ECS-087: Mobile Computing

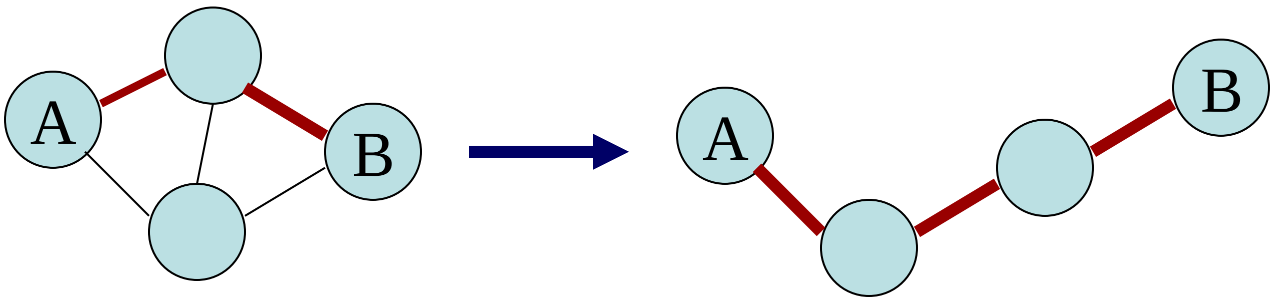
Mobile Adhoc Networks and Routing in MANETS

(most of the slides borrowed from Prof. Sridhar Iyer)

Index

Mobile Ad Hoc Networks (MANET)

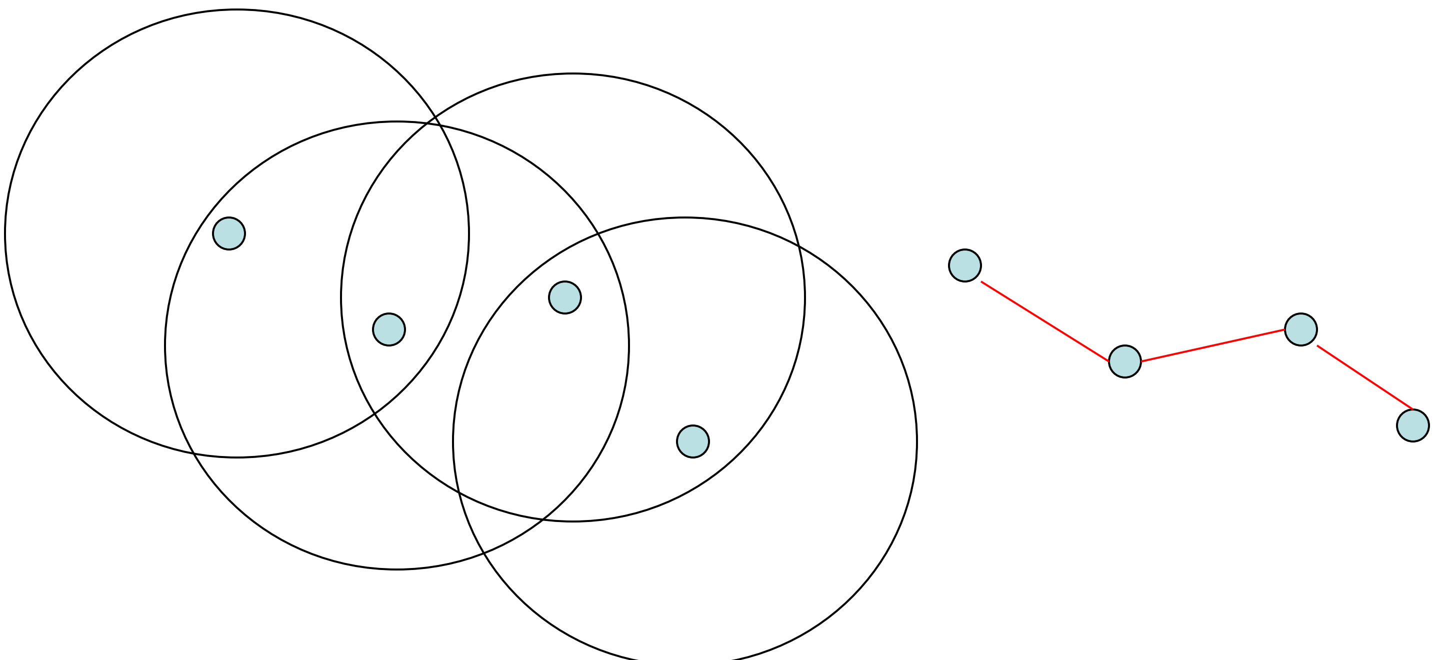
- Host movement frequent
- Topology change frequent



- No cellular infrastructure. Multi-hop wireless links.
- Data must be routed via intermediate nodes.

MANETS

- May need to traverse multiple links to reach destination



- Mobility causes route changes

MANETs

- Do not need backbone infrastructure support
- Are easy to deploy
- Useful when infrastructure is absent, destroyed or impractical
- Infrastructure may not be present in a disaster area or war zone

Applications

- Military environments
  - soldiers, tanks, planes
- Emergency operations
  - search-and-rescue
  - policing and fire fighting
- Civilian environments
  - taxi cab network
  - meeting rooms
  - sports stadiums

MAC in MANET

- IEEE 802.11 DCF is most popular
  - Easy availability
  - Uses RTS-CTS to avoid hidden terminal problem
  - Uses ACK to achieve reliability

- 802.11 was designed for single-hop wireless
  - Does not do well for multi-hop ad hoc scenarios
  - Reduced throughput
  - Exposed terminal problem

Routing in MANET

- Mobile IP needs infrastructure
  - Home Agent/Foreign Agent in the fixed network
  - DNS, routing etc. are not designed for mobility

- MANET
  - no default router available
  - “every” node also needs to be a router

Issues in Routing in MANET

- Mobility
  - Topology highly dynamic due to movement of nodes
    - Ongoing sessions suffer frequent path breaks
  - Even though wired network protocol find alternate paths when a path breaks, the convergence is slow
- Bandwidth constraint
  - Limited bandwidth imposes constraint on routing protocols to maintain topological information
    - Due to frequent changes in topology the control overhead of keeping the topology current could be very high

Issues in Routing in MANET

- Error prone shared broadcast radio channel
  - Wireless links have time varying characteristics in terms of link capacity and link error rate
  - So routing protocol may need to interact with MAC layer to find alternate routes through better quality links
- Energy constraint
  - Limited battery power requires that the nodes do not spend too much resources on routing overhead

Properties of good routing protocol in MANET

- Must be distributed
- Adaptive to frequent topology changes
- Must be localized, since global state maintenance involves a huge state propagation control overhead
- Loop free and free from stale routes
- Convergence should be quick

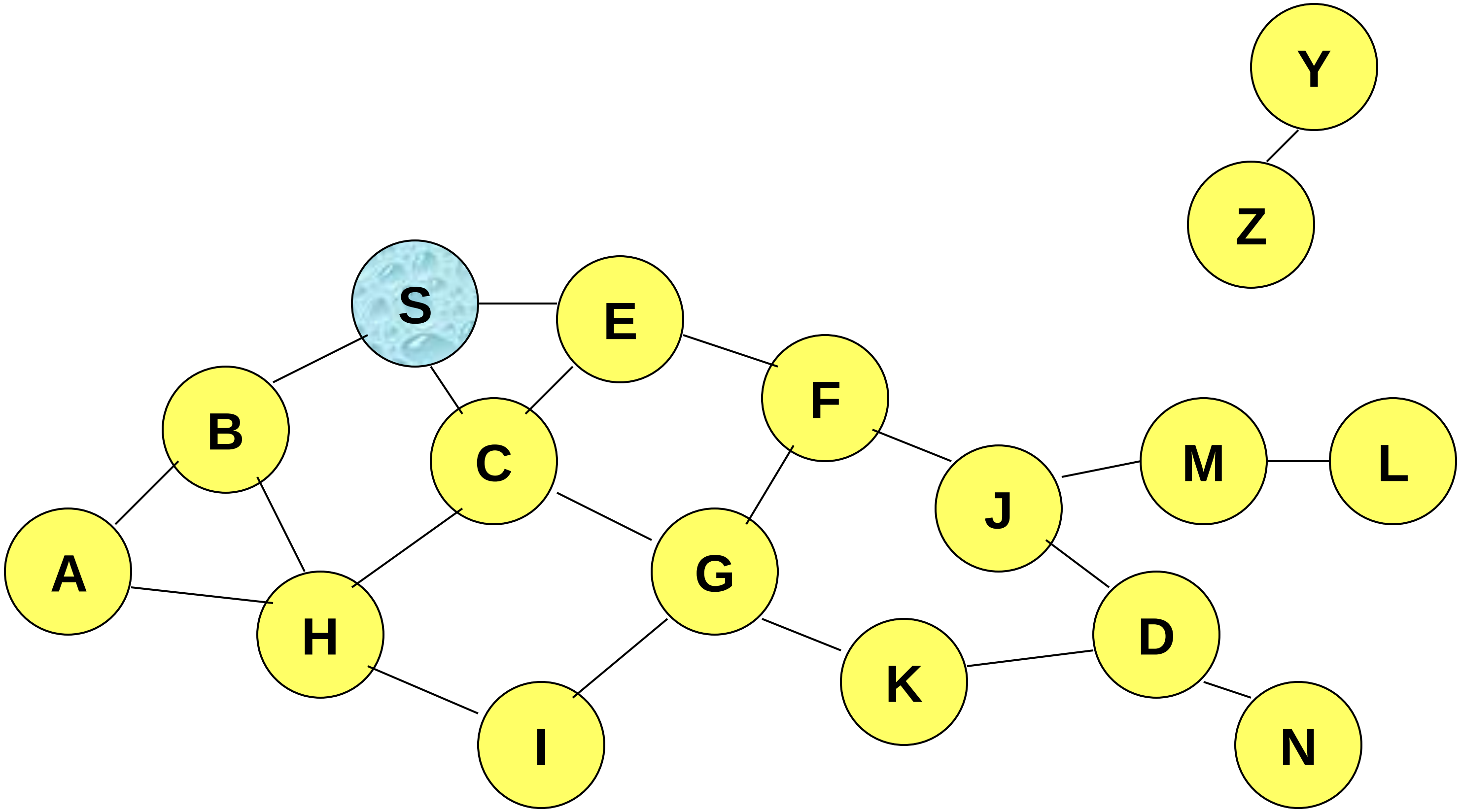
MANET routing protocols

- Reactive protocols
  - Determine route if and when needed
  - Example: DSR (dynamic source routing)
- Proactive protocols
  - Traditional distributed shortest-path protocols
  - Example: DSDV (destination sequenced distance vector)
- Hybrid protocols
  - Adaptive; Combination of proactive and reactive
  - Example : ZRP (zone routing protocol)

Dynamic Source Routing (DSR)

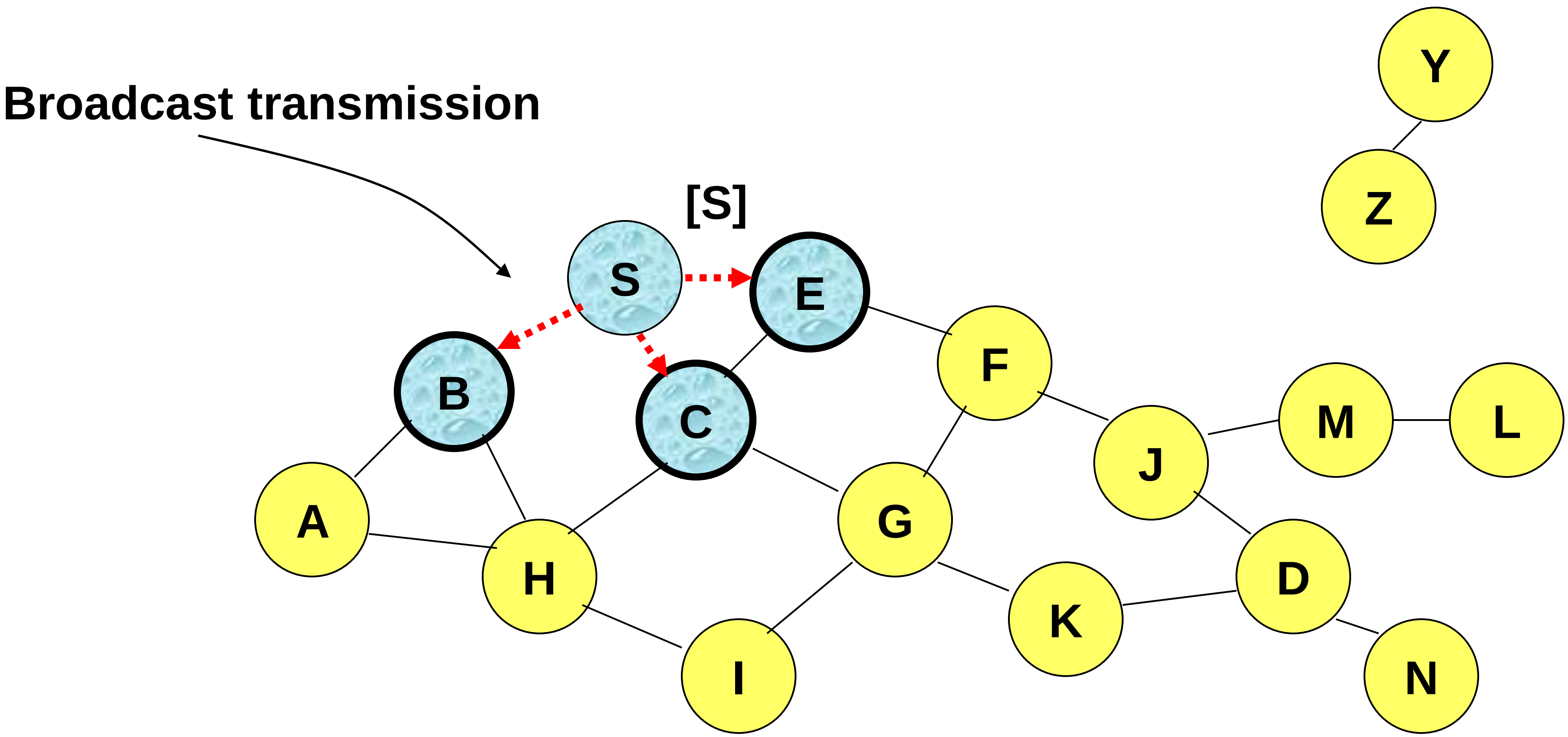
- Source S initiates a route discovery by flooding Route Request (RREQ)
  - Each node appends its own identifier when forwarding RREQ
- Destination D on receiving the first RREQ, sends a Route Reply (RREP)
  - RREP sent on route obtained by reversing the route appended in RREQ
  - RREP includes the route from S to D, on which RREQ was received by D
- S routes data using “source route” mechanism

Route Discovery in DSR



Represents a node that has received RREQ for D from S

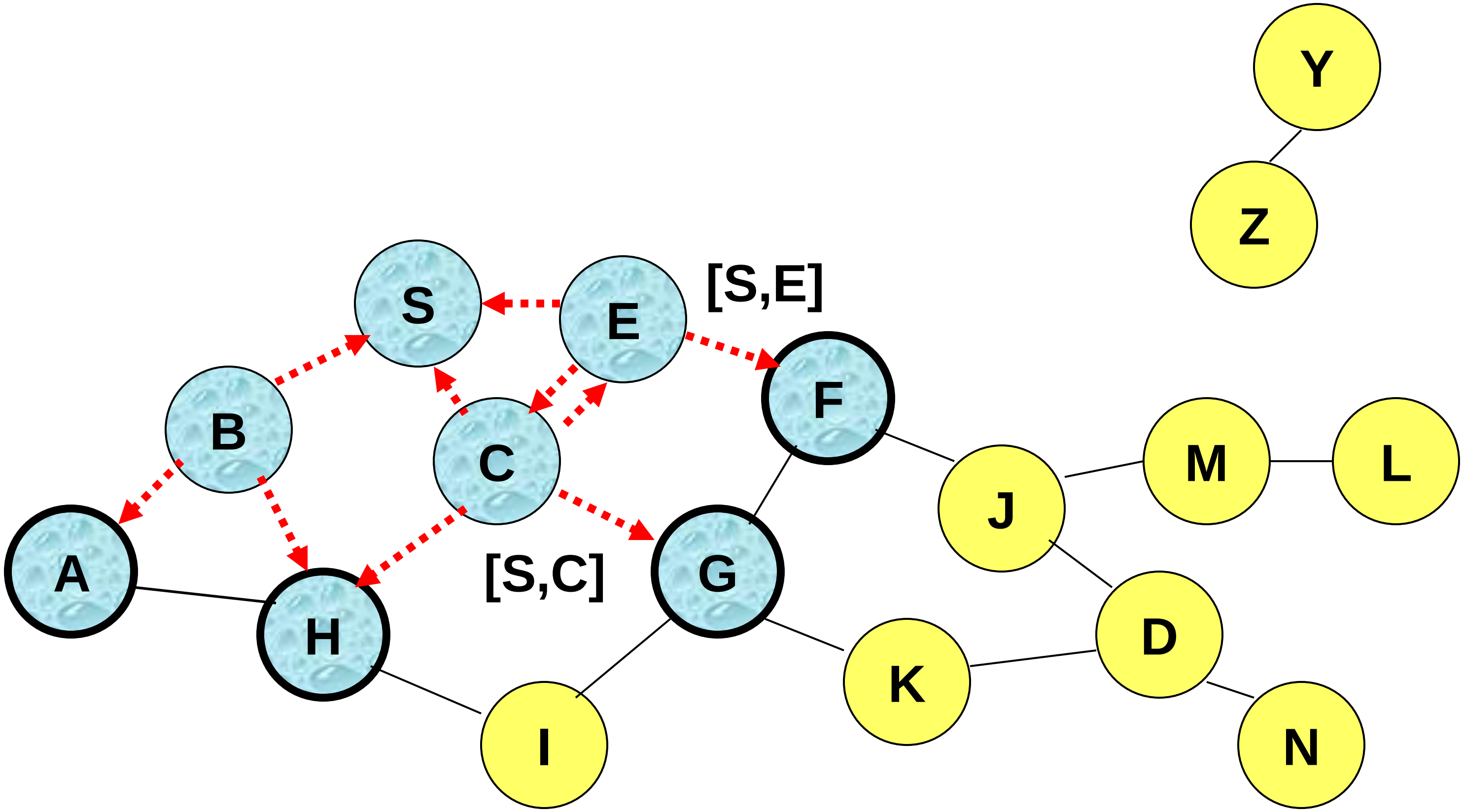
Route Discovery in DSR



Represents transmission of RREQ

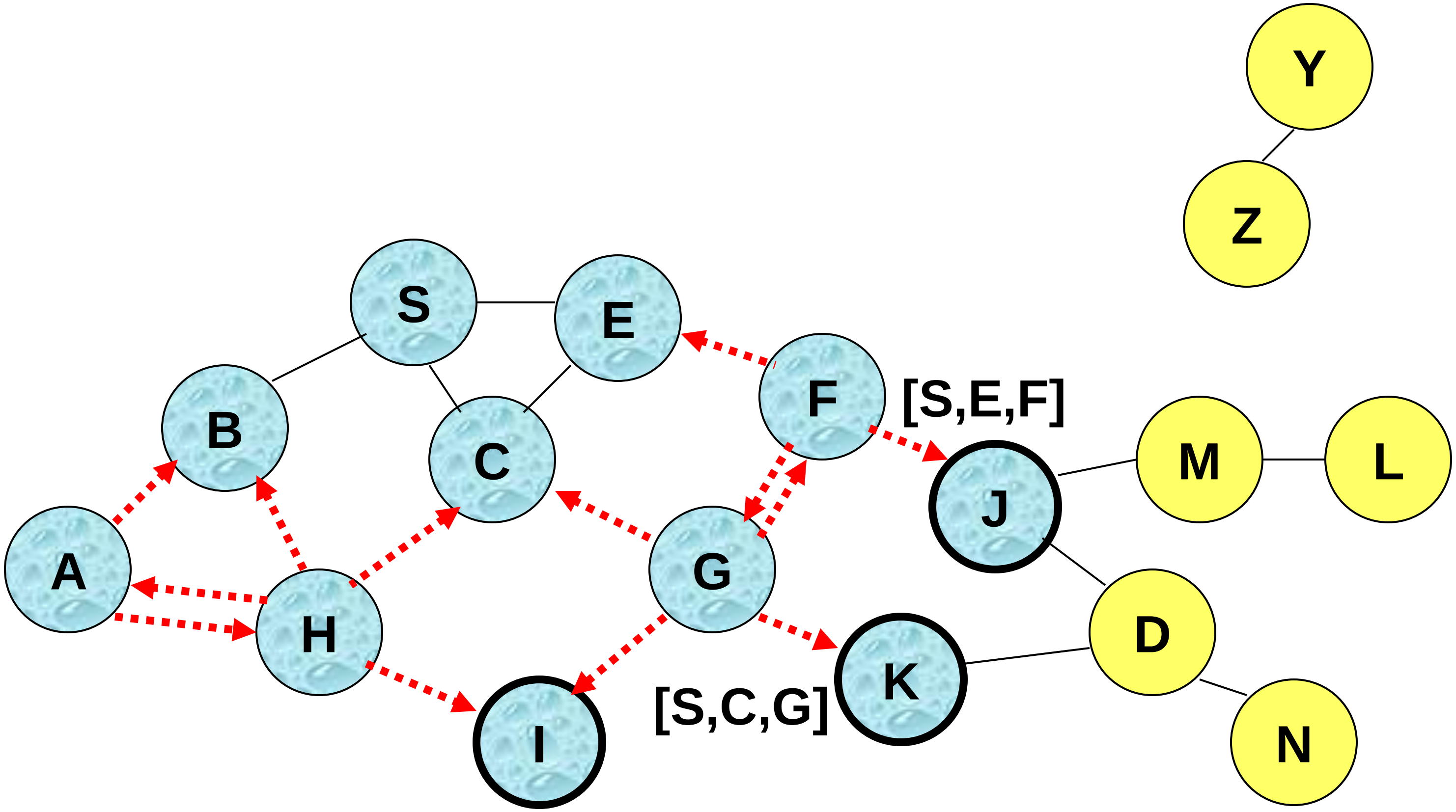
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



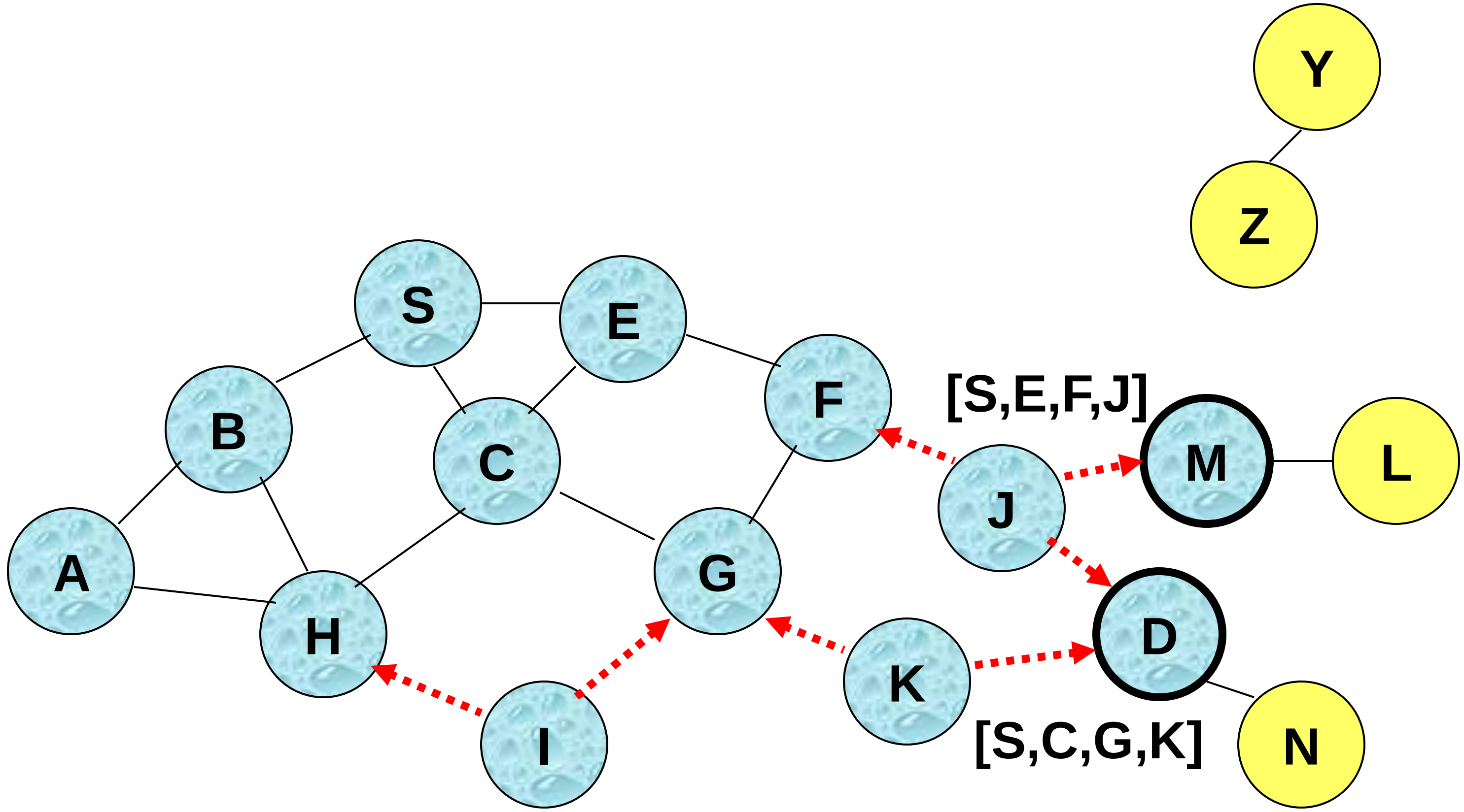
- **Node H receives packet RREQ from two neighbors: potential for collision**

Route Discovery in DSR



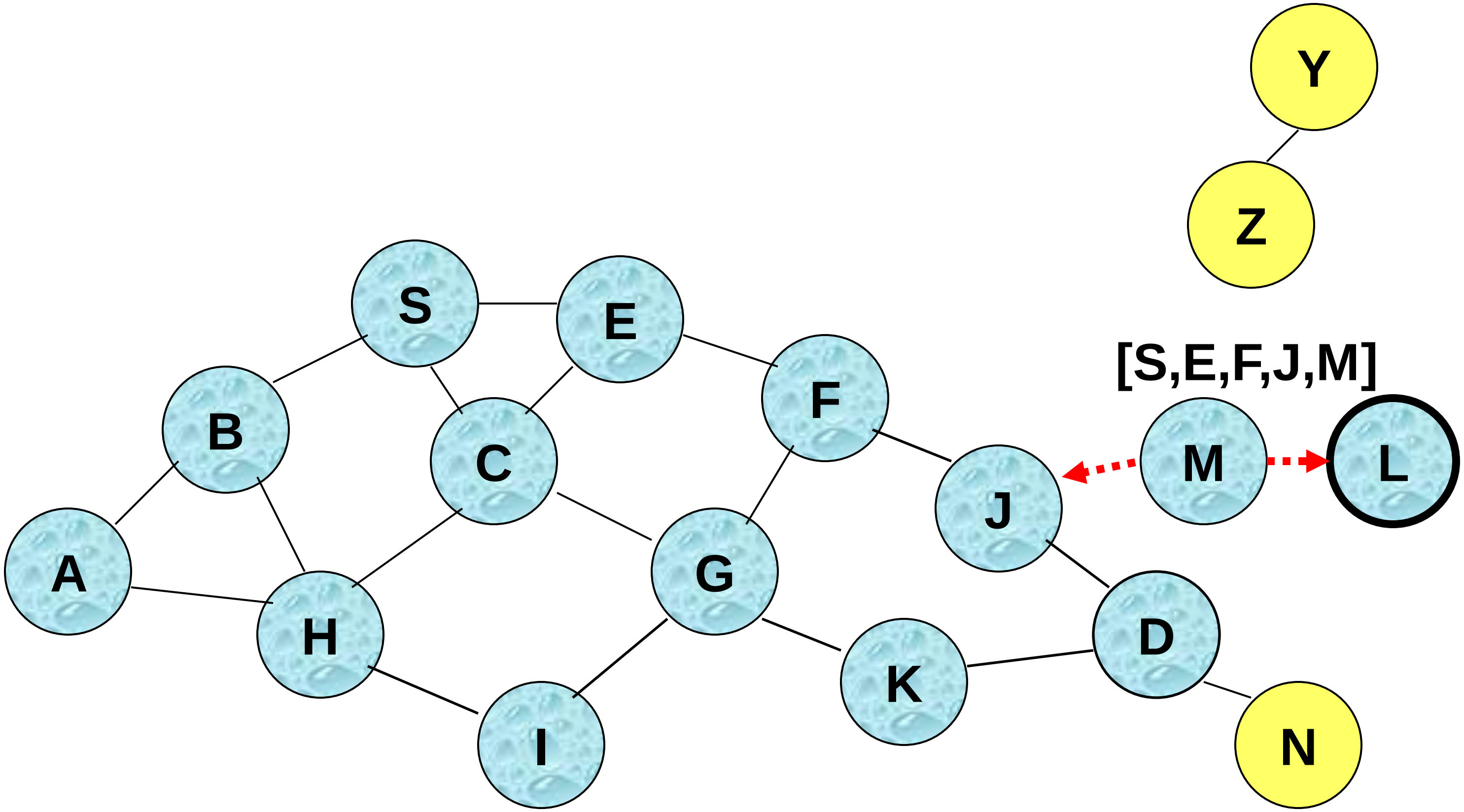
- **Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once**

Route Discovery in DSR



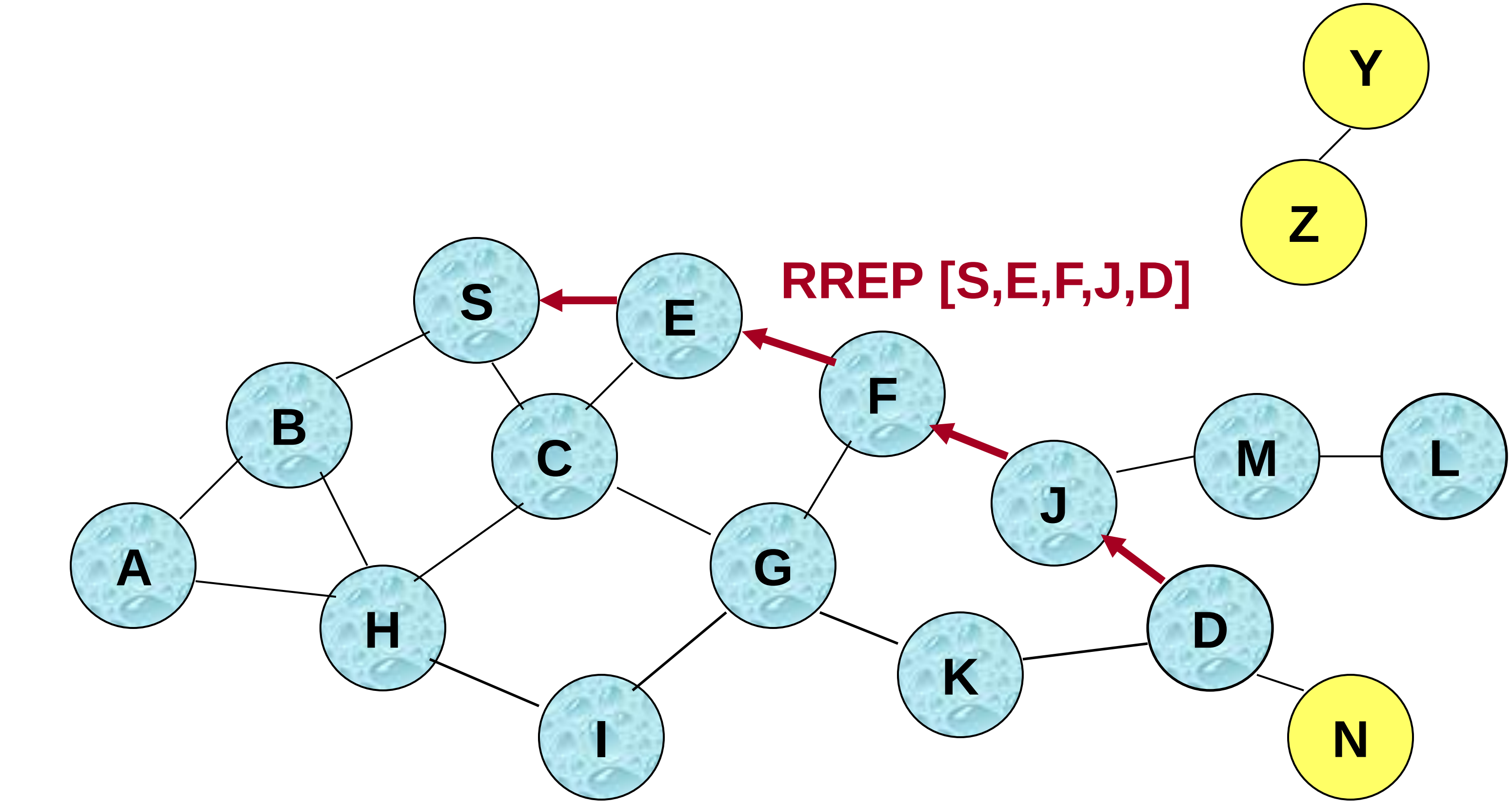
- Nodes J and K both broadcast RREQ to node D
- Since nodes J and K are hidden from each other, their transmissions may collide

Route Discovery in DSR



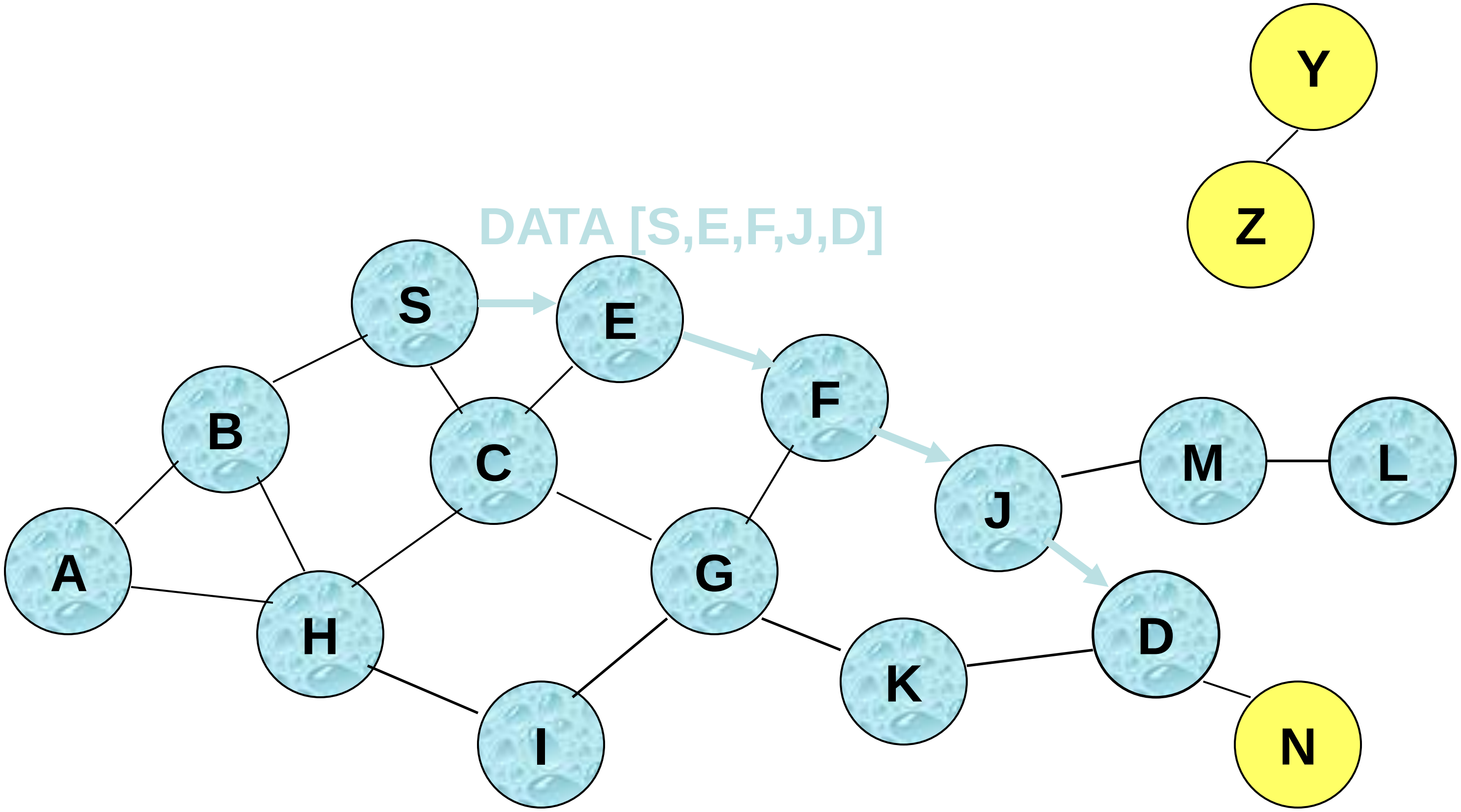
- **Node D** **does not forward** **RREQ, because node D is the** **intended target** **of the route discovery**

Route Reply in DSR



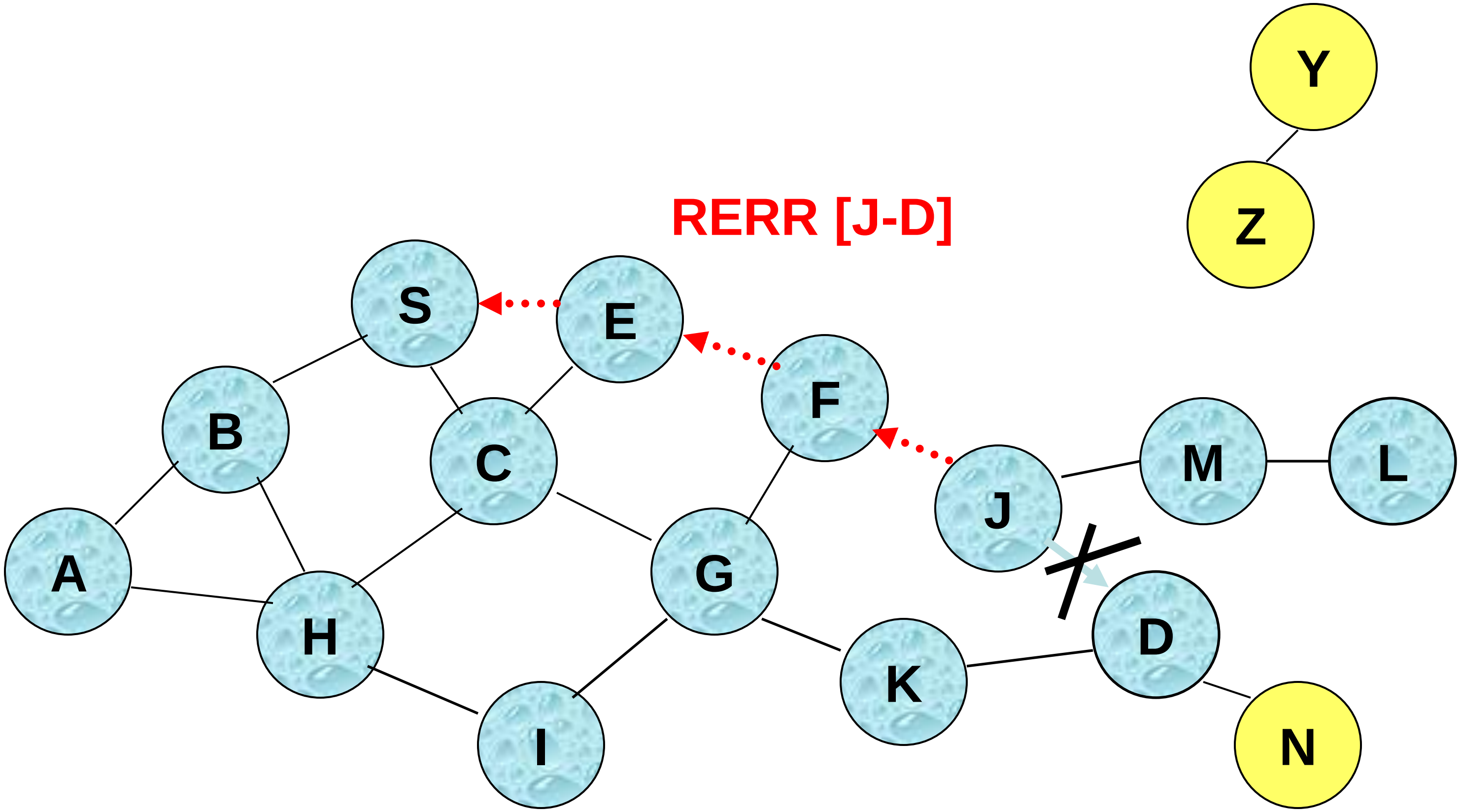
Represents RREP control message

Data Delivery in DSR



Packet header size grows with route length

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 (an ACK mechanism has to be there in packet forwarding)

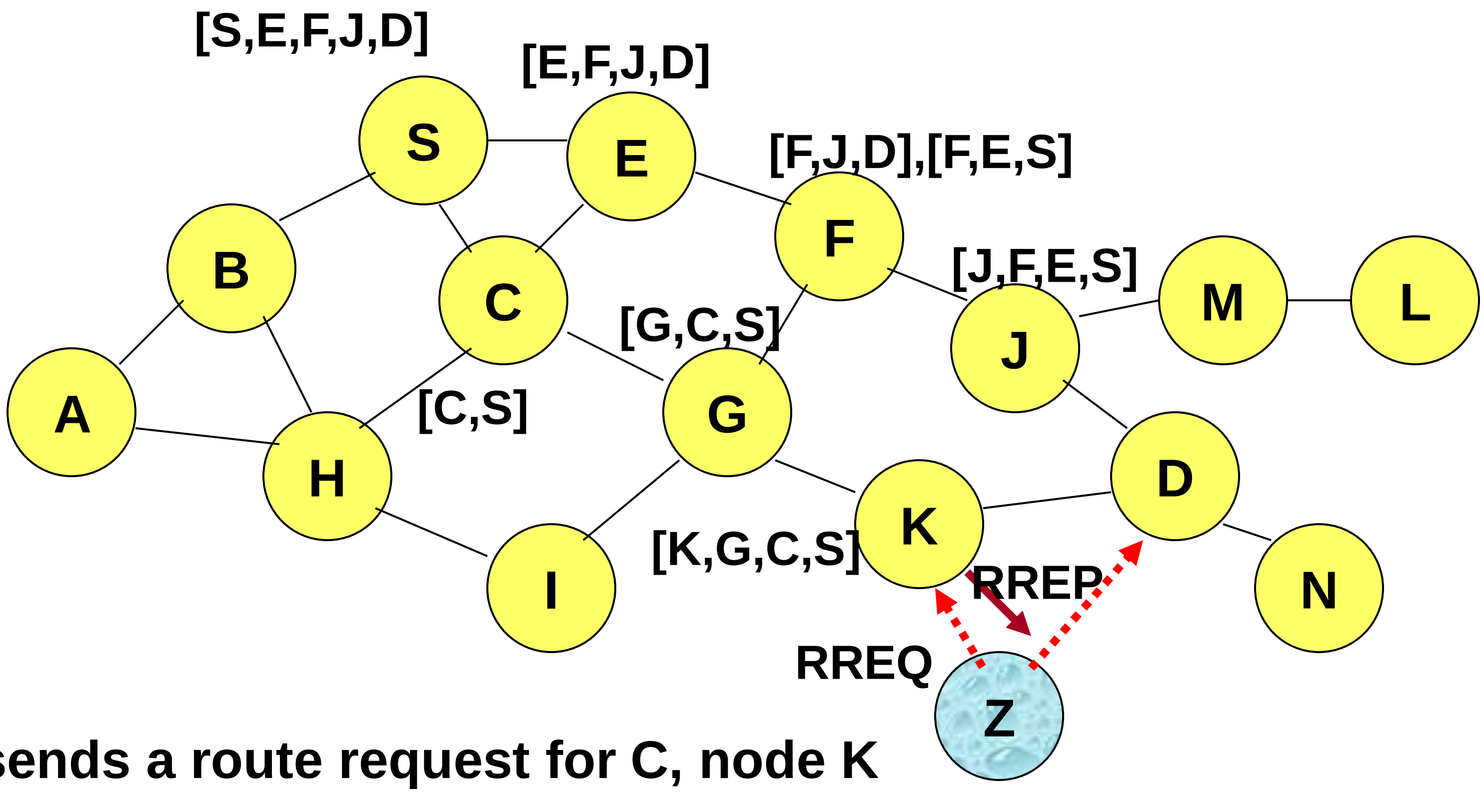
DSR: Route caching

- 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

Route caching

- 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 overhear Data to learn routes

Use of route caching



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

Route caching

- Uses:
  - Finding alternate routes in case original route breaks
  - Route reply from intermediate nodes
- Problems:
  - Cached routes may become invalid over time and due to host mobility
  - Stale caches can adversely affect performance

DSR: 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

DSR: Disadvantages

- Packet header size grows with route length due to source routing
- Latency to discover a route before data can be sent
- Flood of route requests may potentially reach all nodes in the network
- An intermediate node may send Route Reply using a stale cached route, thus polluting other caches
  - Inconsistency during route reconstruction phase

DSDV (Destination-Sequenced DV)

- Very similar to wireline DV protocol
- A table driven routing protocol
  - Routes to all destinations are readily available
- Each mobile node advertises its own routing table to each of its neighbors periodically
- When there is a significant new information (e.g. link failed), a node immediately advertises its routing table

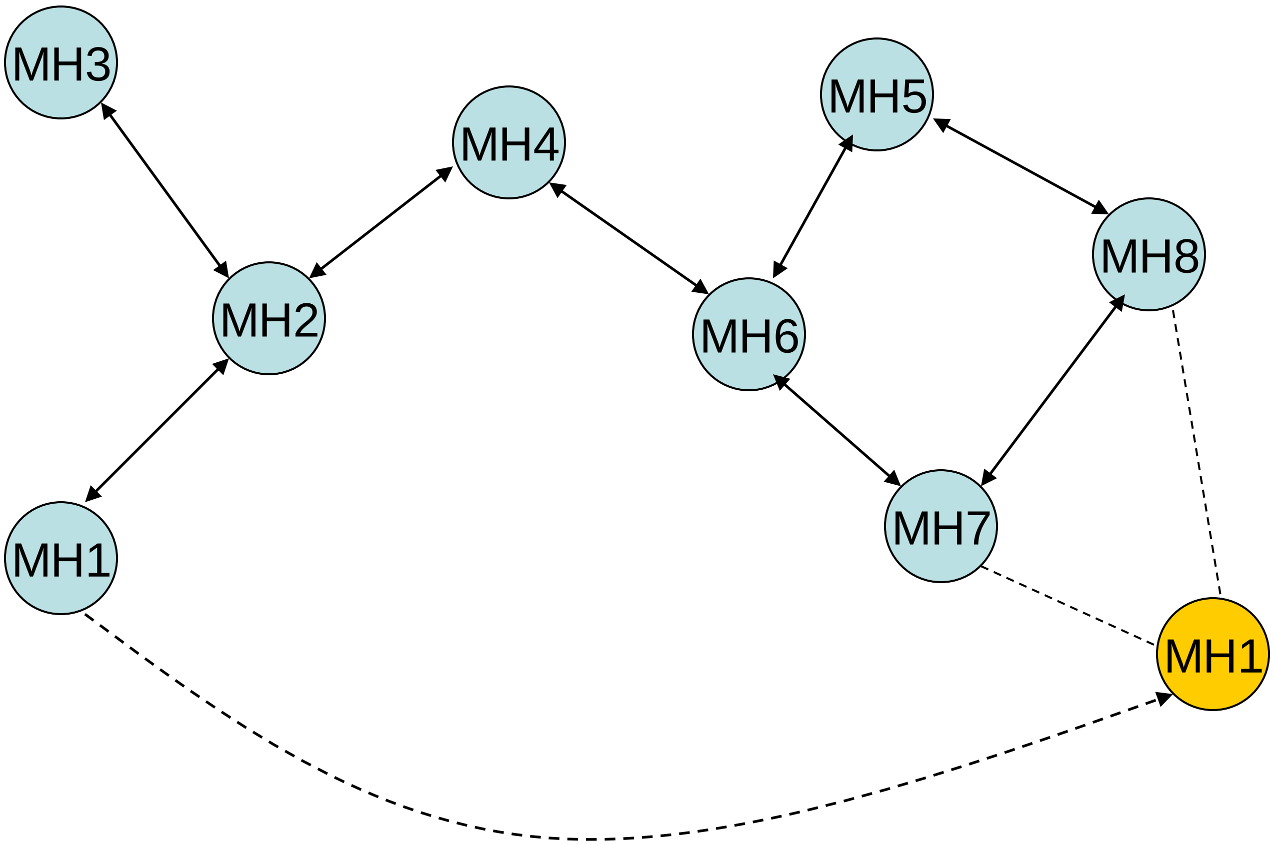
DSDV (Destination-Sequenced DV)

- Each entry of the advertised data contains
  - destination address
  - number of hops required to reach the dst
  - the seq number of the information received regarding that dst
- When a node receives new routing info
  - If it is newer than what is currently in the routing table (comparing the seq number), then it replaces the current info
  - The metric for routes received in the routing info is incremented by one
  - Newly recorded routes are marked for immediate advertisement
  - Routes which only got a more recent sequence number may be scheduled for advertisement at a later time

DSDV

- When a link breaks (because of mobility) (may be detected by layer-2 or inferred by layer-3 when no broadcast is received from the neighbor for a while)
  – infinity is assigned as metric to that link
  – any route through that link is assigned infinity as metric and a new seq number
- When a node receives infinity metric and it has an equal or later seq number with finite metric, then it triggers an update to propagate the new route

Example DSDV



Example DSDV

Routing table at MH4

Destination	Next hop	Metric	Sequence number
MH1	MH2	2	S406_MH1
MH2	MH2	1	S128_MH2
MH3	MH2	2	S564_MH3
MH4	MH4	0	S710_MH4
MH5	MH6	2	S392_MH5
MH6	MH6	1	S076_MH6
MH7	MH6	2	S128_MH7
MH8	MH6	3	S050_MH8

Example DSDV

Advertisement from MH4

Destination	Metric	Sequence number
MH1	2	S406_MH1
MH2	1	S128_MH2
MH3	2	S564_MH3
MH4	0	S710_MH4
MH5	2	S392_MH5
MH6	1	S076_MH6
MH7	2	S128_MH7
MH8	3	S050_MH8

Example DSDV

Routing table at MH4 (after MH1 moves)

Destination	Next hop	Metric	Sequence number
MH1	MH6	3	S516_MH1
MH2	MH2	1	S128_MH2
MH3	MH2	2	S564_MH3
MH4	MH4	0	S710_MH4
MH5	MH6	2	S392_MH5
MH6	MH6	1	S076_MH6
MH7	MH6	2	S128_MH7
MH8	MH6	3	S050_MH8

Example DSDV

Advertisement from MH4 (after MH1 moves)

Destination	Metric	Sequence number
MH4	0	S710_MH4
MH1	3	S516_MH1
MH2	1	S128_MH2
MH3	2	S564_MH3
MH5	2	S392_MH5
MH6	1	S076_MH6
MH7	2	S128_MH7
MH8	3	S050_MH8

DSDV: Advantages

- Routes available to all destinations
  - Less latency in route set up

DSDV: Disadvantages

- Updates are propagated throughout the network
  - Updates due to broken link (due to mobility) can lead to heavy control traffic
  - Even a small network with high mobility or large network with low mobility can choke the network
- In order to get information about a particular destination node, a node has to wait for a table update msg initiated by the same destination node
  - This delay would result in stale routing information

Ad Hoc On-Demand Distance Vector Routing (AODV)

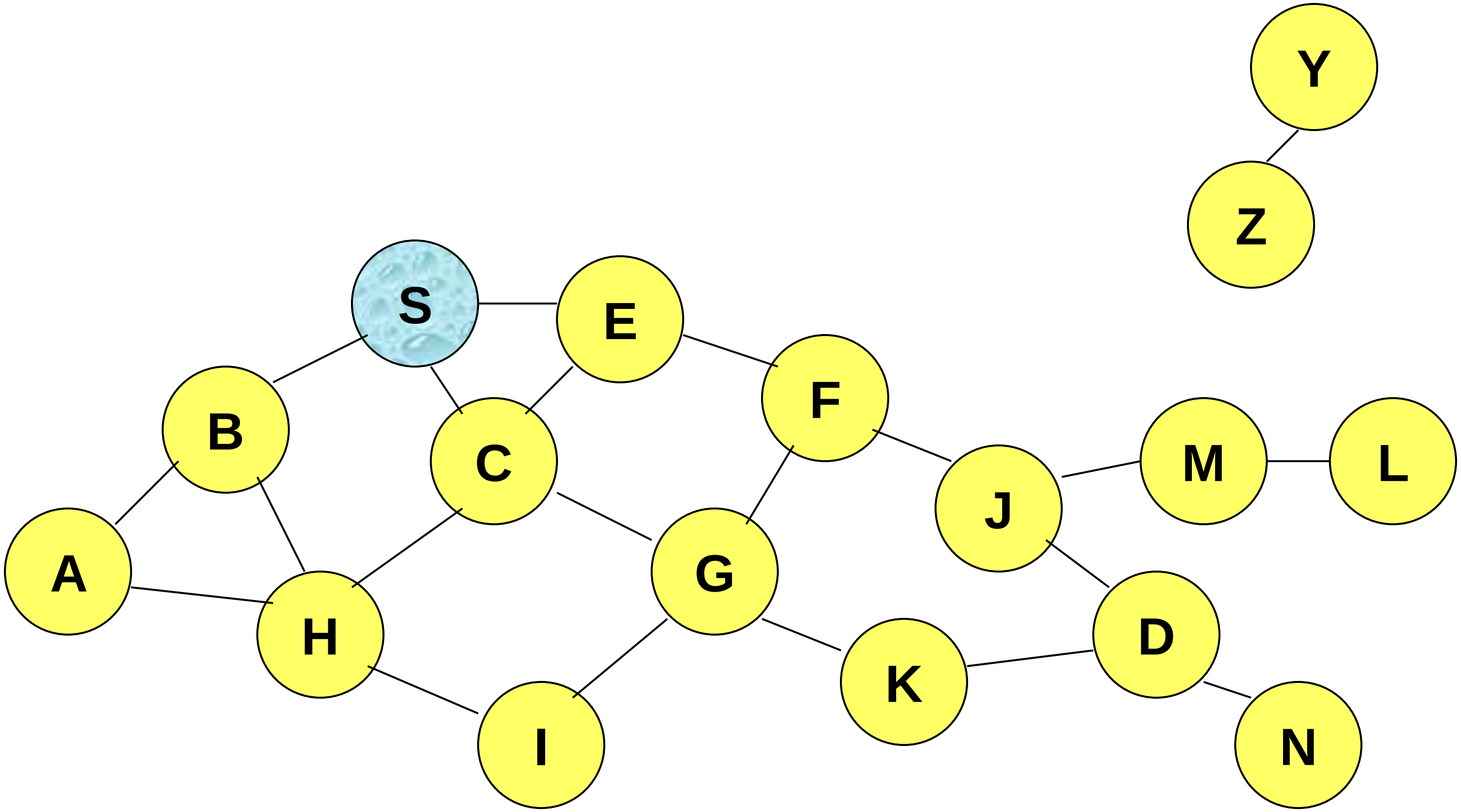
- DSR includes source routes in packet headers
- Resulting large headers can sometimes degrade performance
  - particularly when data contents of a packet are small

- AODV attempts to improve on DSR by maintaining routing tables at the intermediate nodes, so that data packets do not have to contain routes

AODV

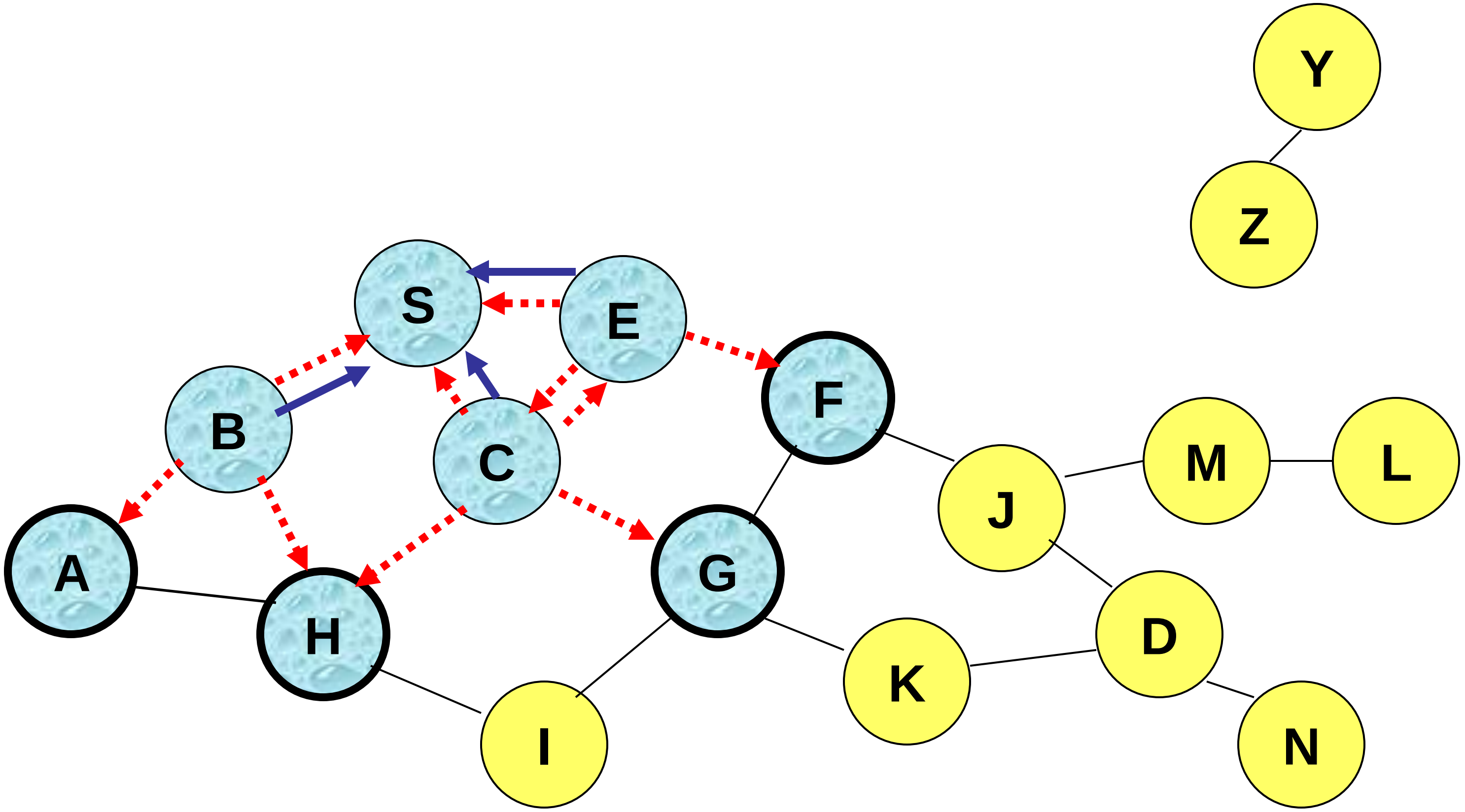
- Route Requests (RREQ) are forwarded in a manner similar to DSR
- When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source
- Route Reply (RREP) travels along the reverse path set-up when Route Request is forwarded

Route Requests in AODV



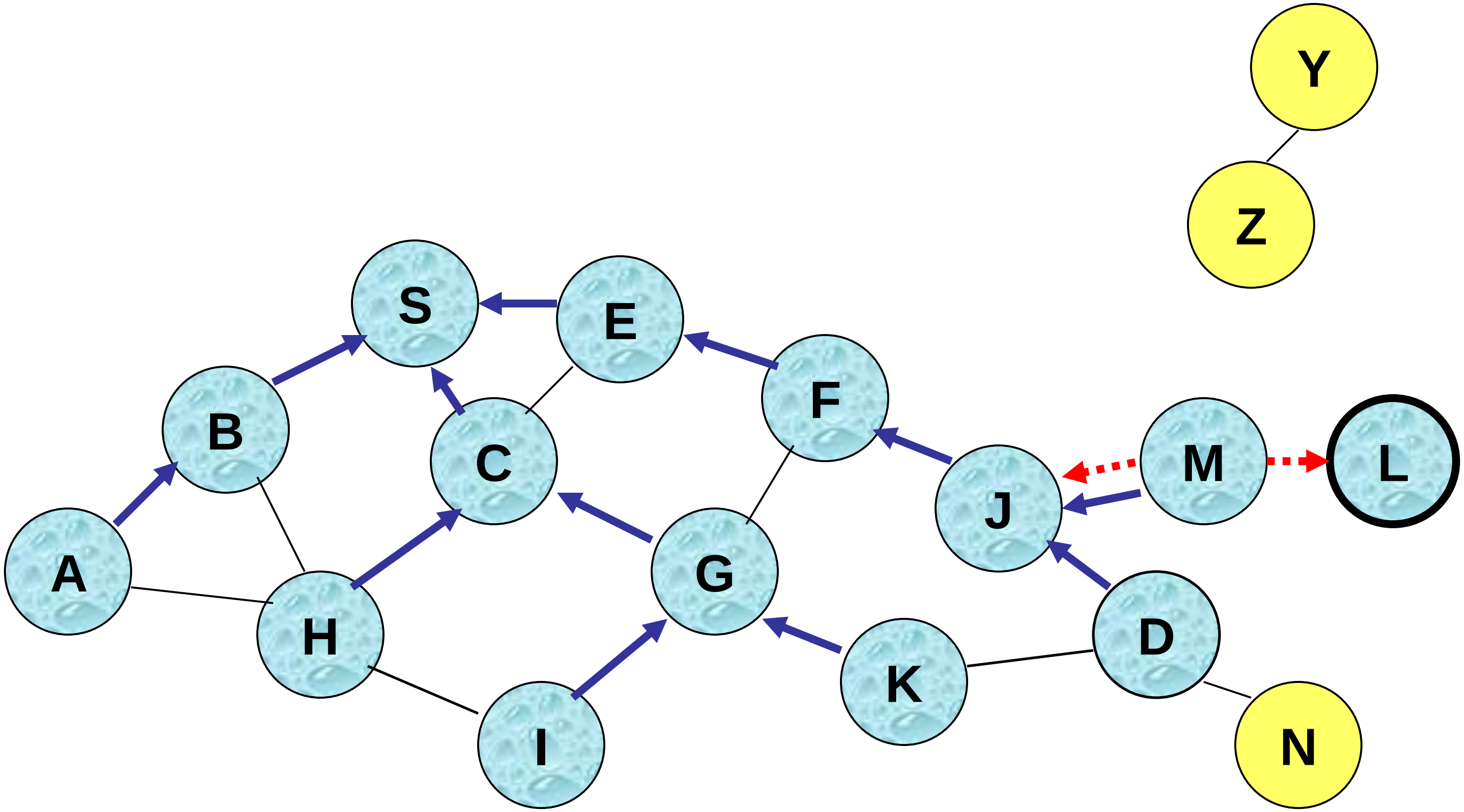
Represents a node that has received RREQ for D from S

Reverse Path Setup in AODV



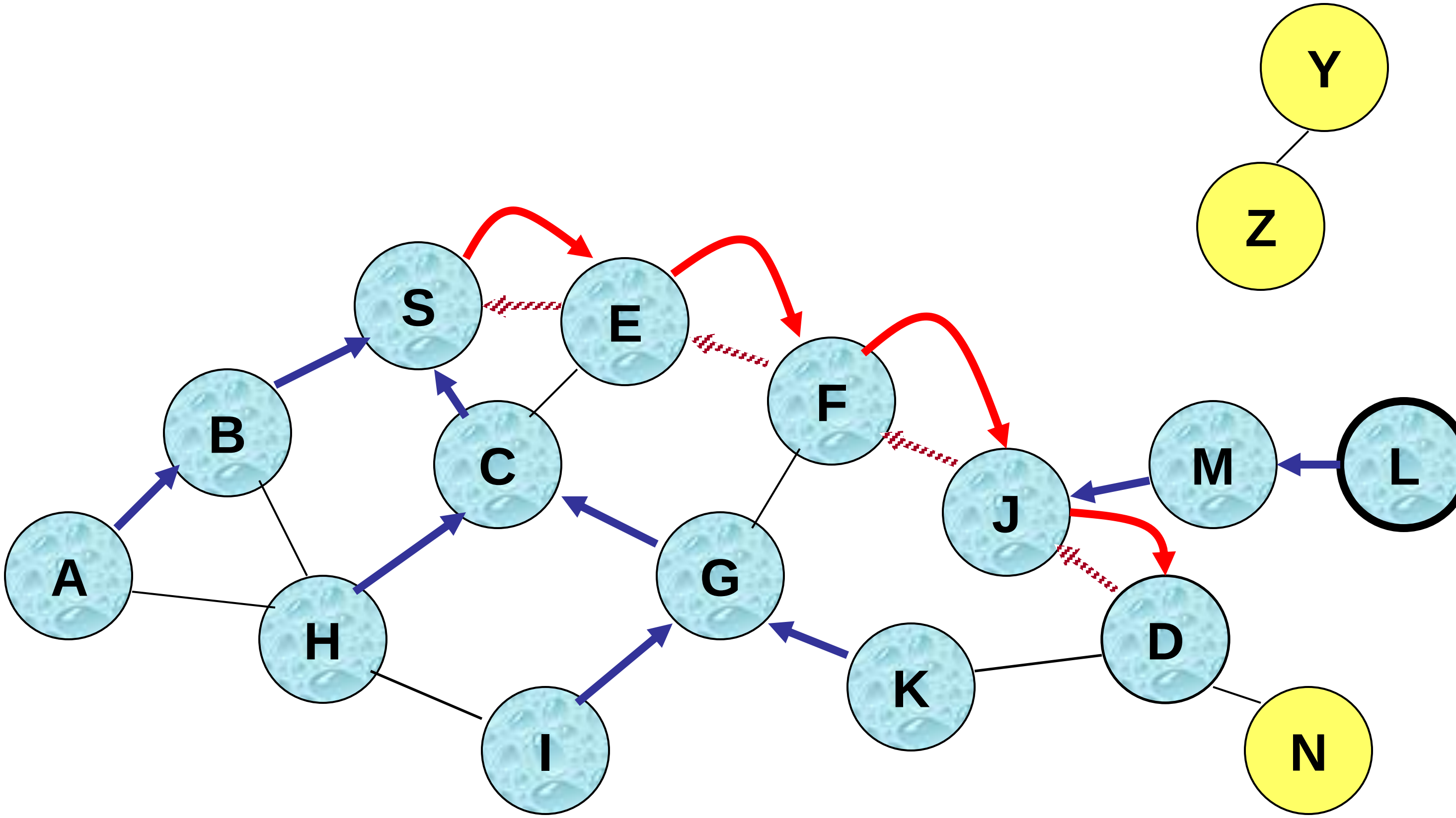
Represents links on Reverse Path

Reverse Path Setup in AODV

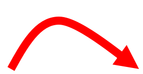


- **Node D does not forward RREQ, because node D is the intended target of the RREQ**

Forward Path Setup in AODV



Forward links are setup when RREP travels along the reverse path



Represents a link on the forward path

Route Request and Route Reply

- The RREQ request at the source contains
  - src, dst ip address
  - current seq number
  - last known seq number
  - broadcast id of the req (which is incremented every time the source node initiates a RREQ
  - broadcast id and source id form a unique id for the RREQ msg
    - used to identify duplicate RREQ msg
- When a node receives RREQ
  - drops the request if it has seen the req (by noting the unique broadcast id and src id)
  - otherwise it sets up a reverse route entry for the src node in the routing table (for forwarding RREP)
    - contains src IP, seq number, IP addr of the neighbor from which the msg came

Route Request and Route Reply

- When a node receives RREP
  - Sets up a forward path entry to the dst in its routing table
    - this entry contains dst IP, nbr IP address from where it received the RREP and the hop count, and lifetime (contained in the RREP msg)
- To respond to a RREQ
  - a node must have an unexpired entry for the destination in its route table
  - the seq number of the entry must be at least as great as carried in the RREQ msg
    - prevents loops

AODV: Timeouts

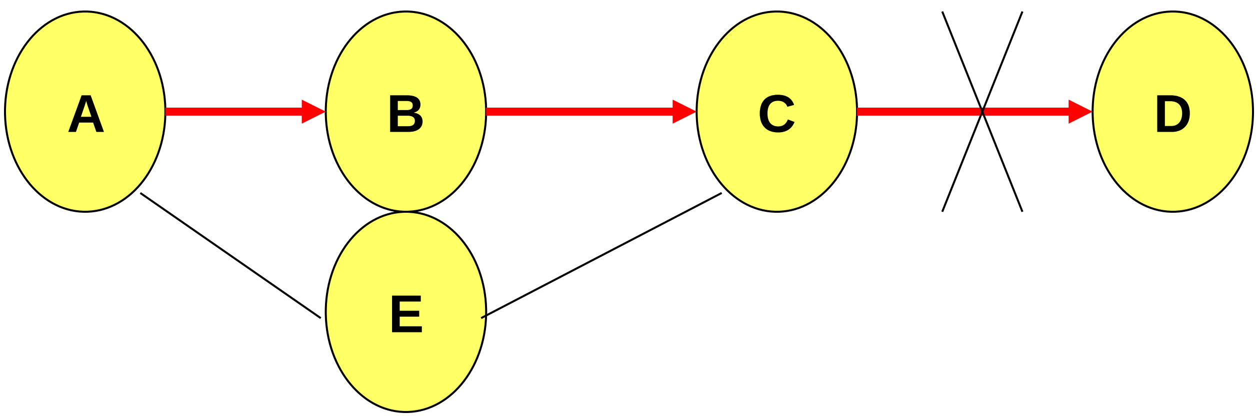
- Neighboring nodes periodically exchange hello message
- A routing table entry maintaining a reverse path is purged after a timeout interval
- A routing table entry maintaining a forward path is purged if *not used* for a *active_route_timeout* interval

AODV: Link failure

- Absence of hello message is used as an indication of link failure
- When the next hop link in a routing table entry breaks, all active neighbors are informed
- Link failures are propagated by means of Route Error (RERR) messages, which also update destination sequence numbers

AODV: Sequence numbers

- To avoid using old/broken routes
  - To determine which route is newer
- To prevent formation of loops



AODV: Sequence numbers

- Assume that A does not know about failure of link C-D because RERR sent by C is lost
- Now C performs a route discovery for D
- Node A receives the RREQ (say, via path C-E-A)
- Node A will reply since A knows a route to D via node B
- Results in a loop (for instance, C-E-A-B-C)

AODV: Expanding ring search

- Each RREQ msg is broadcast to the entire network
  - For a large network this could be detrimental
- To control the scope of broadcast, the src node should use an *expanding ring search* technique
- Route Requests are initially sent with small Time-to-Live (TTL) field, to limit their propagation
  - DSR also includes a similar optimization
- If no Route Reply is received, then larger TTL tried

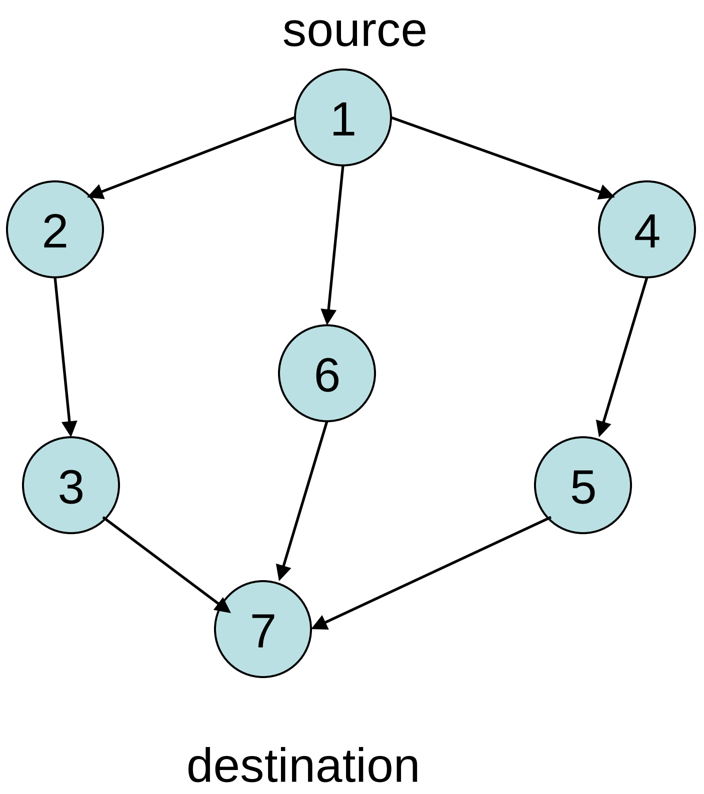
AODV: Summary

- Routes need not be included in packet headers
- Nodes maintain routing tables containing entries only for routes that are in active use
- At most one next-hop per destination maintained at each node
- Sequence numbers are used to avoid old/broken routes and prevent routing loops

Temporally Ordered Routing Algorithm (TORA)

- Source-initiated on-demand routing protocol
- Each node maintains its one hop local topology
- In case of topology change, control packets are limited to small region
  - This is an important property for MANET
- Basically uses a *destination oriented* directed acyclic graph (DAG) using a Query/Update mechanism

TORA



H(7) < H(3) < H(2) < H(1)

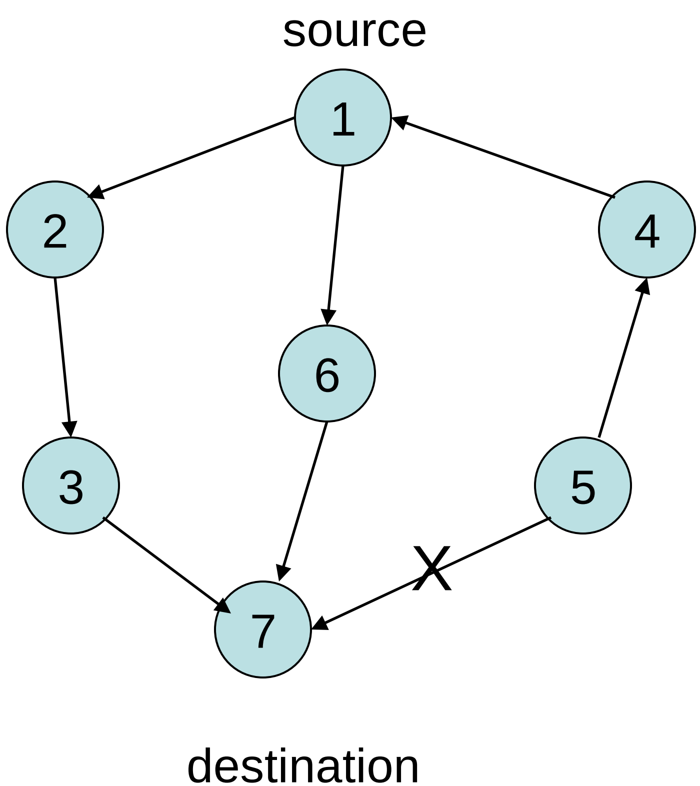
TORA

- When node 1 has data to send to destination 7, it originates a *Query* packet (the packet carries address of destination)
- The Query packet is forwarded by intermediate nodes 2, 3, 4, 5 and 6 and reaches 7
- The node that terminates (in this case, 7) the Query packet, replies with an *Update* packet containing its distance from the destination (zero at the destination).
  - Note that the Query packet need not always travel to the destination
    - Intermediate nodes may have a path to the destination, so they can send Update packet

TORA

- Each node that receives the Update packet sets its distance (or Height) to a value higher than the distance of the sender of the Update packet
- Thus, a set of directed links from the node which originated the Query to the destination node 7 is created.
- This forms a DAG
- Once source node 1 receives Update msg, it starts sending data packets

TORA



H(5) > H(4) > H(1)

TORA

- When node 5 discovers that its link to destination 7 is broken, it changes its Height (or distance) value to a value larger than its neighbors and originates a Update msg.
- 4 receives this Update and reverses the link between 1 and 4 and forwards the Update msg (H(5) < H(4) < H(1))

TORA

- If link between 1 and 4 breaks
  - 4 reverses link between itself and 5 and sends Update msg to 5
  - This conflicts with the earlier reversal: a partition can be inferred by 5

TORA

- Advantages
  - Limits control packets to a small region when topology changes: less overhead
- Disadvantage
  - Local reconfiguration of paths could lead to non-optimal routes
  - Concurrent detection of partitions and subsequent deletion of routes could lead to temporary oscillations and transient loops.

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)

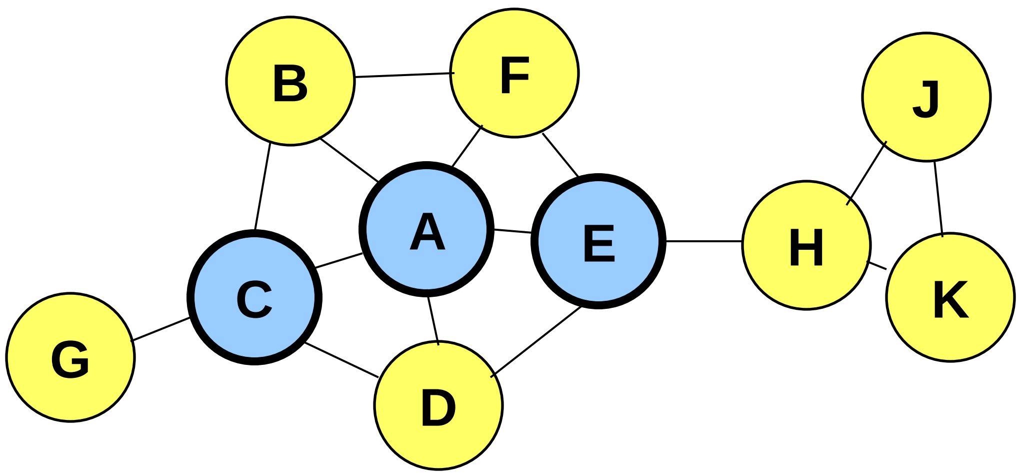
- A Proactive routing protocol
- Optimizes the link state protocol
  - Reducing the number of links that are used for forwarding the link state advertisements
- The overhead of flooding link state information is reduced by requiring fewer nodes to forward the information
  - A broadcast from node X is only forwarded by its *multipoint relays*
  - 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

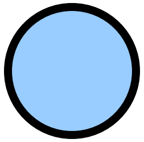
Multi Point Relay (MPR) Set

- 1. MPR(x) = φ
- 2. MPR(x) = {those nodes which belong to $N_1(x)$ and which are the only neighbors of nodes in $N_2(x)$
- 3. While there exists some node in $N_2(x)$ which is not covered by MPR(x)
  - a) For each node in $N_1(x)$ which is not in MPR(x), compute the maximum number of nodes that it covers among the uncovered nodes in the set $N_2(x)$.
  - B) Add to MPR(x) the node belonging to $N_1(x)$, for which this number is maximum
- $N_i(x) = i^{th}$ hop neighbor of x

Optimized Link State Routing (OLSR)

- Nodes C and E are multipoint relays of node A
- Nodes C and E forward information received from A




Node that has broadcast state information from A

Protocol Trade-offs

- Proactive protocols
  - Based on traditional wired routing protocols
  - Always maintain routes
  - Little or no delay for route determination
  - Consume bandwidth to keep routes up-to-date
  - Maintain routes which may never be used

Protocol Trade-offs

- Reactive protocols
  - Lower overhead since routes are determined on demand
  - routes carried in the data packets
  - Significant delay in route determination
  - Employ flooding (global search)
  - Control traffic may be bursty

Zone Routing Protocol (ZRP)

- Hybrid protocol
- Intra-zone routing: Pro-actively maintain state information for links within a short distance from any given node
  - Routes to nodes within short distance are thus maintained proactively (using, say, link state or distance vector protocol)

- Inter-zone routing: Use a route discovery protocol for determining routes to far away nodes. Route discovery is similar to DSR with the exception that route requests are propagated via *peripheral* nodes.

ZRP

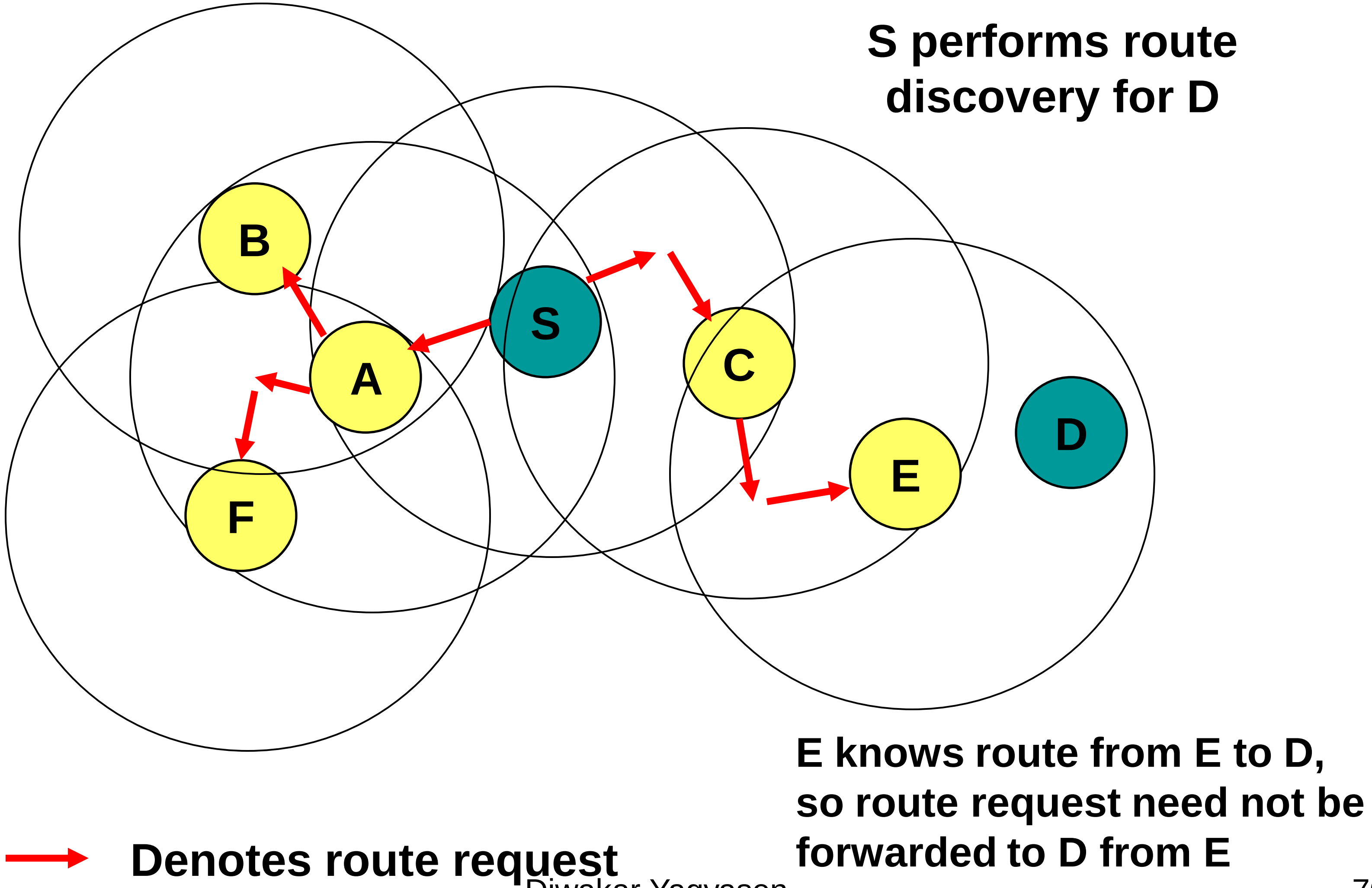
- All nodes within hop distance at most *d* from a node X are said to be in the routing zone of node X

- All nodes at hop distance exactly *d* are said to be peripheral nodes of node X's routing zone

ZRP

- Each node maintains the information about routes to all nodes within its routing zone by exchanging periodic route updates
- If source s and destination d are in the same zone, then the packet is directly delivered to the destination (the route is available in the routing database)
- Otherwise, s bordercasts (uses unicast routing to deliver packets directly to the border nodes) the *RouteRequest* packet to its peripheral nodes
  - If any peripheral node finds d in its *routing zone*, it sends *RouteReply* back to s indicating the path.
  - Otherwise, the node rebordercasts the *RouteRequest* packet to the peripheral nodes.

ZRP example: Zone Radius = *d* = 2



ZRP

- Advantages
  - Combines the best features of proactive and reactive routing schemes
- Disadvantages
  - When there are overlaps in the nodes' routing zones, there may be redundant RouteRequests sent out. These need to be suppressed
  - Choosing zone radius is quite tricky

MANET variations

- Fully symmetric environment
  - all nodes have identical capabilities and responsibilities
- Asymmetric Capabilities
  - transmission ranges, battery life, processing capacity may differ at different nodes
- Asymmetric Responsibilities
  - only some nodes may route packets

MANET variations

- Mobility patterns may differ from one scenario to another
- Mobility characteristics (speed, predictability) may be different for different applications
- Traffic characteristics may differ
  - timeliness constraints
  - reliability requirements

MANET summary

- Routing is the most studied problem
- Cross-layer approach being researched

- Large number of simulation based experiments
- Small number of field trials
- Very few reported deployments

References

- D. B. Johnson, D. A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks”, Mobile Computing, Kluwer Academic Publishers, vol. 353, pp. 153-181, 1996.
- C. E. Perkins, E. M. Royer, “Ad Hoc On-Demand Distance Vector Routing”, Proc. of IEEE Workshop on Mobile Computing Systems and Applications, 1999, pp. 90-100, February 1999.