Wireless Multihop Ad Hoc Networks

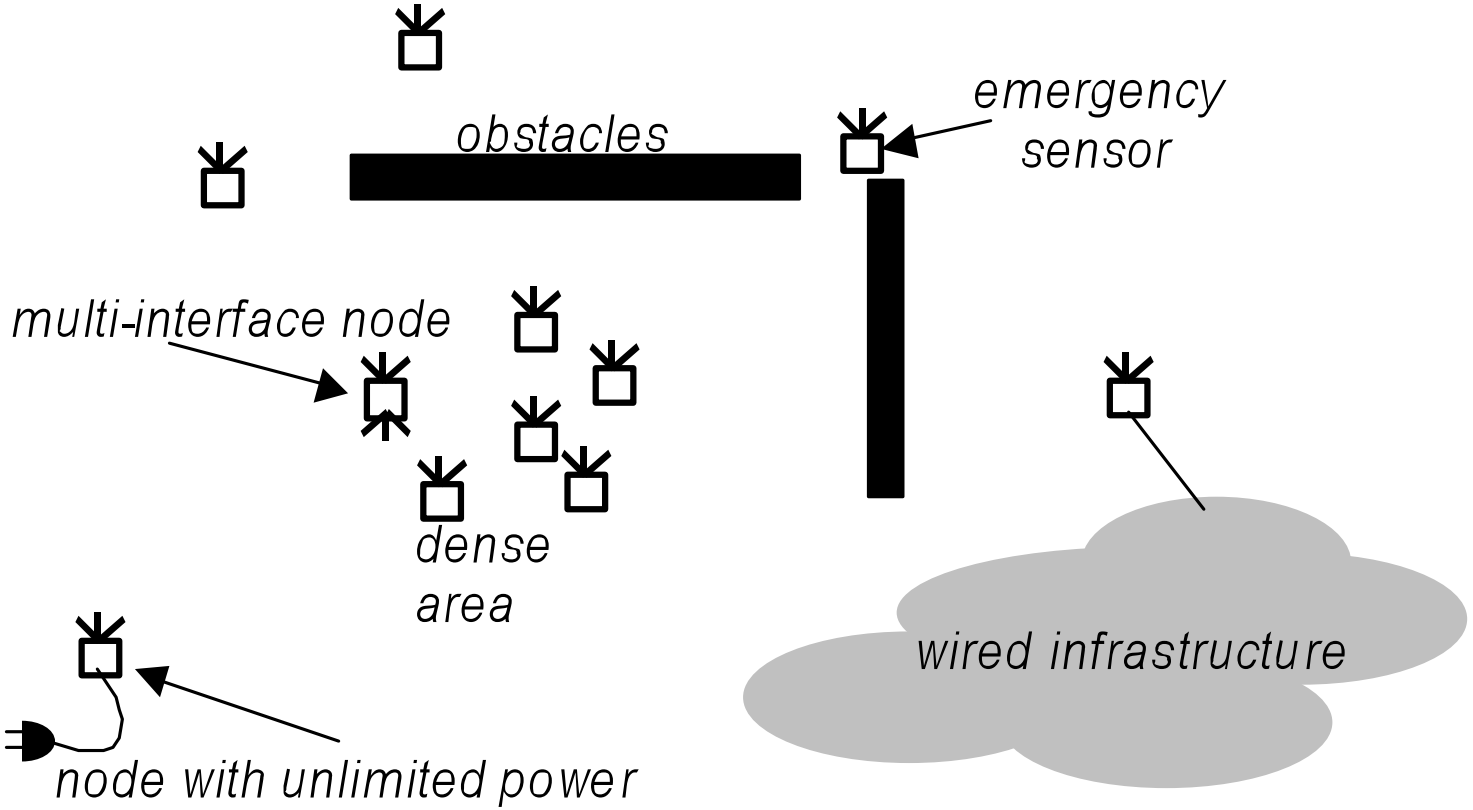
Guevara Noubir

noubir@ccs.neu.edu

Some slides are from Nitin Vaidya's tutorial.

Infrastructure vs. Ad Hoc Wireless Networks

- Infrastructure networks:
  - One or several Access-Points (AP) connected to the wired network
  - Mobile nodes communicate through the AP
- Ad hoc network:
  - Mobile nodes communicate directly with each other
  - Multi-hop ad hoc networks: all nodes can also act as routers
- Hybrid (nodes relay packets from AP):
  - Goal: increase capacity, reduce power consumption, and guarantee a minimum service


obstacles
emergency
sensor
multi-interface node
dense
area
wired infrastructure
node with unlimited power

Constraints

- Limited radio spectrum
- Broadcast Medium (collisions)
- Limited power available at the nodes
- Limited storage memory
- Connection QoS requirements (e.g., delay, packet loss)
- Unreliable network connectivity (depends on the channel)
- Dynamic topology (i.e., mobility of nodes, density)
- Need to provide a full coverage
- Need to enforce fairness

Parameters

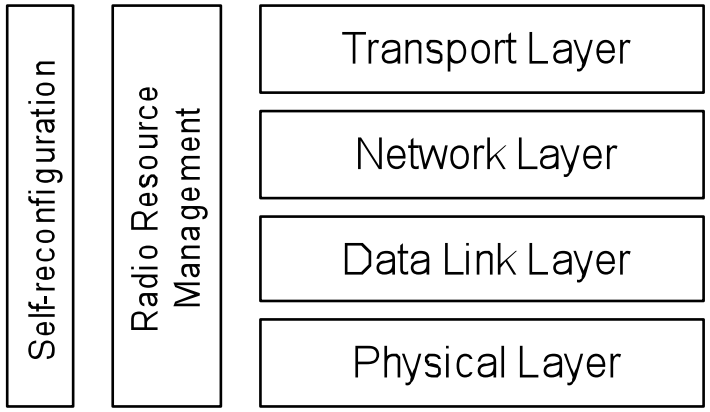
- Use of various coding/modulation schemes
- Use of packets fragmentation
- Use of various transmission power level
- Use of smart antennas and MIMO systems
- Use of multiple RF interfaces (multiple IF characteristics)
- Clustering and backbone formation
- Planning of the fixed nodes location
- Packets scheduling schemes
- Application adaptivity

Theoretical Results

- Capacity of a wireless network [Gupta & Kumar 2000]
  - *n* identical randomly located nodes each capable of transmitting *W* bits can only achieve a throughput per node of $\Theta(\frac{W}{\sqrt{n \log n}})$ bit/sec
  - *n* optimally placed nodes within a $1m^2$ disc with an optimal traffic pattern and an optimal transmission power can only achieve $\Theta(W\sqrt{n})\ bit\text{-}meters/\sec$

Adaptivity and Cooperation

- Classical networking stacks have only minimum interaction between adjacent layers



- Multi-hop wireless ad hoc networks require more cooperation between layers because:
  - Channel variation and network topology changes affect the application
  - Routing versus single hop communication considerably affects the medium access control (MAC) performance
  - Collisions versus channel fading affects both the physical layer and the MAC
  - Battery power has implications on all layers

Adaptive Coding

- Example:
  - ½ rate convolutional code (K=5) versus uncoded communication
  - Channel with two states: E_b/N_0 = 6.8 dB or 11.3 dB (AWGN), L=200 Bytes

E_b/N_0	BER		FER		Nb_Transmit		Total_Tx_Bytes	
	UC	½ CC	UC	½ CC	UC	½ CC	UC	½ CC
6.8dB	10^{-3}	10^{-7}	0.8	$1.6\ 10^{-4}$	5	~ 1	5*200	2*200
11.3dB	10^{-7}	~ 0	$1.6\ 10^{-4}$	~ 0	~ 1	~ 1	200	2*200

- Need to estimate the channel and adapt to it
- Differentiate between congestions and a bad channel condition
- Use of Hybrid-ARQ?

Adaptive Fragmentation

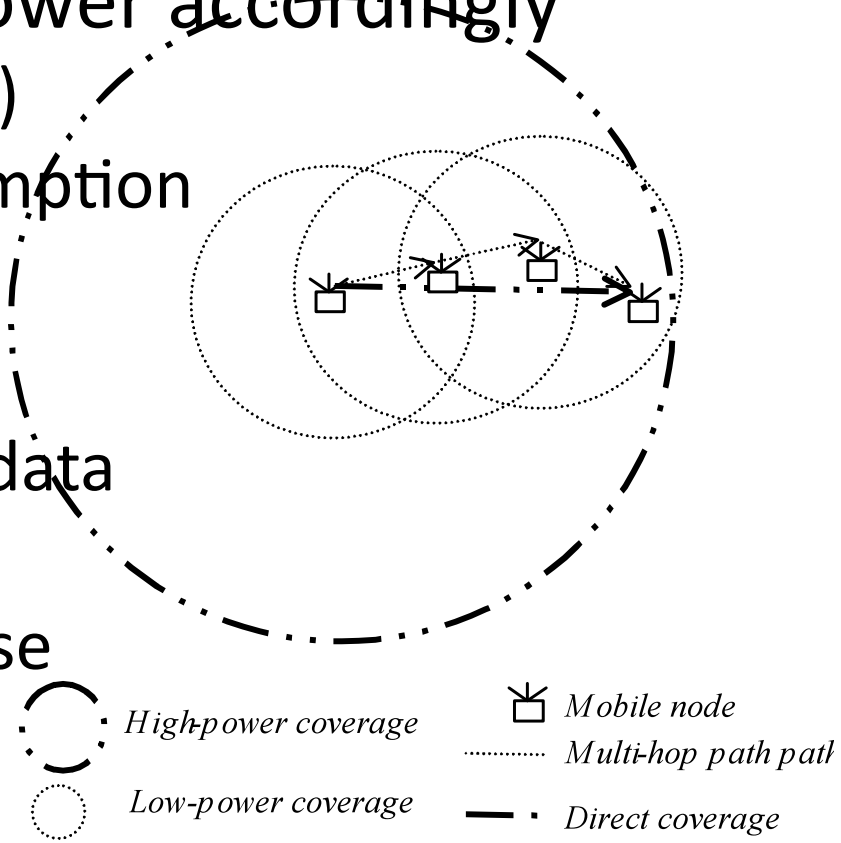
- Example:
  - To transmit a frame of length 200 Bytes, we can fragment into 4 frames of length 50 Bytes (+ 10 Bytes overhead)

BER	FER		Nb_Transmit		Total_Tx_Bytes (incl. overhead)	
	L=60B	L=200B	L=60B	L=200B	L=60B	L=200B
10^{-3}	0.38	0.8	1.6	5	384	1000
10^{-7}	~ 0	~ 0	~ 1	~ 1	240	200

- Need to estimate the channel and adapt to it

Multiple Power Levels

- Using multi-hop transmission (*h* hops) and reducing the transmission power accordingly
  - Increases capacity (factor of *h*)
  - Reduces overall power consumption (by a factor of *h*)
- In asymmetric environments
  - Low power node can encode data and transmit it at low power
  - Powerful nodes can decode use higher transmission power



Parameters of IEEE802.11

- IEEE802.11 has three mechanisms that can be used to improve performance under dynamic channels:
  - Fragmentation (also used to avoid collision)
  - Multiple coding/modulation schemes
  - Multiple power levels

Problems of Multi-Hop Routing

- Routing:
  - How to maintain up-to-date information on the network topology? Routing messages overhead
  - How to determine number of hops
  - How to estimate buffers size
- Higher delay
- Risk of congestion on nodes

Practical Approaches

- Solving sub-problems independently
  - Improving TCP to be wireless aware
  - Routing in multi-hop wireless ad hoc networks: DSDV, DSR, AODV, TORA, FSR
    - Not power or resource aware. Single hop whenever possible (no interaction with the MAC of higher layers)
  - Fragmenting packets according to the channel performance
  - Adapting coding/modulation scheme to the channel
  - Adapting transmission power to destination
- There is a need for a global approach:
  1. Combine: transmission power, coding, and fragmentation
  2. Add routing
  3. Add medium access control

- Engineering perspective: what minimal subset of functionalities do we need to implement to achieve near optimal performance?
  - What minimal set of coding/modulation schemes? What power levels do we need?

Existing Unicast Routing Protocols

- Types:
  - 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

- Some existing protocols
  - Dynamic Source Routing (DSR)
  - Location Aware Routing (LAR)
  - Adhoc On-demand Distance Vector (AODV)
  - Temporally Ordered Reversal Algorithm

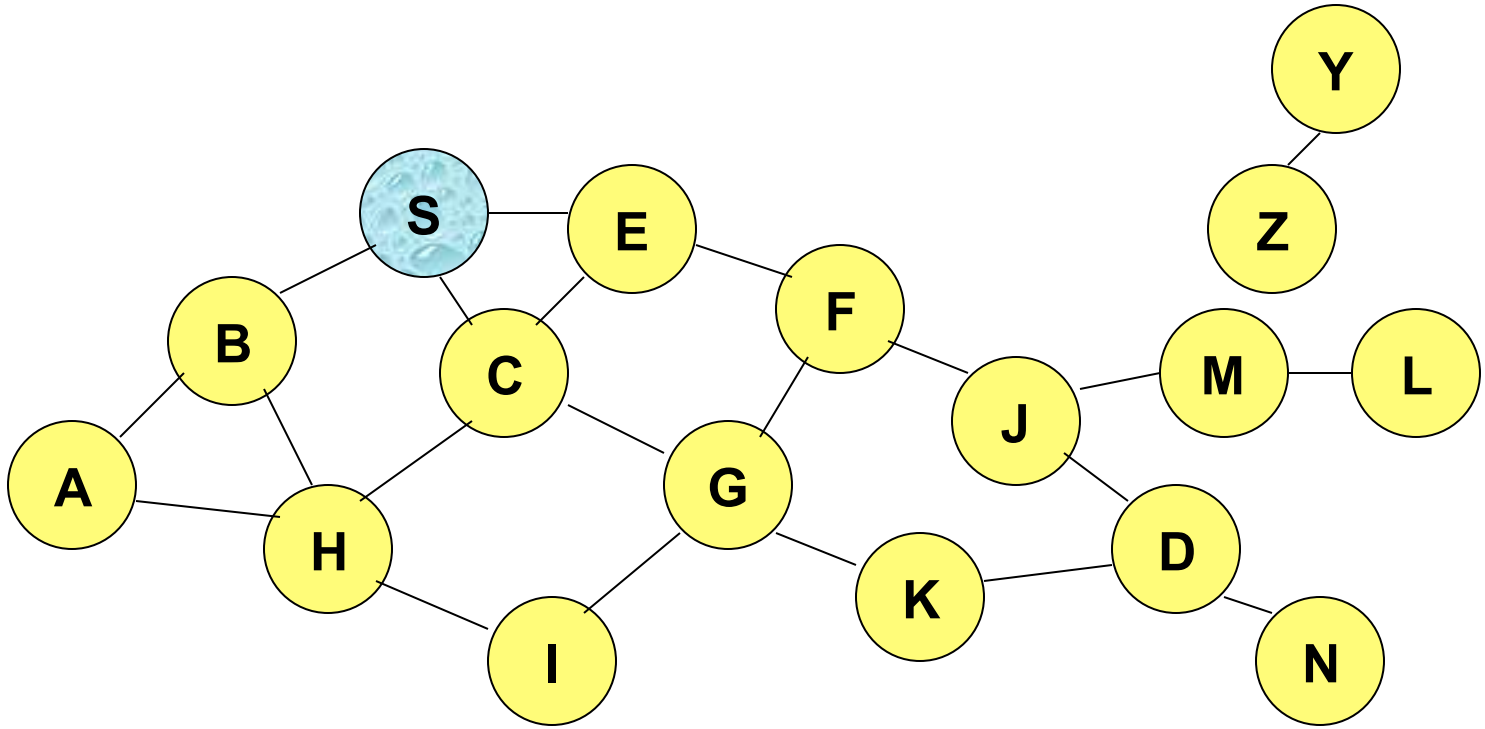
Trade-Off Between Proactive and Reactive

- 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

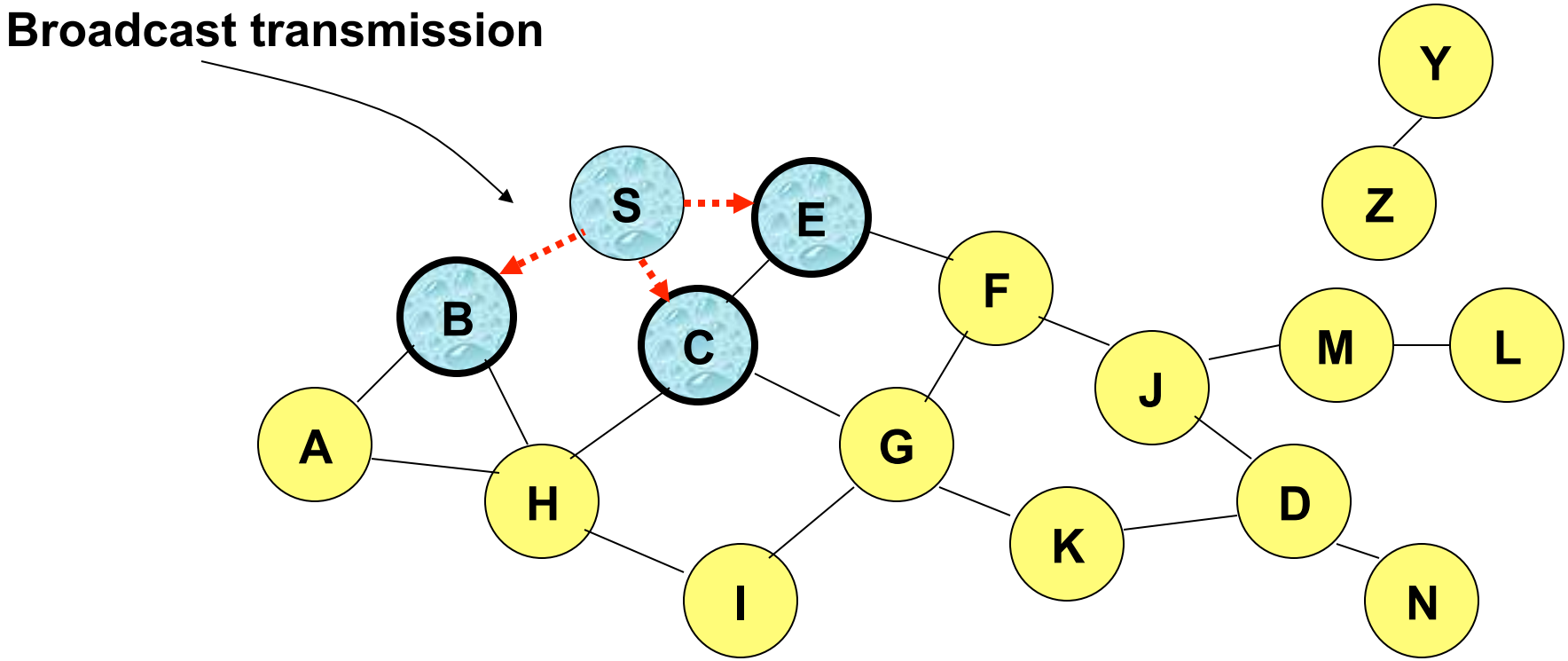
Flooding for Data Delivery



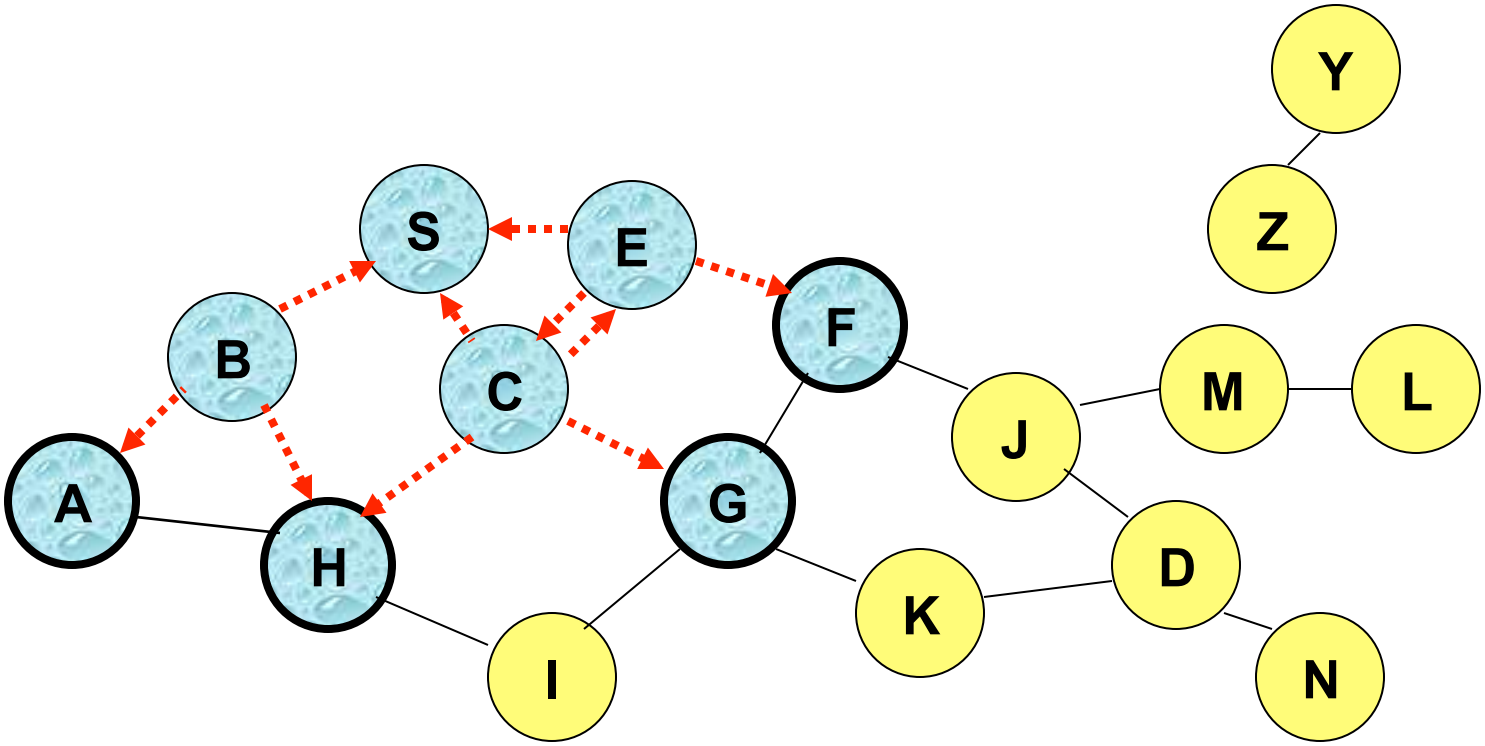
Represents a node that has received packet P

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

Flooding for Data Delivery

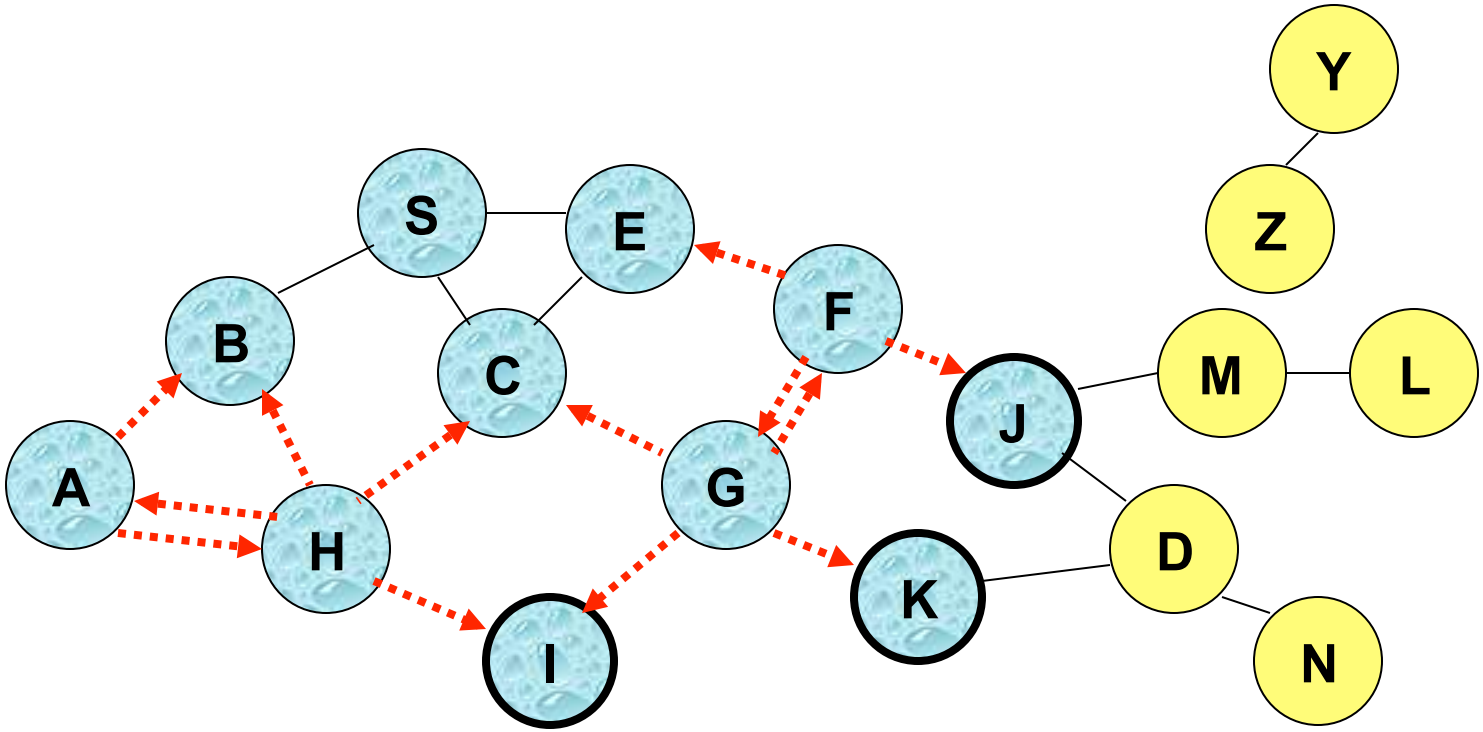


Flooding for Data Delivery



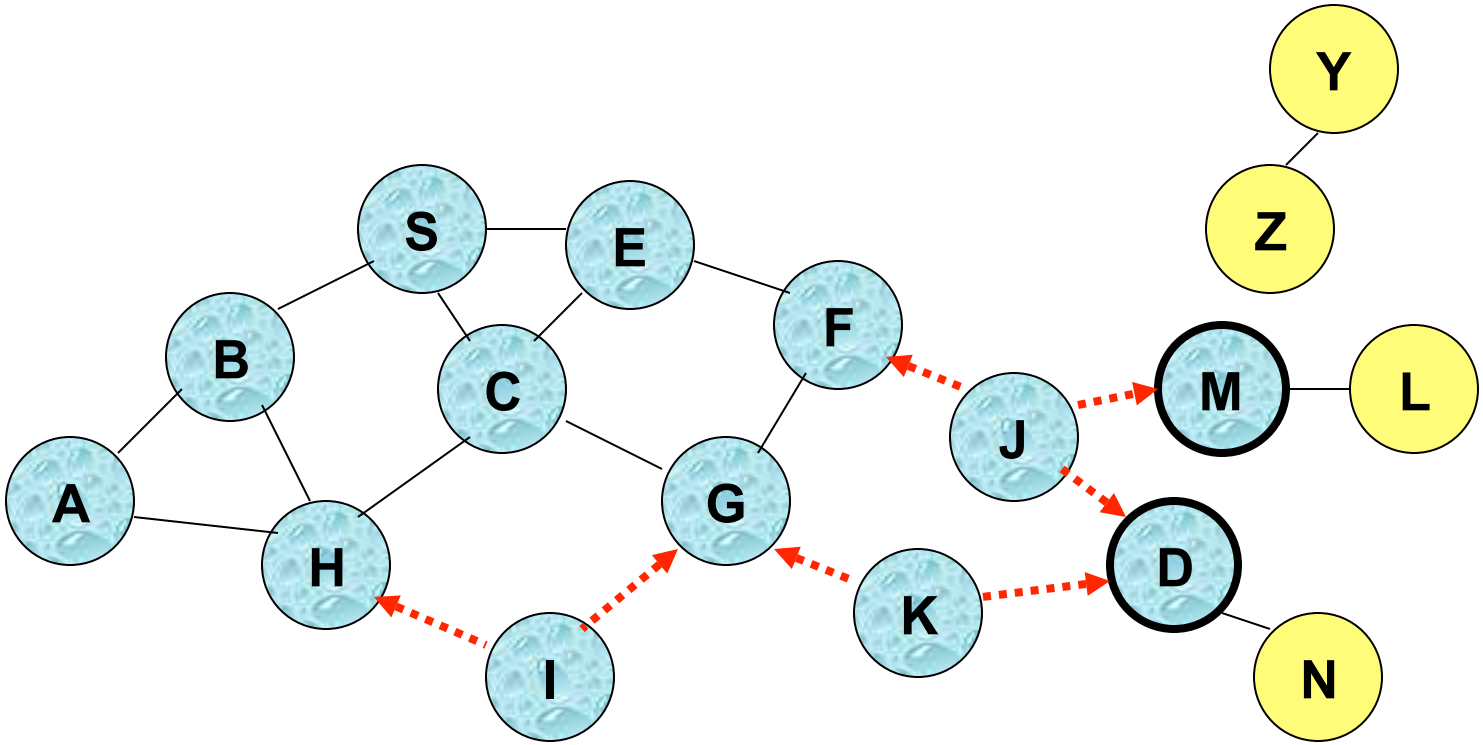
- **Node H receives packet P from two neighbors:**
  potential for collision

Flooding for Data Delivery



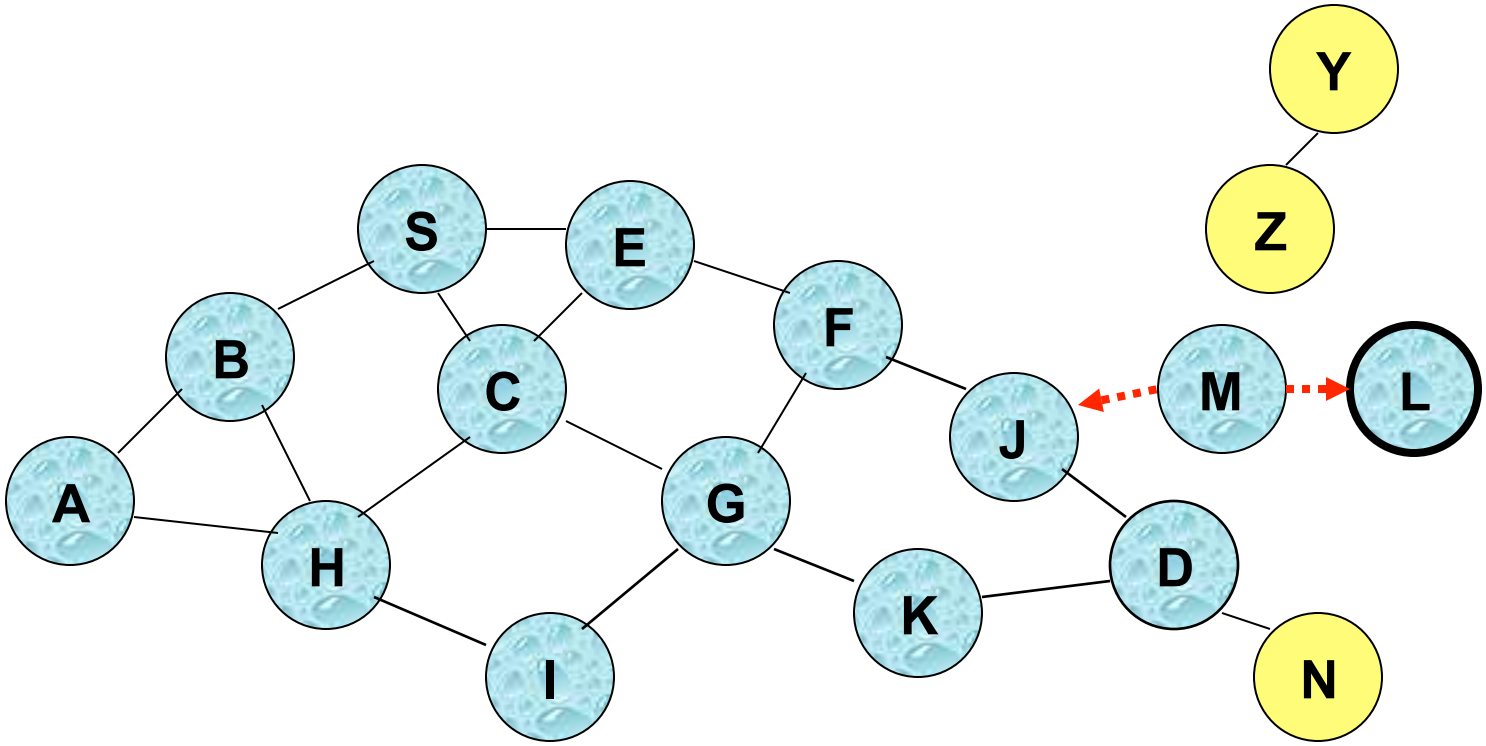
- **Node C receives packet P from G and H, but does not forward it again, because node C has already forwarded packet P once**

Flooding for Data Delivery



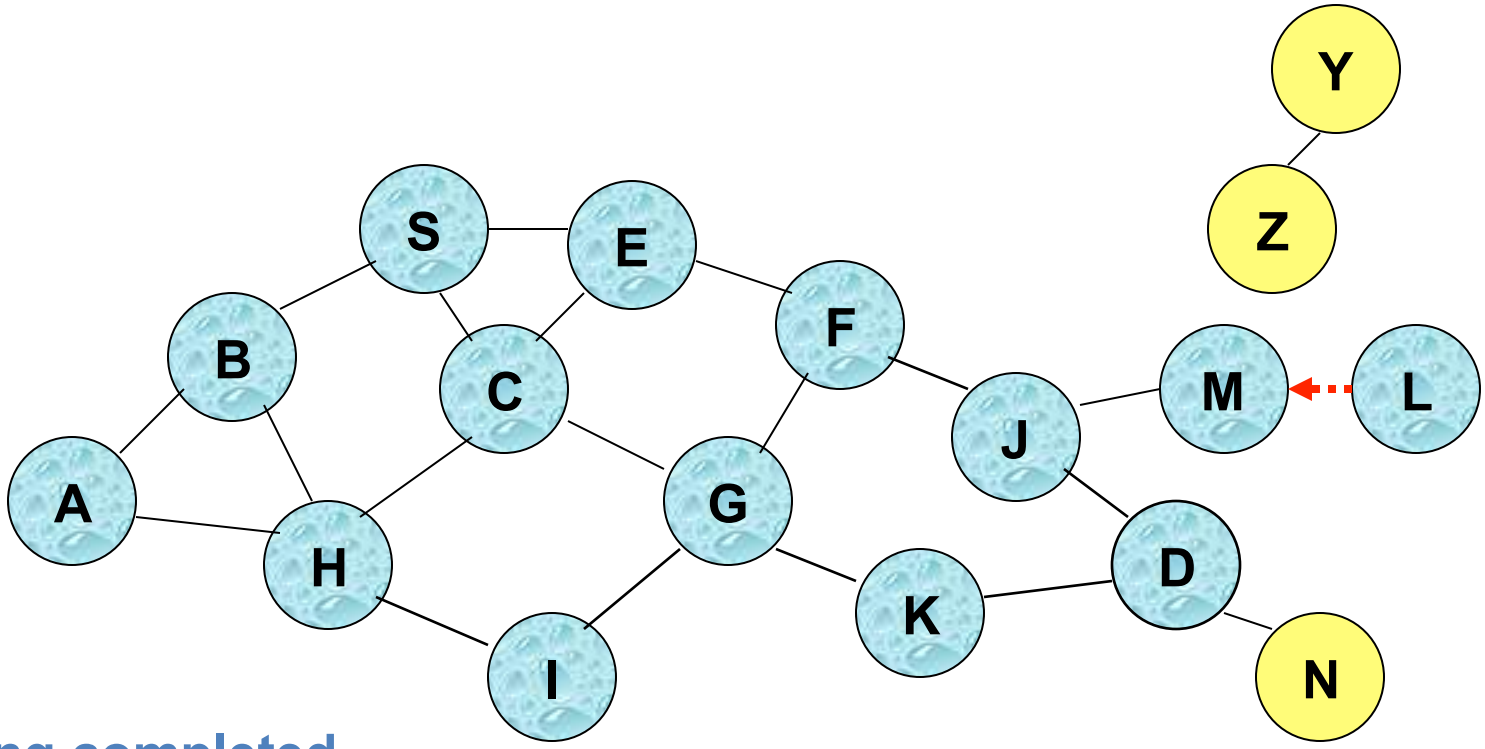
- **Nodes J and K both broadcast packet P to node D**
- **Since nodes J and K are hidden from each other, their transmissions may collide**
  - **=> Packet P may not be delivered to node D at all**

Flooding for Data Delivery



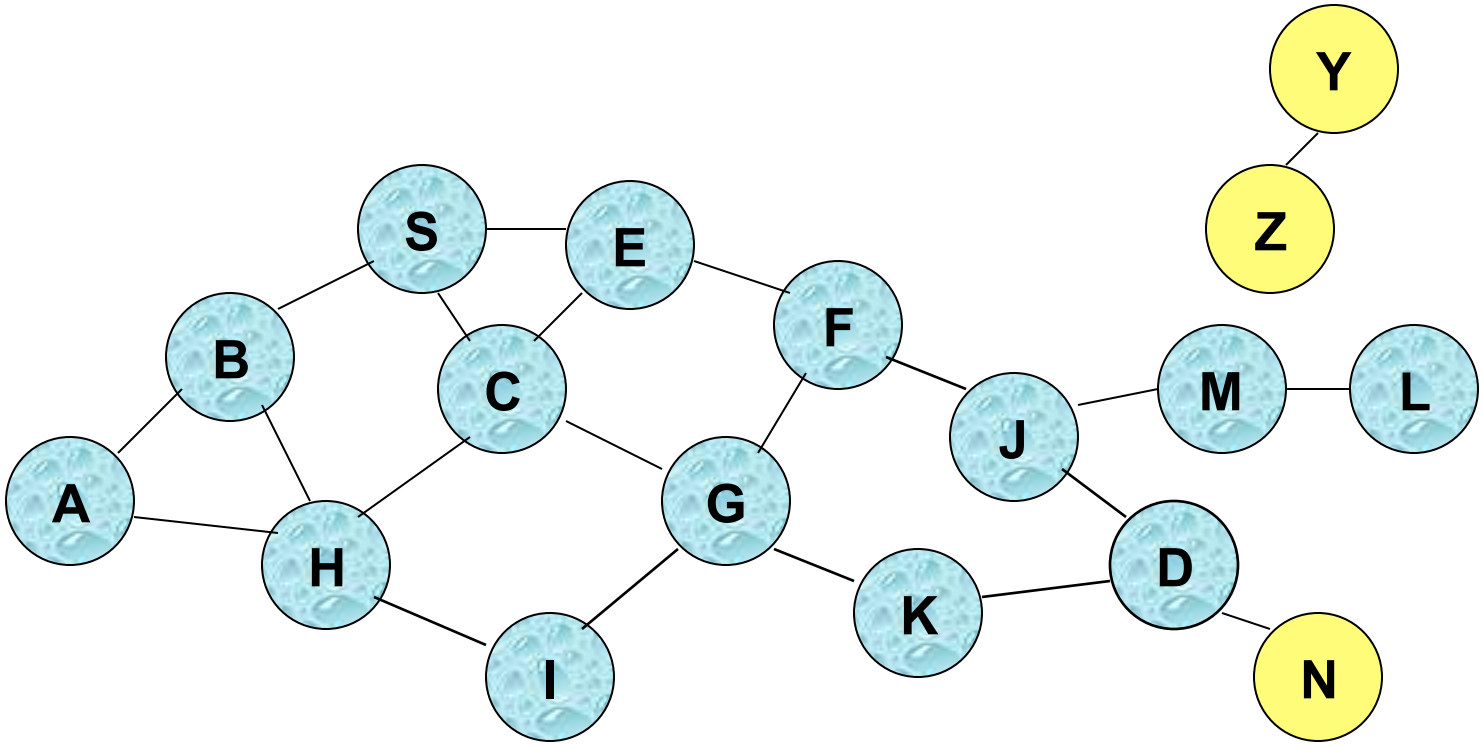
- **Node D does not forward packet P, because node D is the intended destination of packet P**

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

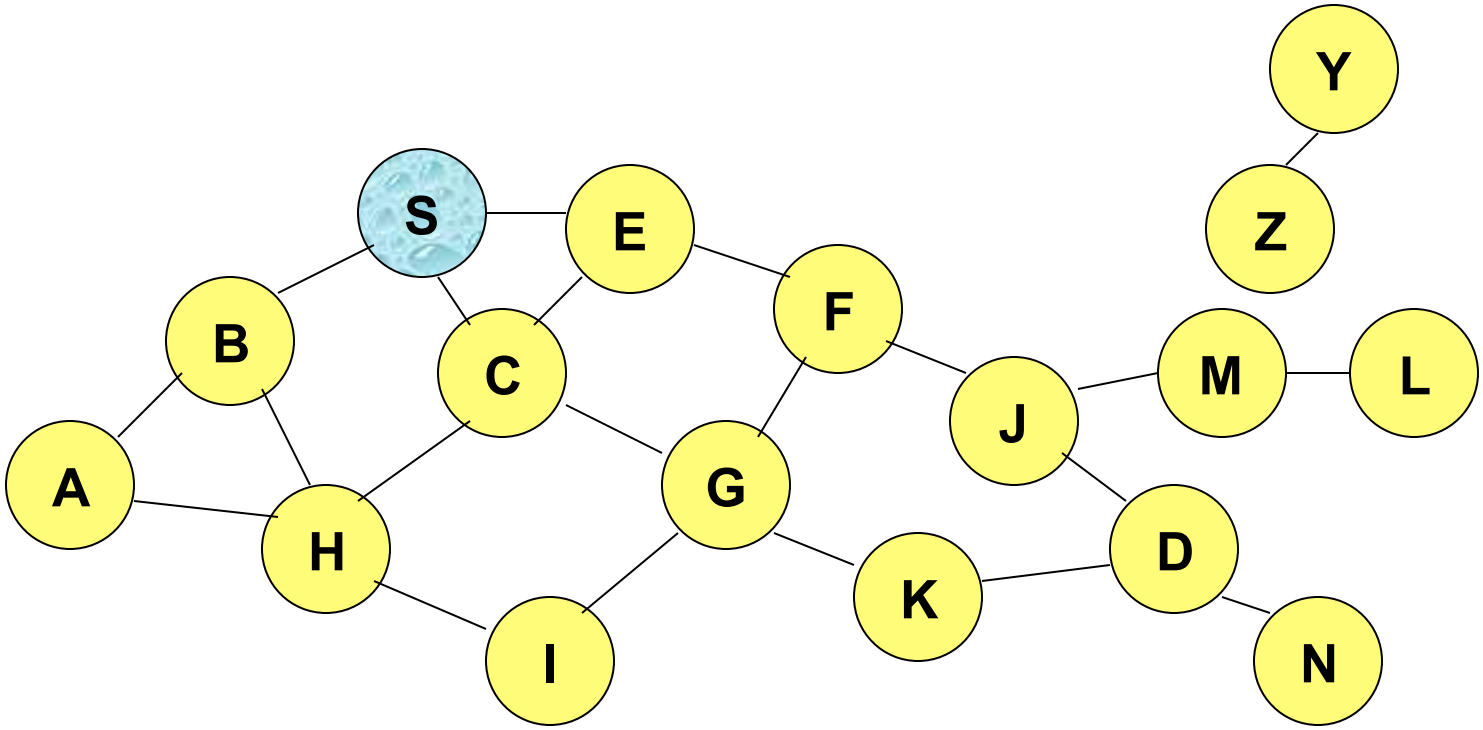
Flooding of Control Packets

- 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]

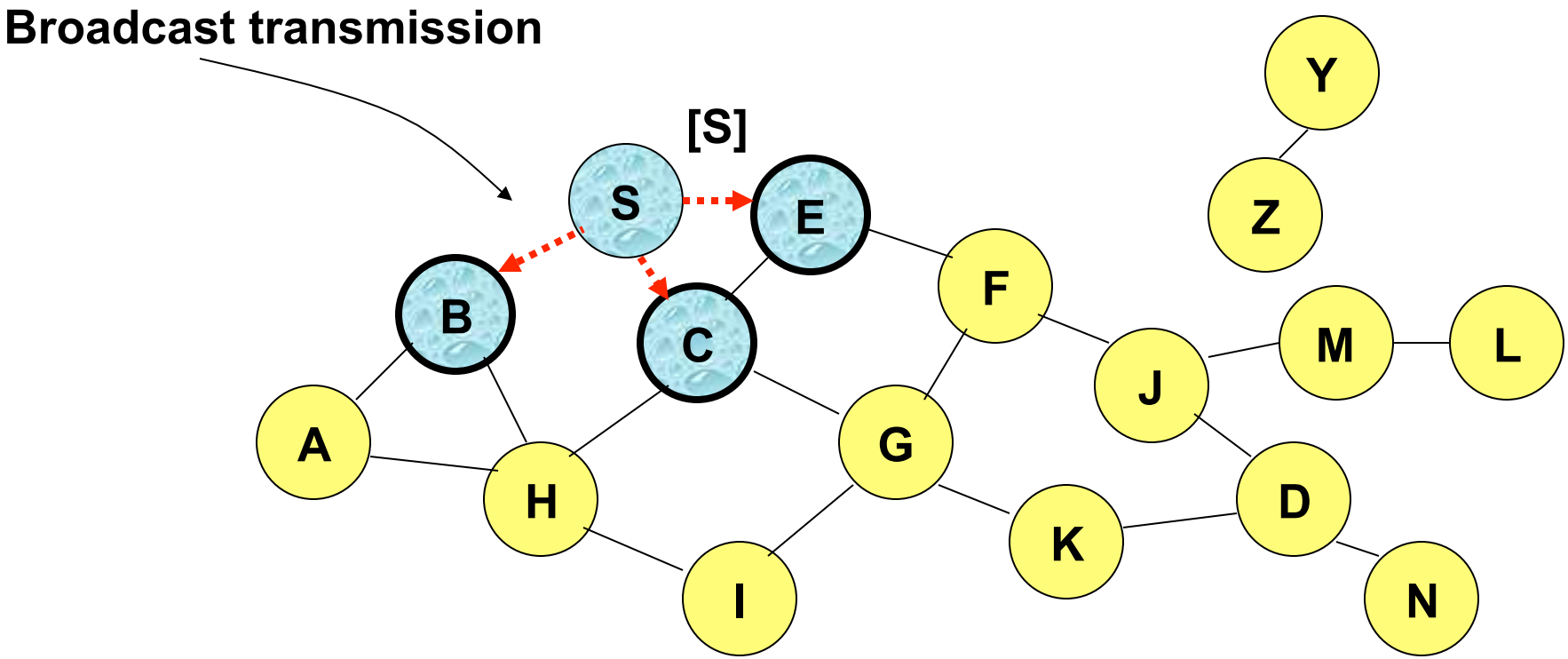
- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a route discovery
- Source node S floods Route Request (RREQ)
- Each node appends own identifier when forwarding RREQ

Route Discovery in DSR



Represents a node that has received RREQ for D from S

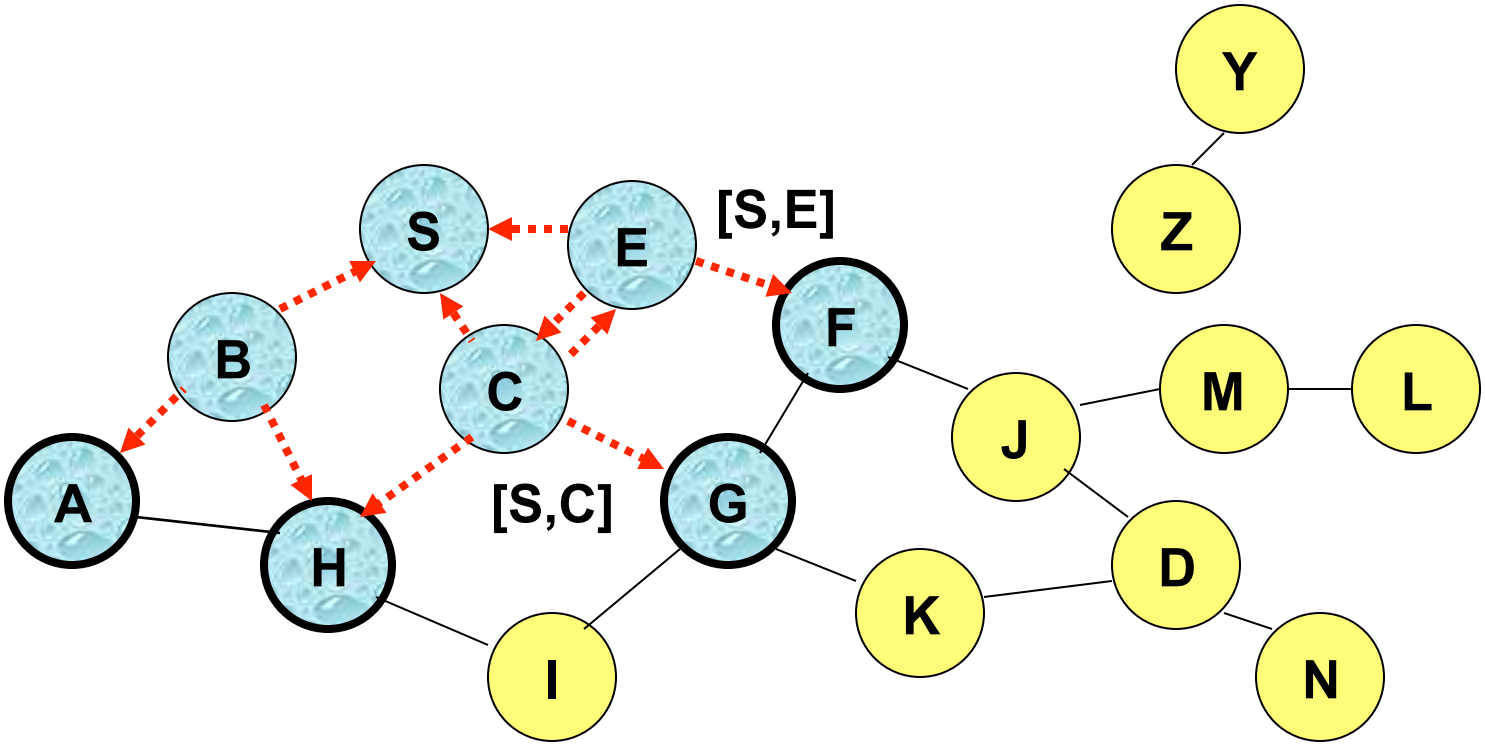
Route Discovery in DSR



Represents transmission of RREQ

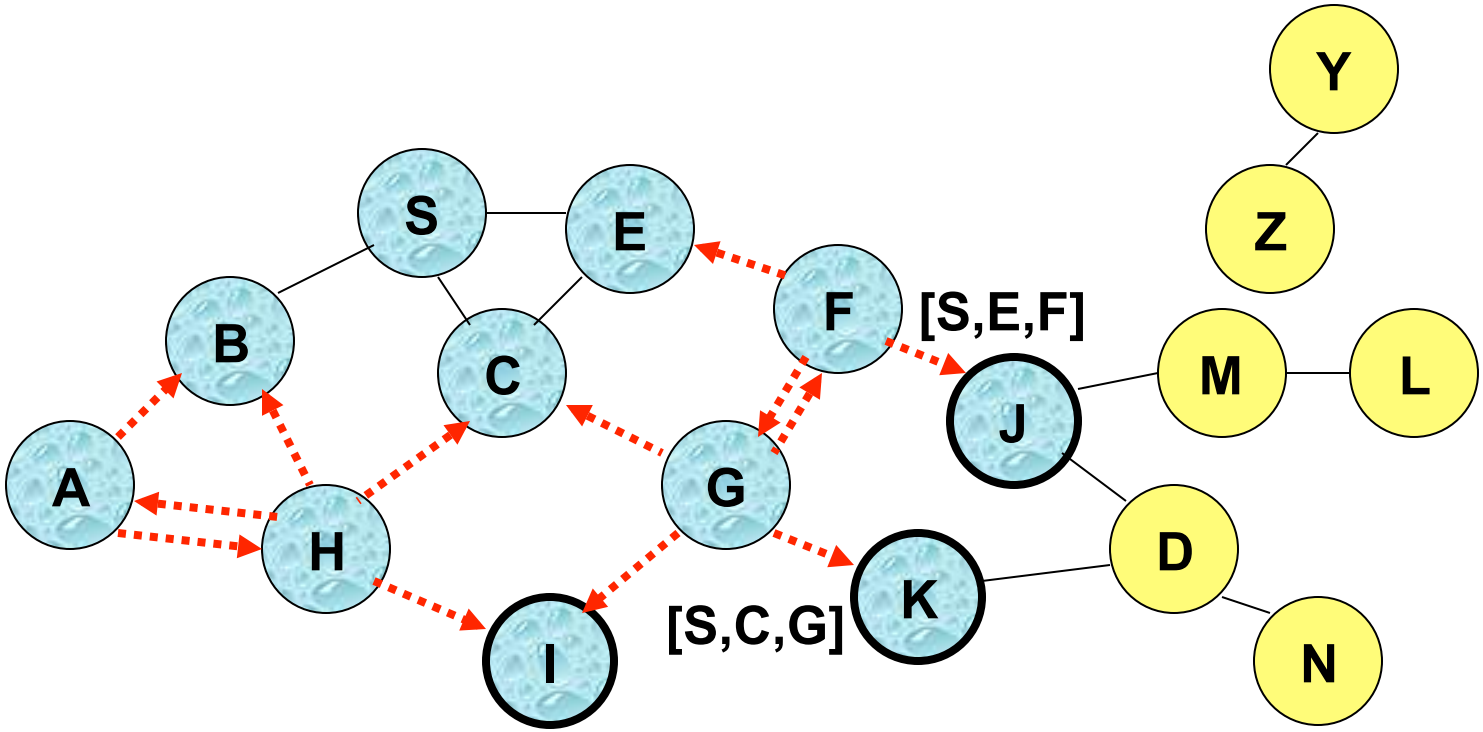
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



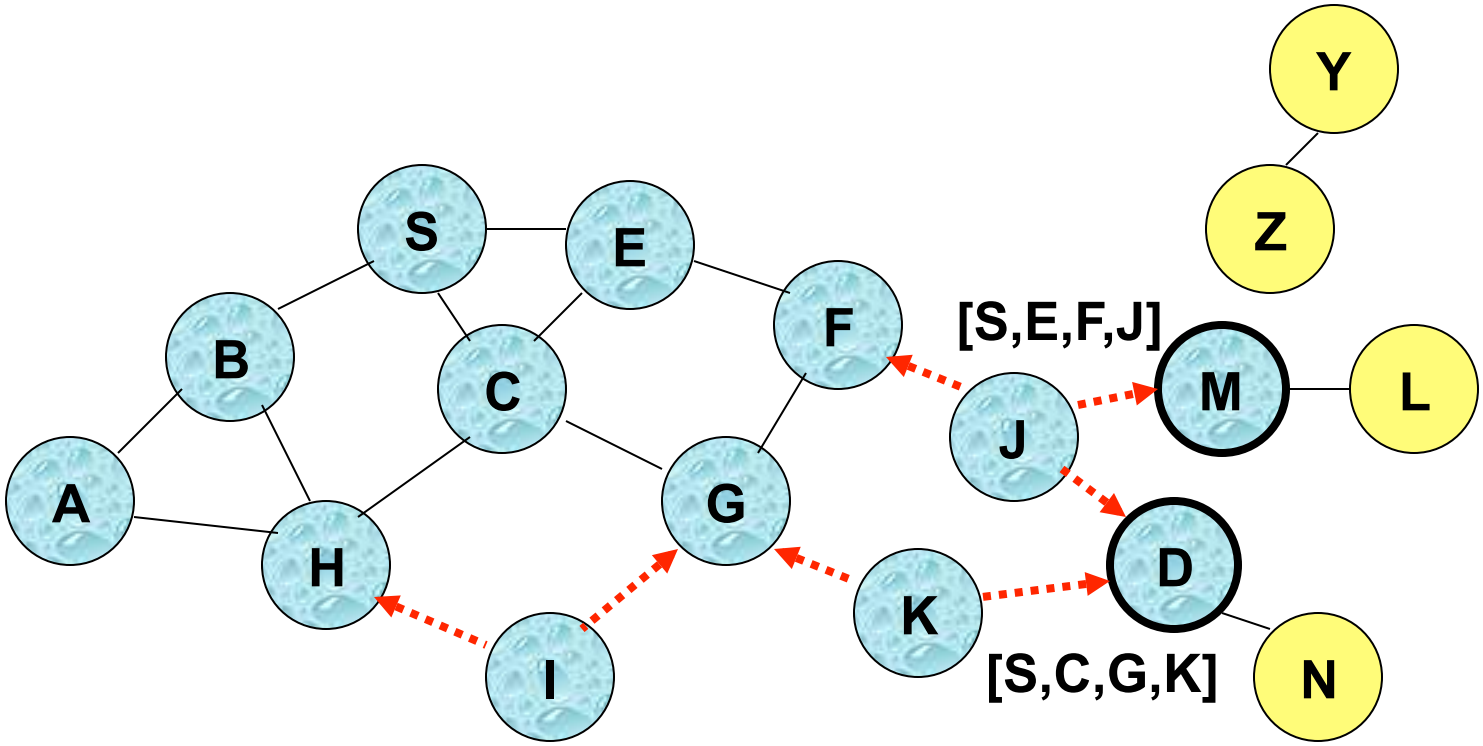
- **Node H receives packet RREQ from two neighbors:**
  potential for collision

Route Discovery in DSR



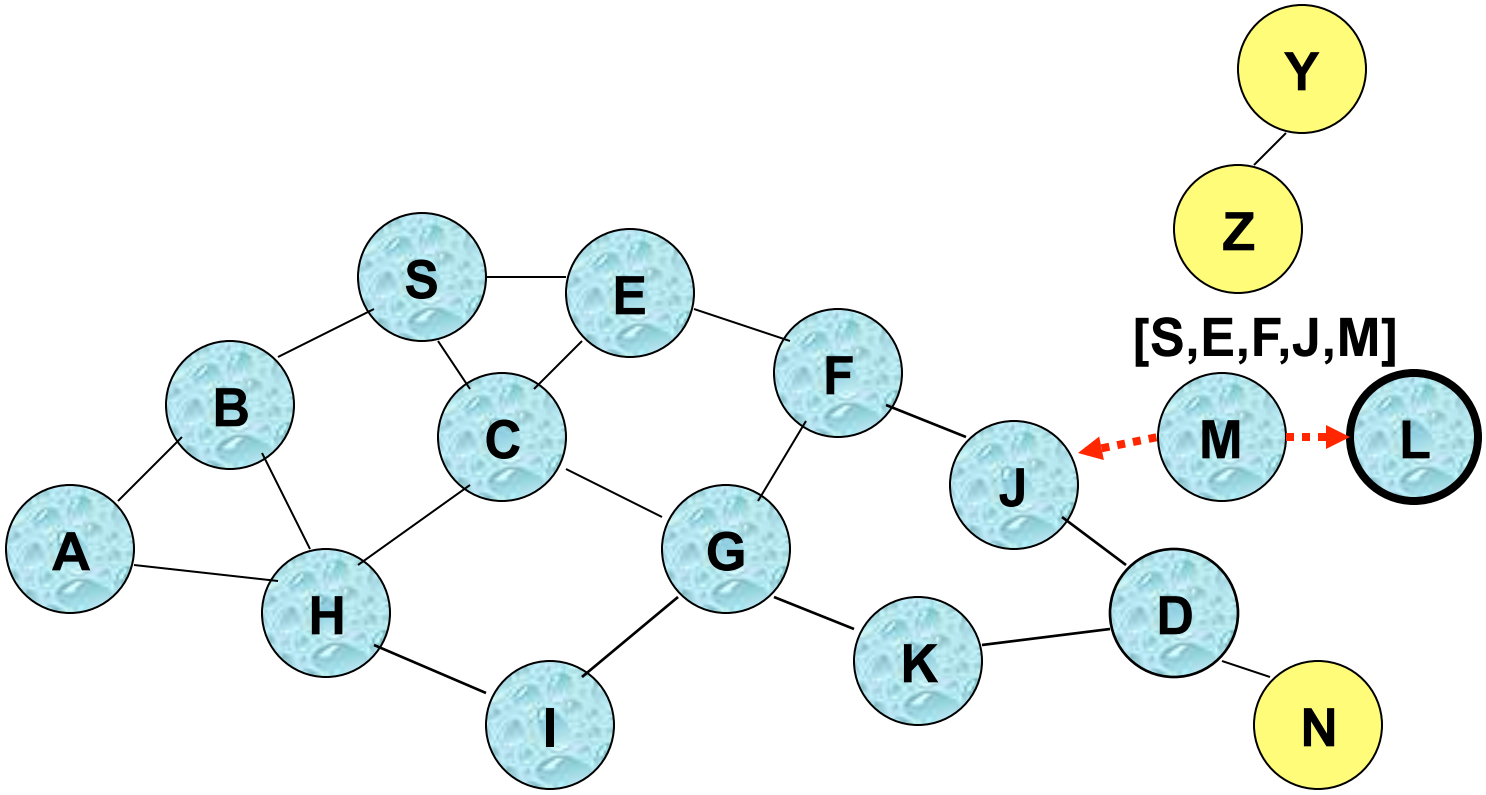
- **Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once**

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

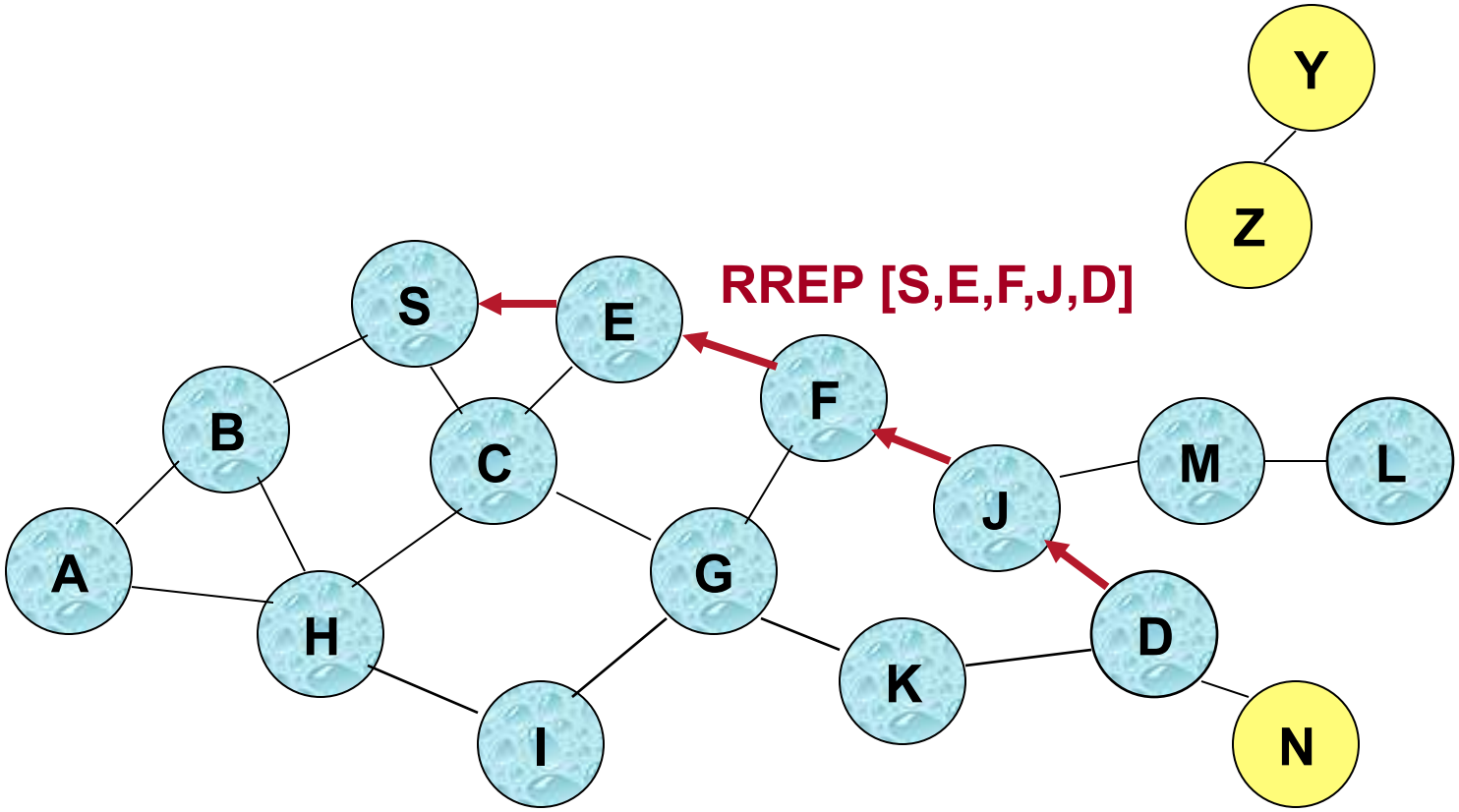


- **Node D does not forward RREQ, because node D is the intended target of the route discovery**

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



← **Represents RREP control message**

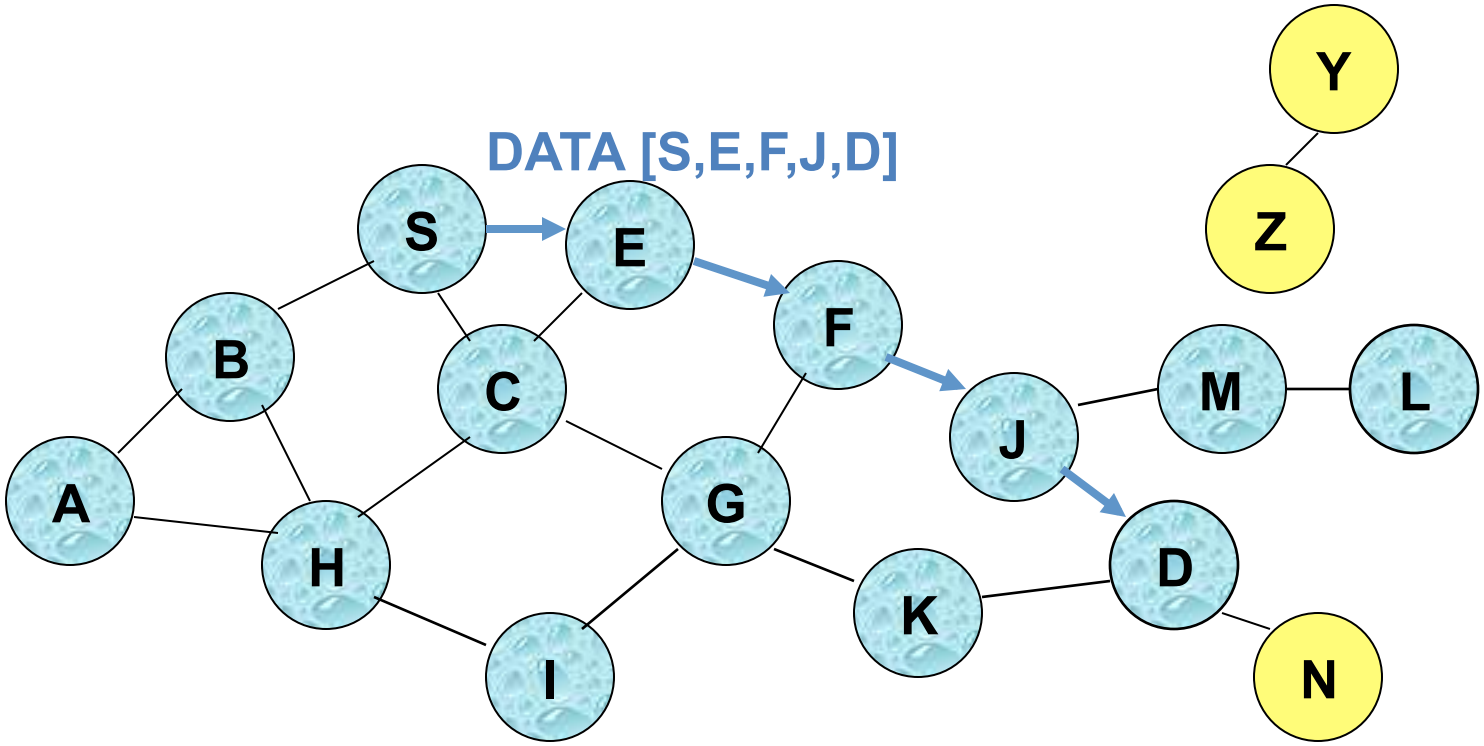
Route Reply in DSR

- 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 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

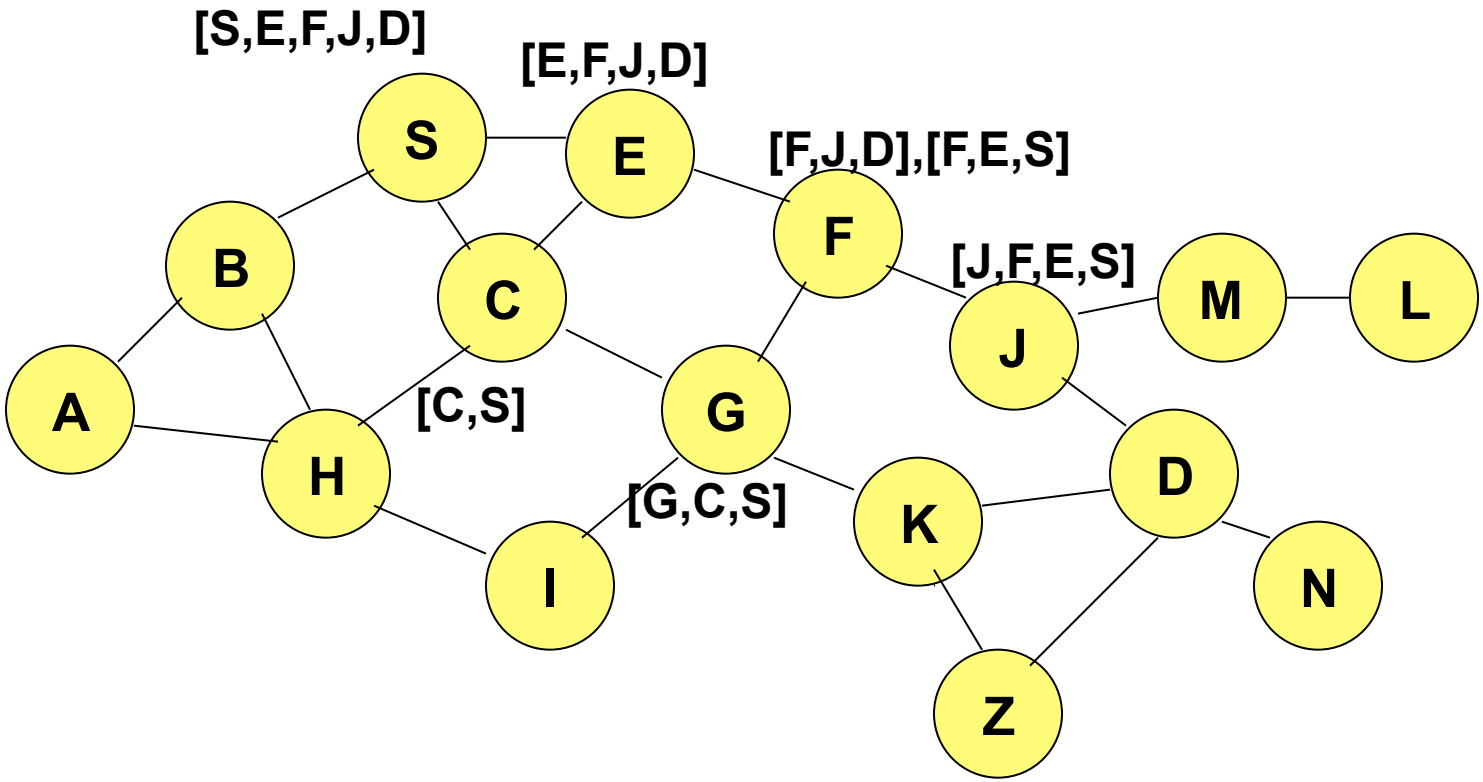
DSR Optimization: Route Caching

- 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

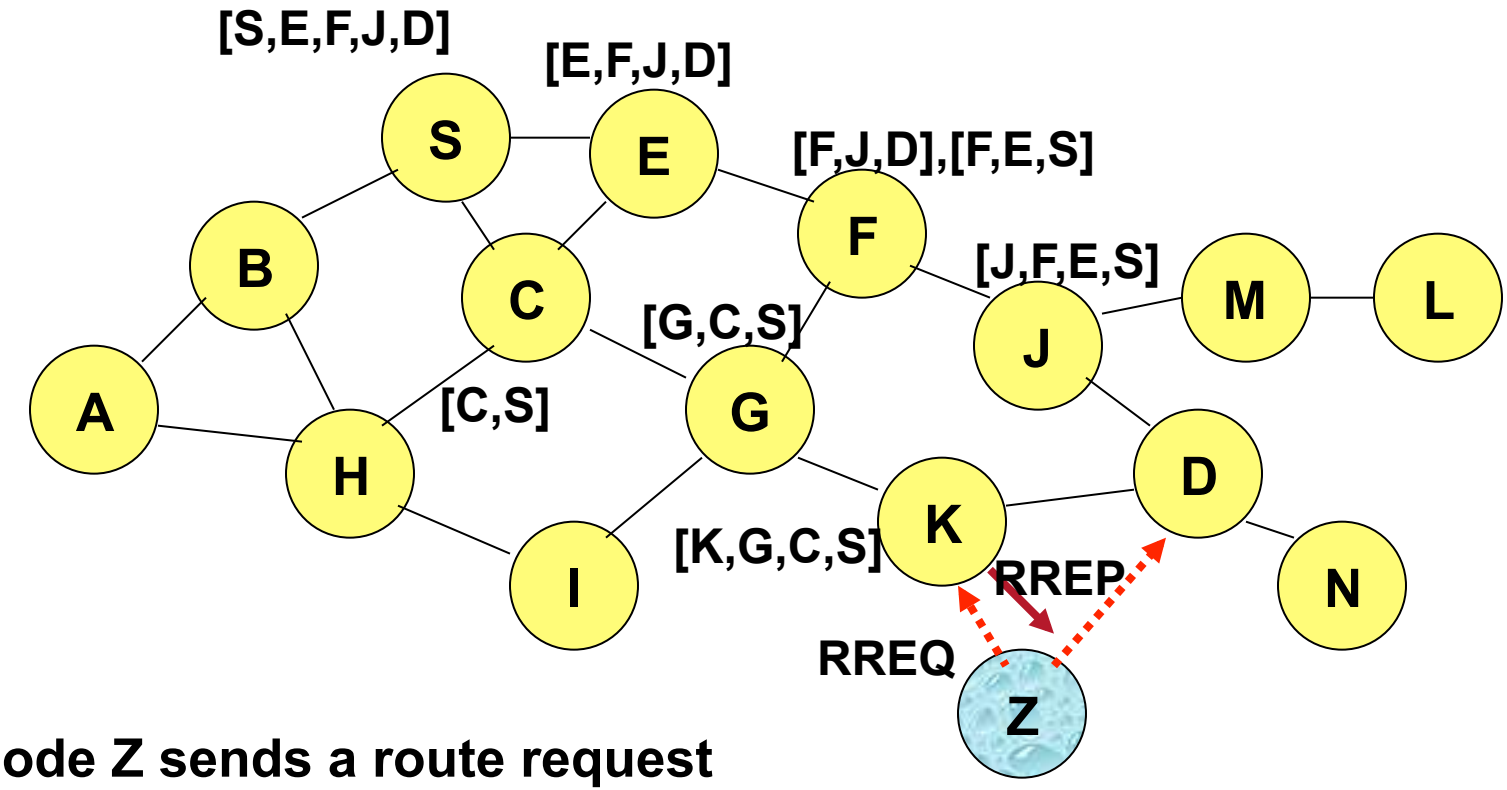
- When node S learns that a route to node D is broken, it uses another route from its local cache, if such a route to D exists in its cache. Otherwise, node S initiates route discovery by sending a route request
- Node X on receiving a Route Request for some node D can send a Route Reply if node X knows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

Use of Route Caching



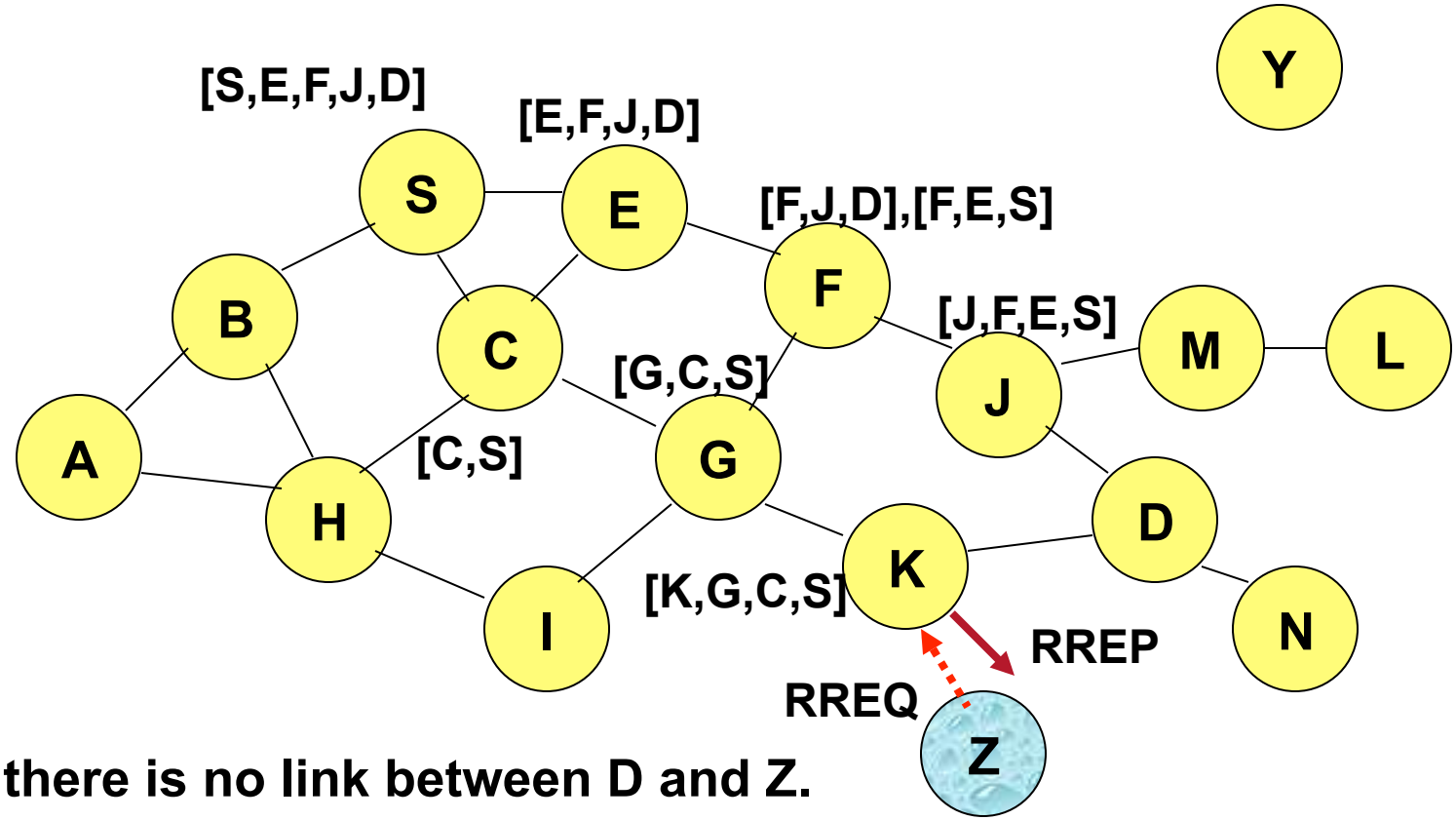
[P,Q,R] Represents cached route at a node
(DSR maintains the cached routes in a tree format)

Use of Route Caching:
Can Speed up Route Discovery



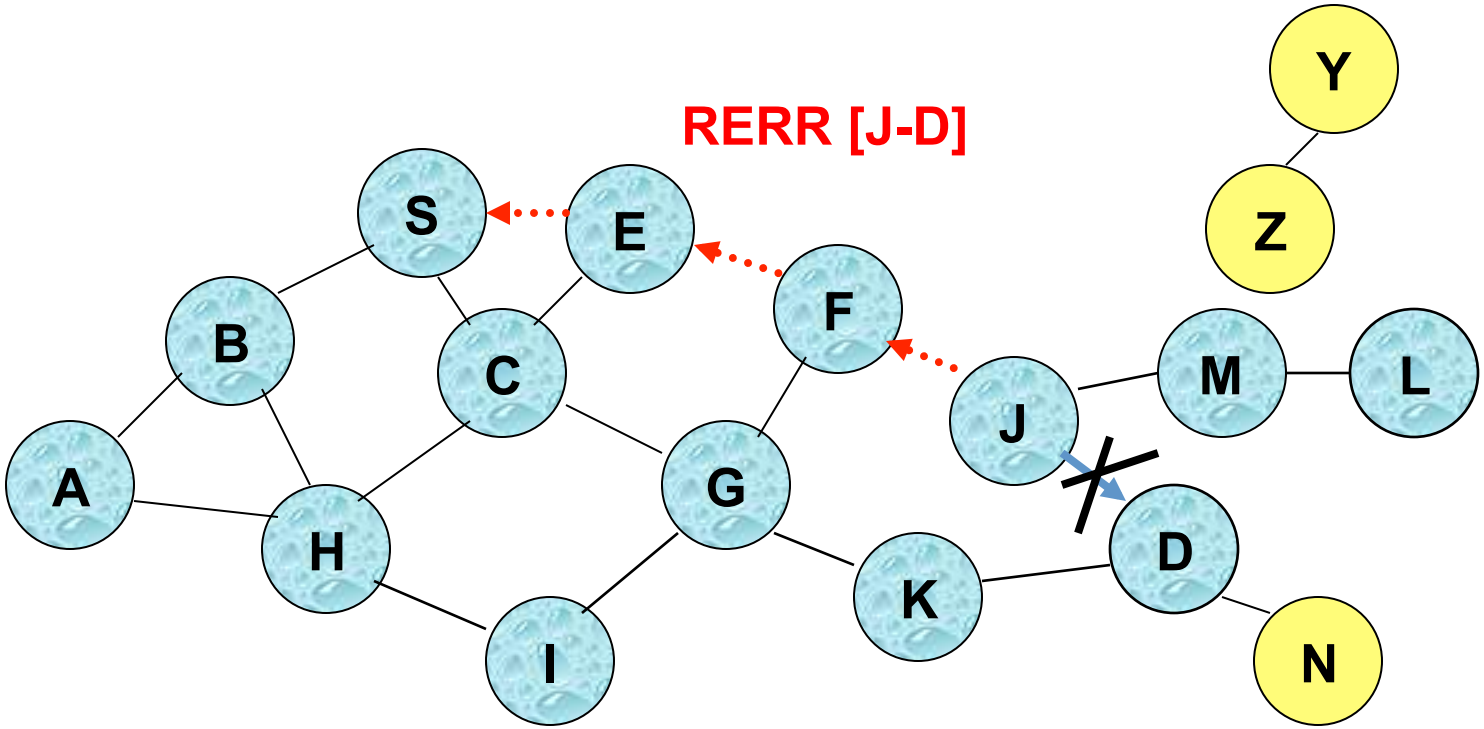
When node Z sends a route request for node C, node K sends back a route reply [Z,K,G,C] to node Z using a locally cached route

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.
- For some proposals for cache invalidation, see [Hu00Mobicom]
  - Static timeouts
  - Adaptive timeouts based on link stability