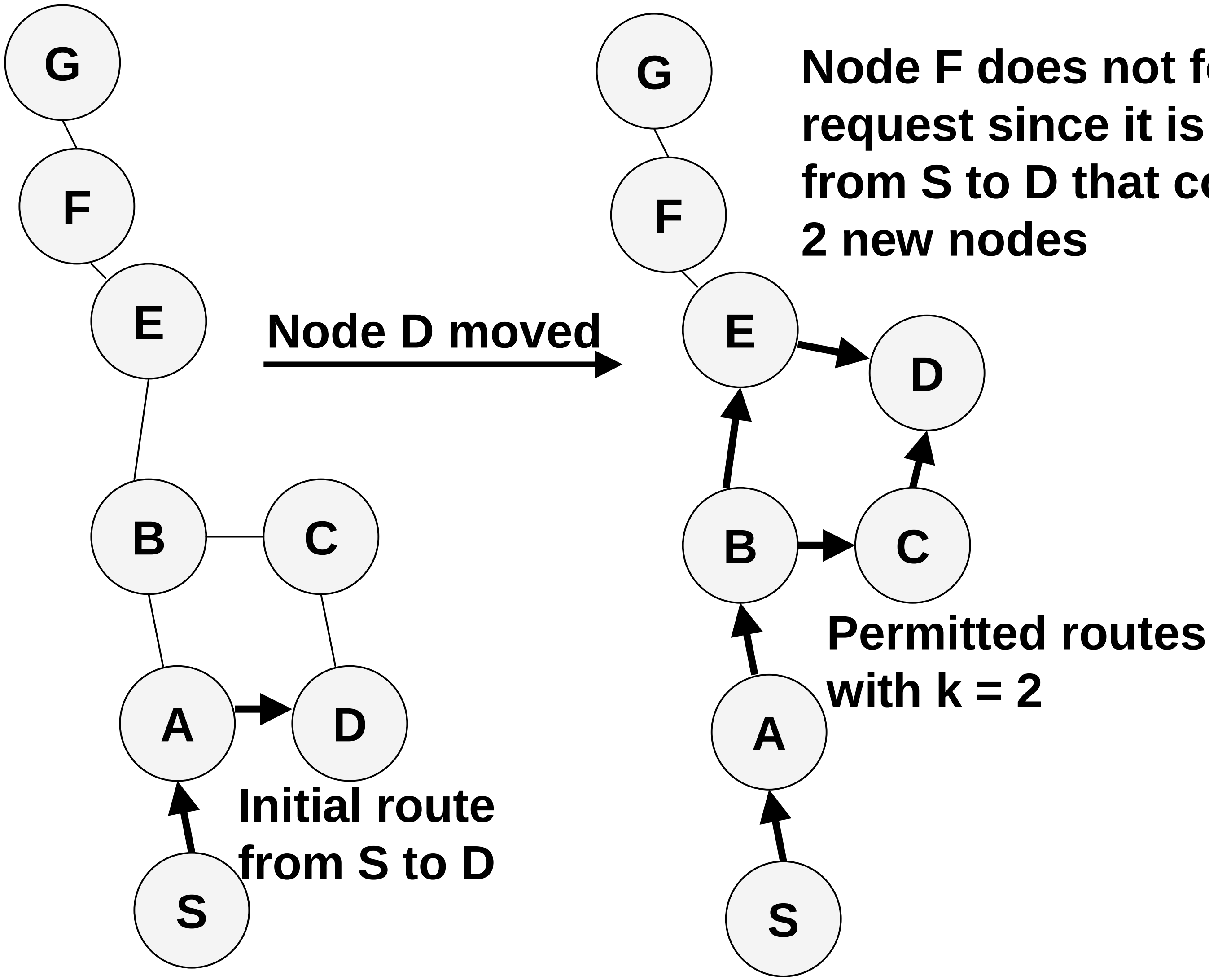
Query Localization [Castaneda99Mobicom]

- Limits route request flood without using physical information
- Route requests are propagated only along paths that are *close* to the previously known route
- The *closeness* property is defined without using physical location information

Query Localization

- Path locality heuristic: Look for a new path that contains at most *k* nodes that were not present in the previously known route
- Old route is piggybacked on a Route Request
- Route Request is forwarded only if the accumulated route in the Route Request contains at most *k* new nodes that were absent in the old route
  - this limits propagation of the route request

Query Localization: Example



Node F does not forward the route request since it is not on any route from S to D that contains at most 2 new nodes

Query Localization

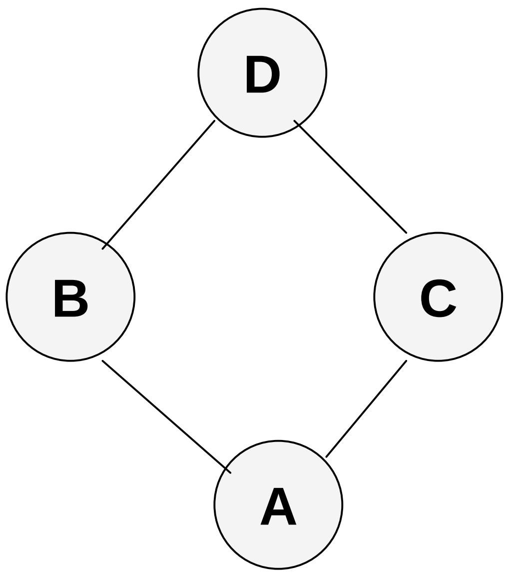
- Advantages:
  - Reduces overhead of route discovery without using physical location information
  - Can perform better in presence of obstructions by searching for new routes in the *vicinity* of old routes

- Disadvantage:
  - May yield routes longer than LAR

    (Shortest route may contain more than k new nodes)

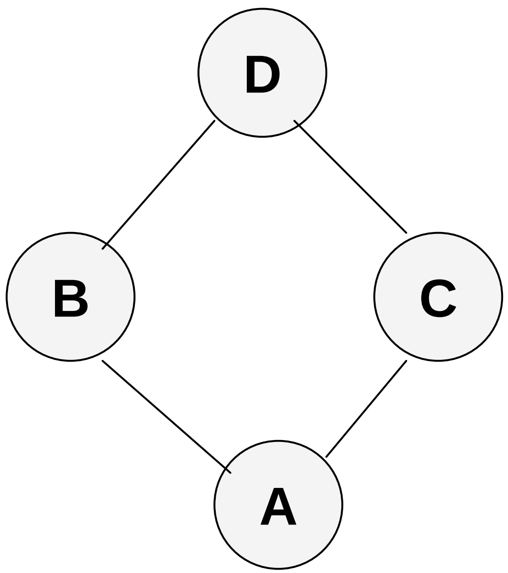
Broadcast Storm Problem [Ni99Mobicom]

- When node A broadcasts a route query, nodes B and C both receive it
- B and C both forward to their neighbors
- B and C transmit at about the same time since they are reacting to receipt of the same message from A
- This results in a high probability of collisions



Broadcast Storm Problem

- Redundancy: A given node may receive the same route request from too many nodes, when one copy would have sufficed
- Node D may receive from nodes B and C both



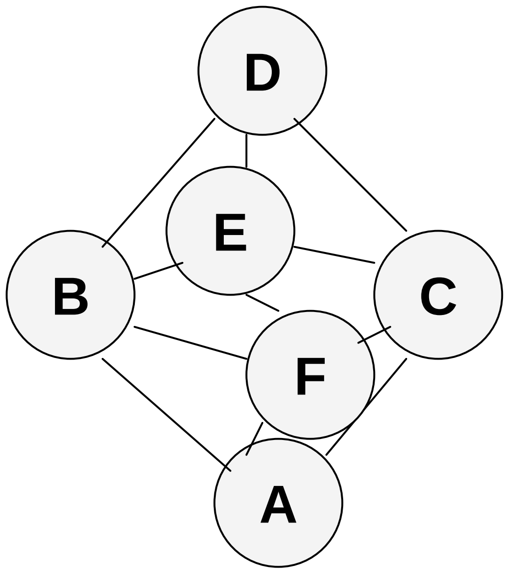
Solutions for Broadcast Storm

- Probabilistic scheme: On receiving a route request for the first time, a node will re-broadcast (forward) the request with probability p

- Also, re-broadcasts by different nodes should be staggered by using a collision avoidance technique (wait a random delay when channel is idle)
  - this would reduce the probability that nodes B and C would forward a packet simultaneously in the previous example

Solutions for Broadcast Storms

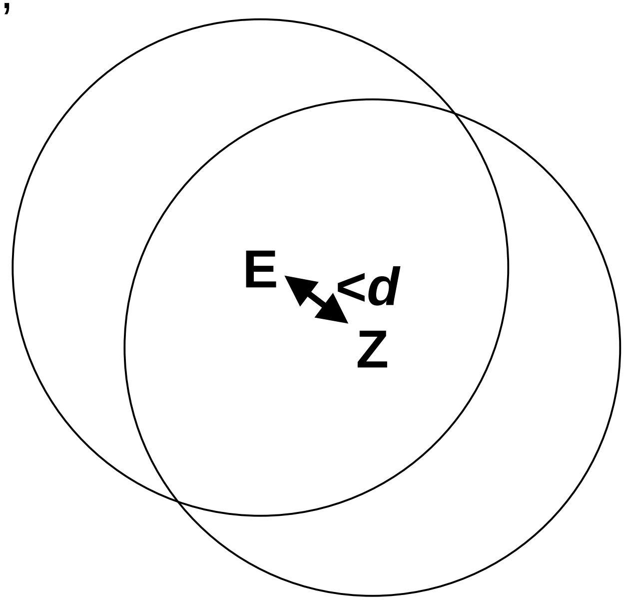
- Counter-Based Scheme: If node E hears more than *k* neighbors broadcasting a given route request, before it can itself forward it, then node E will not forward the request
- Intuition: *k* neighbors together have probably already forwarded the request to all of E’s neighbors



Solutions for Broadcast Storms

- Distance-Based Scheme: If node E hears RREQ broadcasted by some node Z within physical distance *d*, then E will not re-broadcast the request

- Intuition: Z and E are too close, so transmission areas covered by Z and E are not very different
  - if E re-broadcasts the request, not many nodes who have not already heard the request from Z will hear the request



Summary: Broadcast Storm Problem

- Flooding is used in many protocols, such as Dynamic Source Routing (DSR)

- Problems associated with flooding
  - collisions
  - redundancy

- Collisions may be reduced by “jittering” (waiting for a random interval before propagating the flood)

- Redundancy may be reduced by selectively re-broadcasting packets from only a subset of the nodes

Summary

- Ad hoc protocols can be classified into proactive and reactive
- Another classification is whether they use location information
- A basic problem is to reduce the flooding overhead (e.g. by using location information)
- Scalability for large networks (large number of hops) is potentially a problem

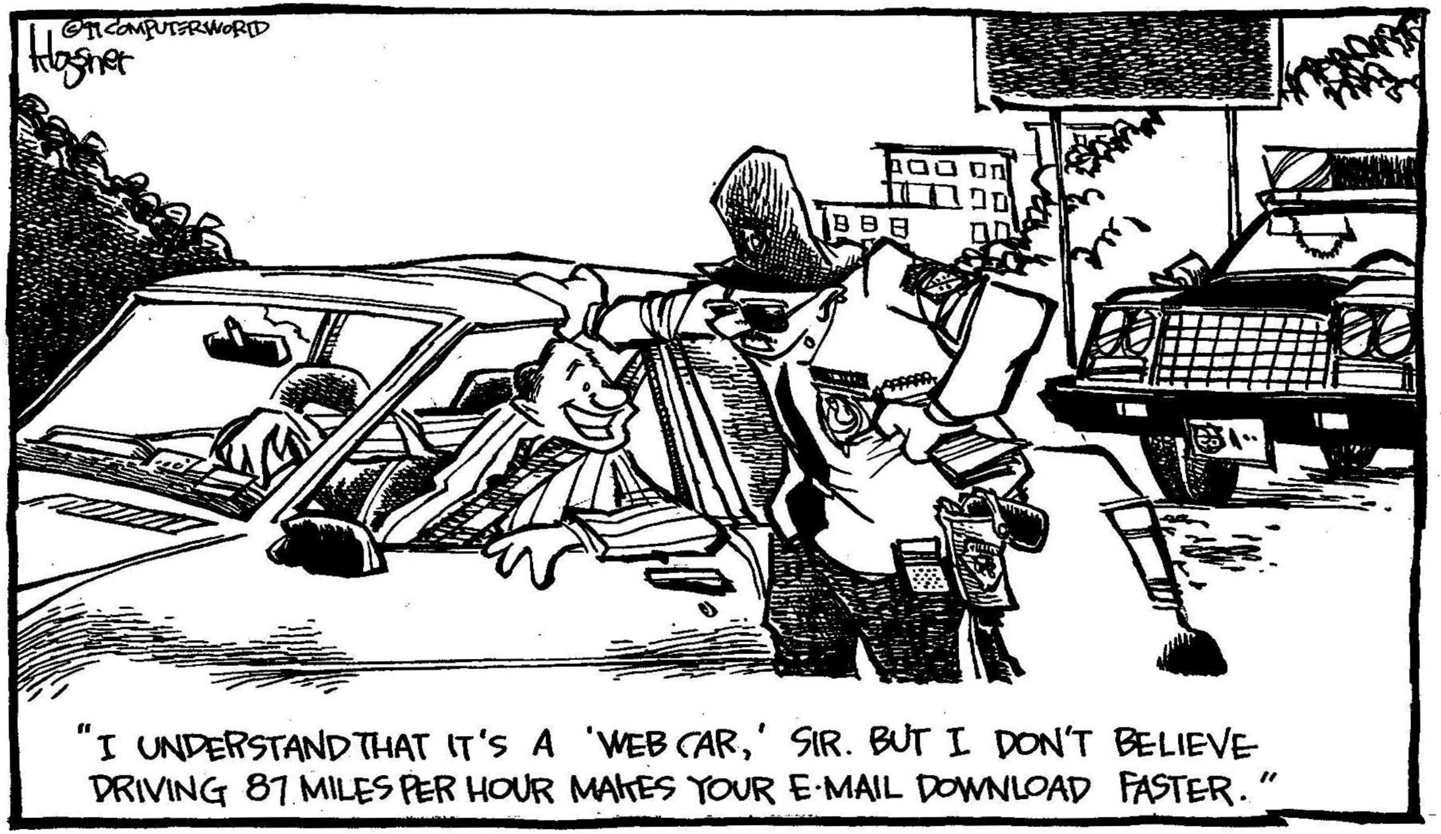
- DaimlerChrysler's vision is to establish an ad hoc network of vehicles (Project FleetNet)

Further Reading

- E.M. Royer and C.K. Toh: “A review of current routing protocols for ad hoc mobile wireless networks”, IEEE Personal Communications, April 1999, 46-55

- Martin Mauve and Jörg Widmer and Hannes Hartenstein: "A Survey on Position-Based Routing in Mobile Ad Hoc Networks", IEEE Network,15(6) , Dec 2001, 30--39

Thank you for your attention!



"I UNDERSTAND THAT IT'S A 'WEB CAR,' SIR. BUT I DON'T BELIEVE DRIVING 87 MILES PER HOUR MAKES YOUR E-MAIL DOWNLOAD FASTER."

Contact Information:

Christian Maihöfer
DaimlerChrysler Research Telematics and E-Business
Communication Technology (RIC/TC)
89013 Ulm
E-Mail: christian.maihoefer@daimlerchrysler.com