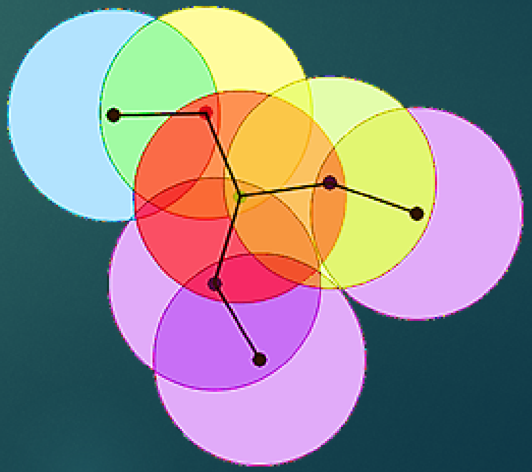
Mobile Ad-Hoc Networks & Routing Algorithms

EMMANOUIL G. SPANAKIS, PhD.

spanakis@csd.uoc.gr

COLLABORATING RESEARCHER, COMPUTATIONAL BIOMEDICINE LABORATORY, FORTH-ICS

VISITING LECTURER, COMPUTER SCIENCE DEPARTMENT, UNIVERSITY OF CRETE



Introduction

- An ad-hoc network is a **collection of mobile nodes** (ad hoc means "for this“ or "for this purpose only.”), that :
  - connect over the **wireless/wired medium**
  - **without the need of any pre-deployed existing infrastructure**.
- Nodes in a MANET can **dynamically self-organize into temporary and arbitrary and network topologies**
- Multi-hop flexible low cost last mile-extensions of wired infrastructure

Why Ad Hoc Networks ?

- Ease and Speed in deployment
- Decreased dependence on infrastructure
- Only possible solution to interconnect a group of nodes
- Many Commercial Products available today

Mobile Ad-Hoc network Applications

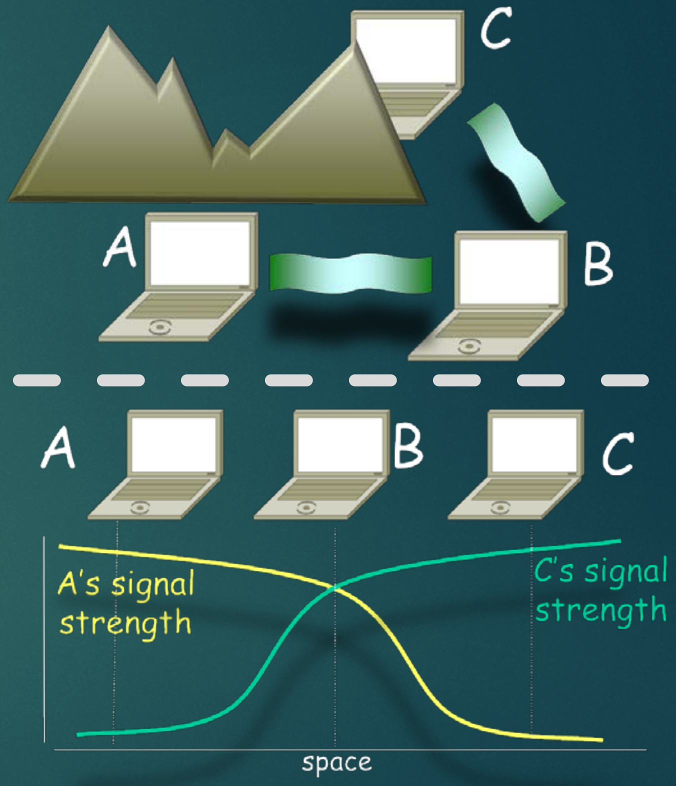
- Body Area Networking
  - body sensors network,
- Personal area Networking
  - cell phone, laptop, ear phone, wrist watch
- **Disaster Recovery Areas**
- **Emergency operations**
  - search-and-rescue (earthquakes, boats, airplanes...)
  - policing and fire fighting
- Military environments
  - **soldiers**, tanks, planes, **battlefield**
- Civilian environments
  - **vehicle networks**
  - meeting rooms
  - sports stadiums
  - boats, small aircraft
- eHealth/mHealth/uHealth

What’s unique about a mobile ad-hoc network ?

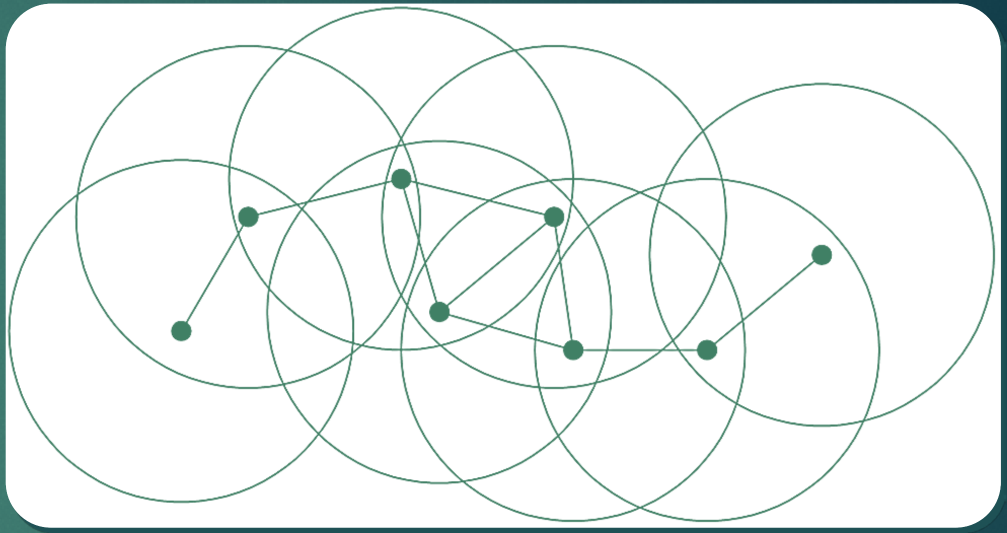
- **Traffic characteristics may differ** in different ad hoc networks
  - various and volatile wireless **link quality**
  - bit rate, reliability requirements, unicast, multicast,
  - host-based/ content-based/ capability-based addressing
- **Co-exist and Co-operate** with infrastructure-based networks
- **Mobility characteristics** may be different
  - speed, direction of movement, pattern of movement
- **Symmetric vs. Asymmetric** (nodes’ capabilities and responsibilities)
- **Pervasive (cheap) devices:** Power constraints
- **Security/**Confidentiality issues

Issues in Mobile Ad-hoc Networks

- Limited wireless transmission range
- Broadcast nature of the wireless medium
  - **Hidden terminal problem**
- 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)

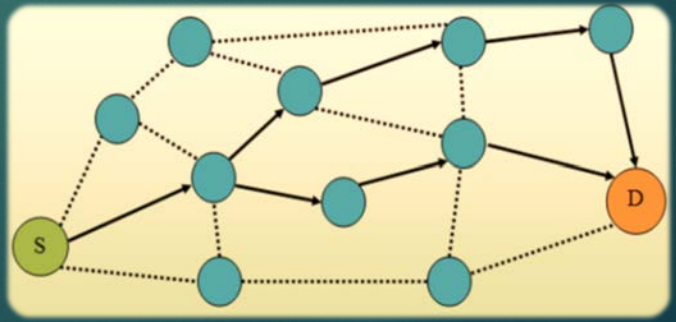


Routing in Mobile Ad-Hoc Networks



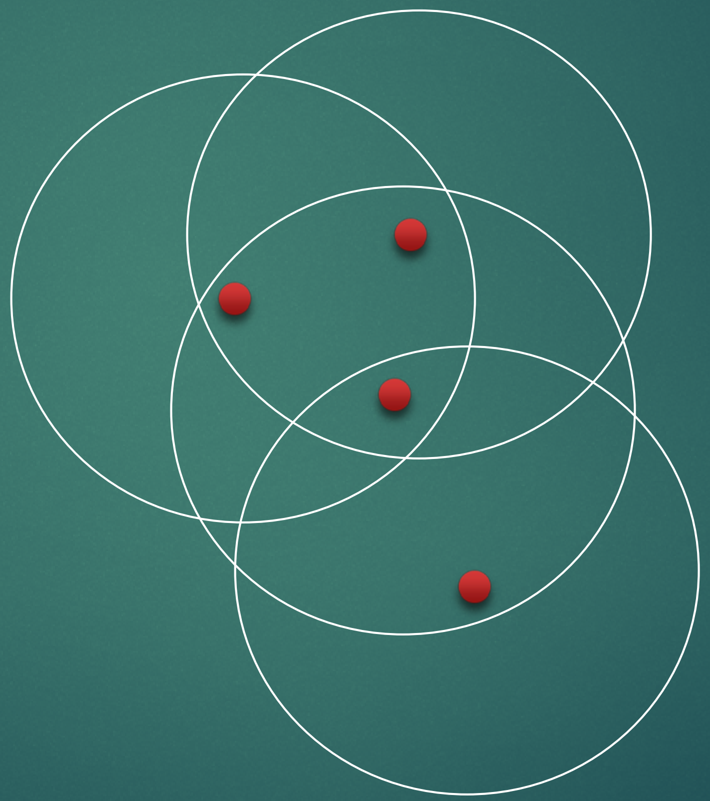
Mobile Ad Hoc Networks (MANETs)

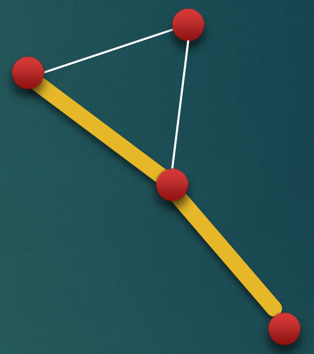
- Formed by a collection of wireless mobile hosts
- Without any pre-existing infrastructure or the aid of any centralized administration
- **Network characteristics change over time**
  - **Routes between nodes may potentially contain multiple hops**
  - Number of hosts in the network



Mobile Ad Hoc Networks

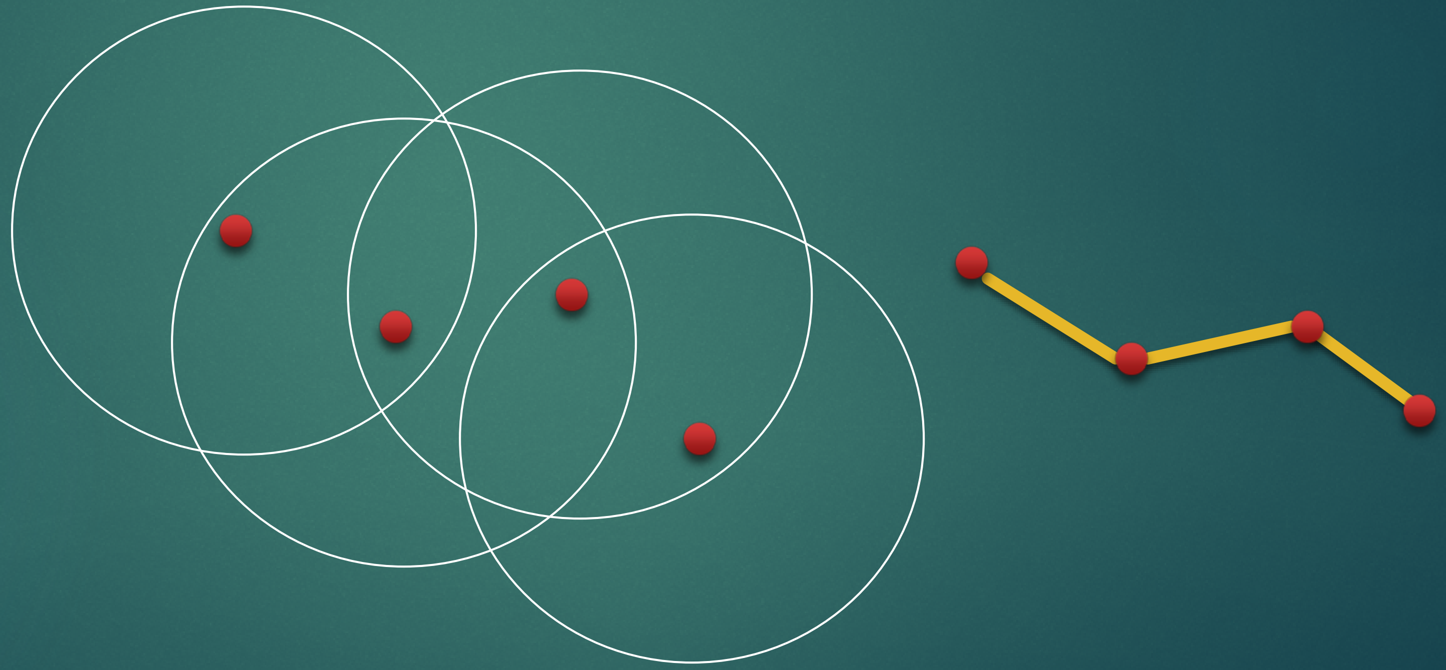
- Mobile wireless hosts
  - Only subset within range at given time
  - Want to communicate with any other node
- May need to traverse multiple links to reach a destination





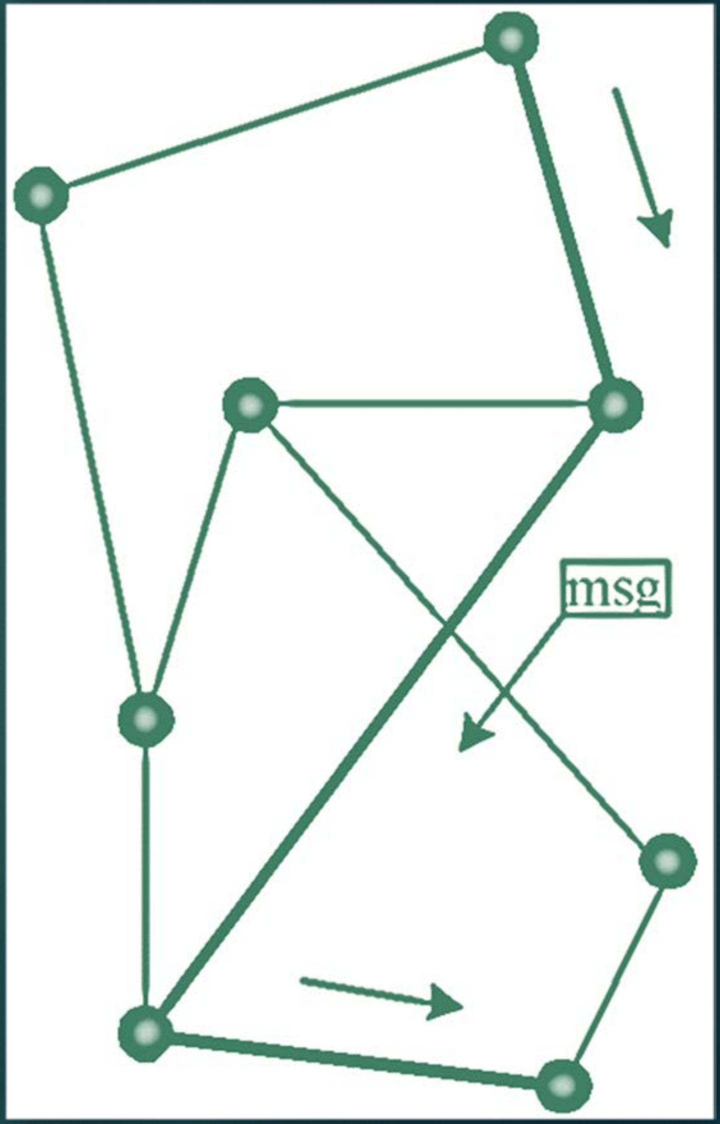
Mobile Ad Hoc Networks (MANET)

- Mobility causes route changes



Routing Overview

- Network with **nodes**, **edges**
- Goal: ***transfer message from one node to another***
  - → Which is the *best path*?
  - → Who *decides*
    source, intermediate or
    destination node(s)



Which path?

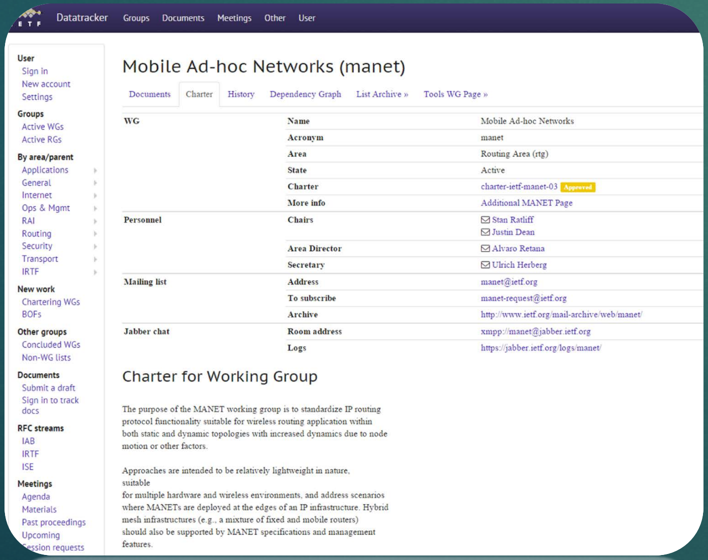
- Generally try to optimize one of the following:
  - Shortest path (*fewest hops*)
  - Shortest time (*lowest latency*)
  - Shortest weighted path (*utilize available bandwidth, battery*)

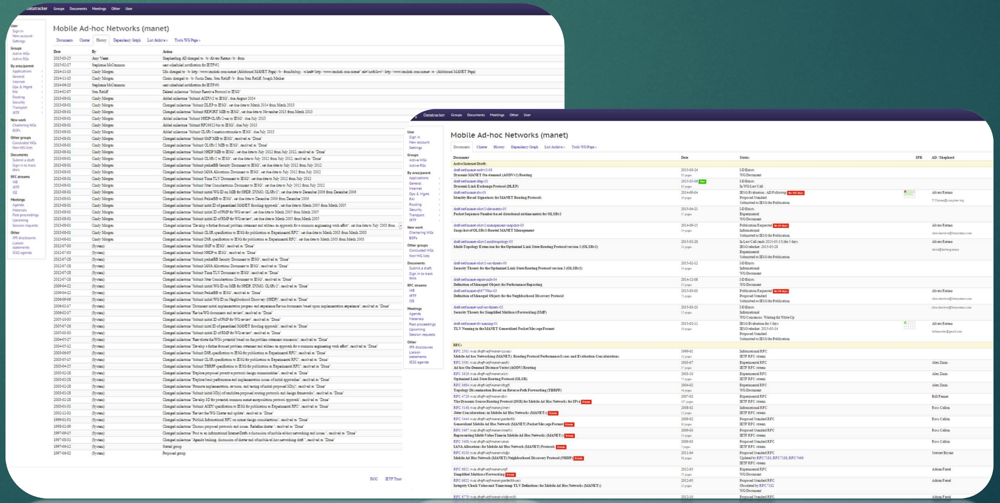
Who determines route?

- **Source** ("path") routing [Like airline travel]
  - Source specifies entire route
  - Intermediate nodes just forward to specified next hop
- **Destination** ("hop-by-hop") routing [Like postal service]
  - Source specifies only destination in message header
  - Intermediate nodes look at destination in header, consult internal tables to determine appropriate next hop

IETF **MANET** Working Group

- The Mobile Ad-hoc Networking (manet) Working Group is a chartered working group within the Internet Engineering Task Force (IETF) to **investigate and develop candidate standard Internet routing support for mobile, wireless IP autonomous segments**.
- The charter and official IETF Home Page for manet are found at : https://datatracker.ietf.org/wg/manet/charter/





Description of Working Group

- The purpose of the MANET working group is to ***standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies*** with increased dynamics due to node motion or other factors.
- Approaches are intended to be
  - lightweight in nature,
  - suitable for multiple hardware and wireless environments, and
  - address scenarios where MANETs are deployed at the edges of an IP infrastructure.
- Hybrid mesh infrastructures (e.g., a mixture of fixed and mobile routers) should also be supported by MANET specifications and management features.
- Using mature components from previous work on experimental reactive and proactive protocols, the **WG will develop two Standards track routing protocol specifications**:
  - **Reactive MANET Protocol** (RMP)
  - **Proactive MANET Protocol** (PMP)

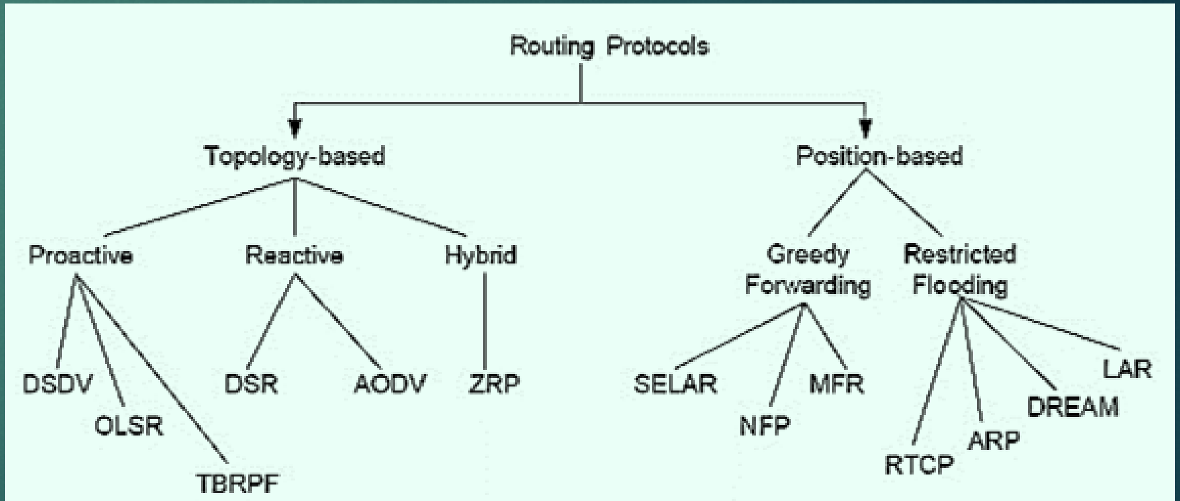
MANET Research Topics

- Routing
  - *Better metrics, higher throughput*
- Transport Layer
  - *TCP performance: throughput, fairness, etc.*
- MAC Layer
  - *MAC performance, channel utilization*
- Security
  - Reliable routing against malicious nodes
- Power Management
  - Power saving and power control

MANET Protocol Zoo

- Topology based routing
  - Proactive approach, e.g., DSDV.
  - Reactive approach, e.g., **DSR**, **AODV**, TORA.
  - Hybrid approach, e.g., Cluster, **ZRP**.

- Position based routing
  - Location Services:
    - DREAM, Quorum-based, GLS, Home zone etc.
  - Forwarding Strategy:
    - Greedy, GPSR, RDF, Hierarchical, etc.



MANET Routing Properties

- **Qualitive Properties**
  - Distributed operation
  - Loop Freedom
  - Demand Based Operation
  - Security
  - Sleep period operation
  - Unidirectional link support
- **Quantitative Properties**
  - End-to-End data throughput
  - Delays
  - Route Acquisition time
  - Out of order delivery (percentage)
  - Efficiency

MANET Routing Properties

- No distinction between “routers” and “end nodes”: **all nodes participate in routing**
- No external network setup: **self-configuring**
- **Efficient** when network topology is dynamic (frequent network changes – links break, nodes come and go)
- **Self Starting**
- **Adapt to network conditions**

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** are used
  - **route stability** despite mobility
  - **energy consumption**
  - **host position**
- ***Dynamic Solutions*** *much more difficult to be deployed*

Routing Protocols

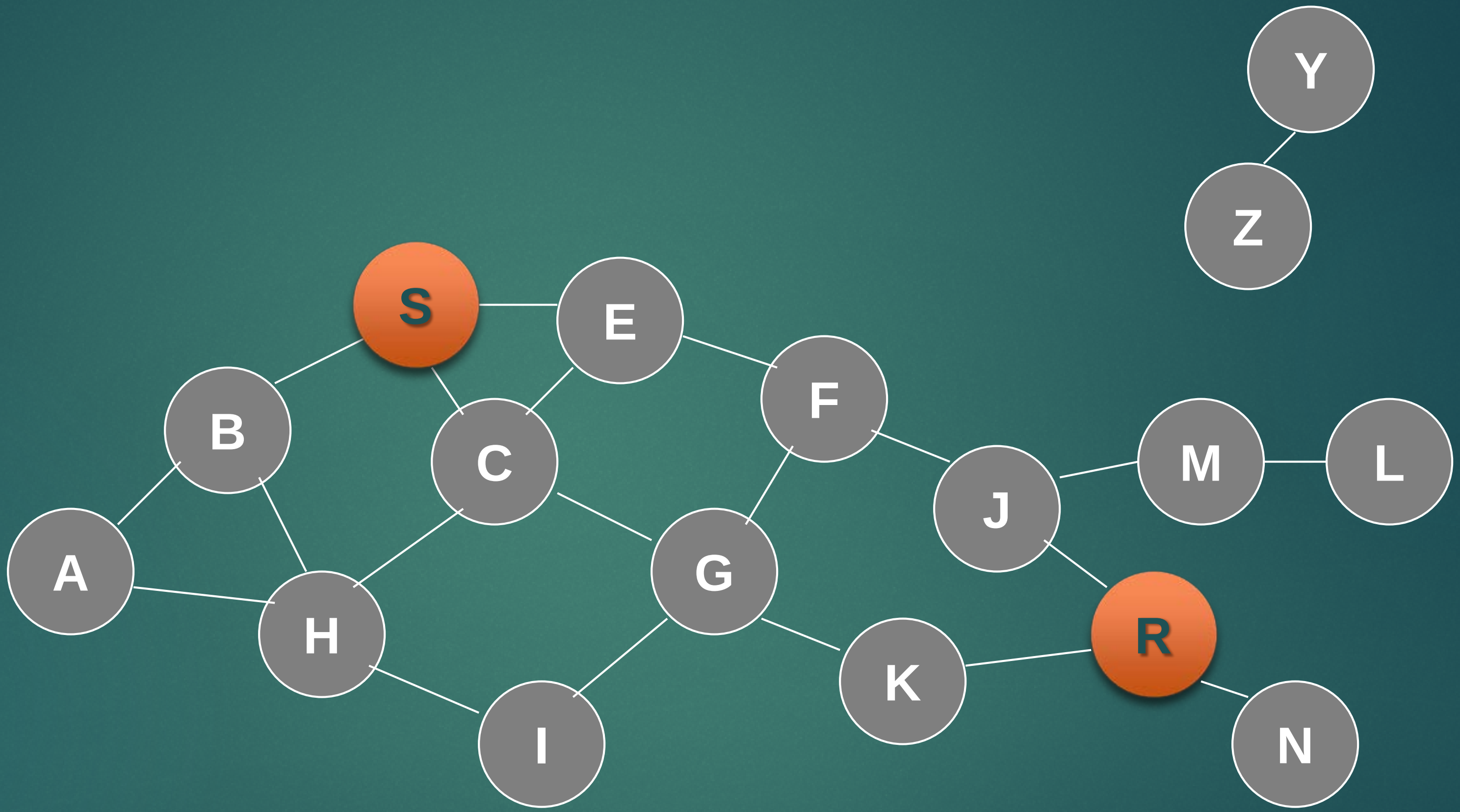
- **No Routing:** Plain Flooding (PF)
- **Proactive protocols**: determine routes independent of traffic pattern, traditional link-state and distance-vector routing protocols are proactive.
  - Destination Sequence Distance Vector (DSDV), Link State Routing
- **Reactive protocols**: discover routes and maintain them only if needed.
  - Dynamic Source Routing (DSR)
  - Ad-hoc On-Demand Distance Vector Routing (AODV)
- **Hybrid protocols:** Zone Based Routing (ZBR)

Trade-Offs

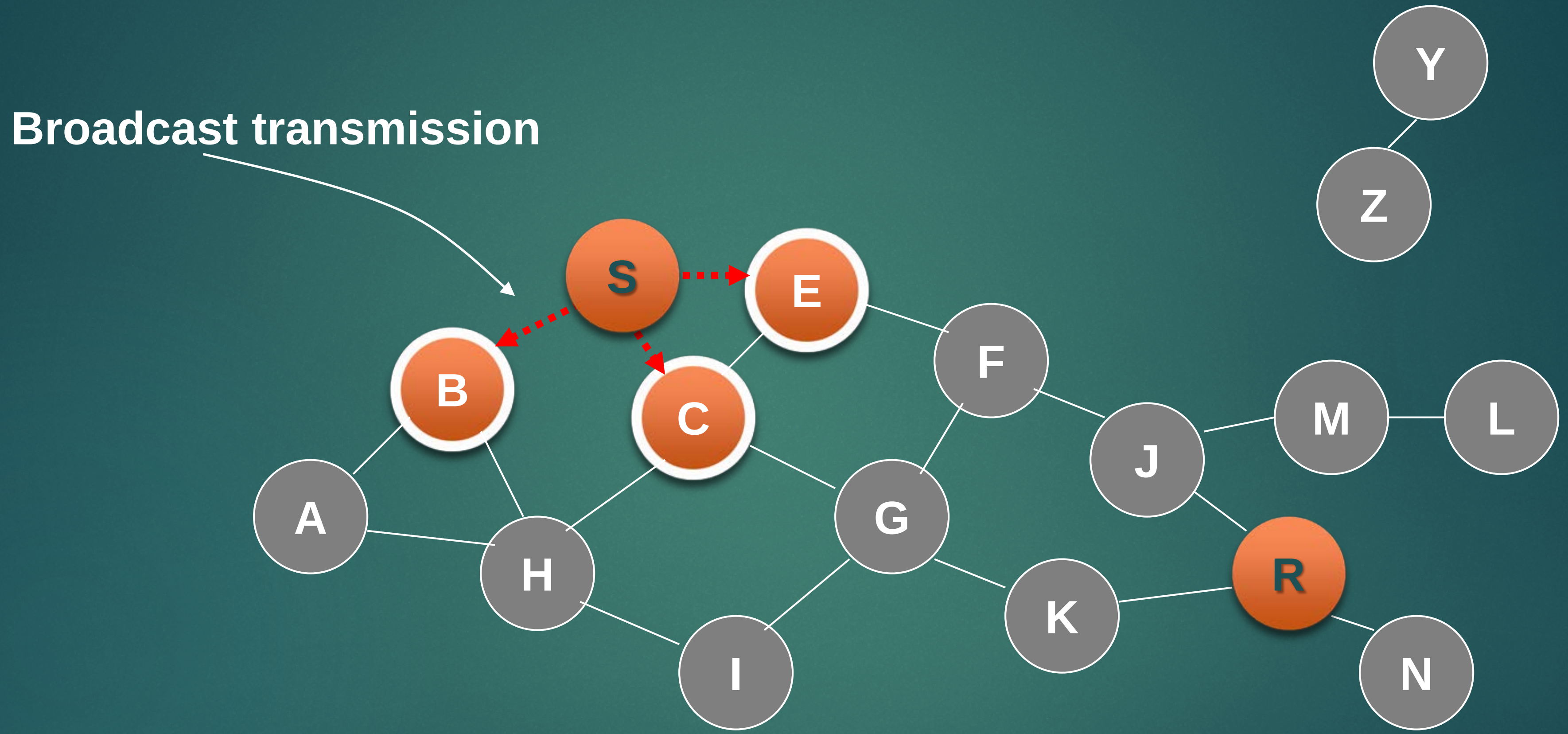
- **Latency of route discovery**
  - Proactive protocols may have lower latency since routes are maintained at all times
  - Reactive protocols may have higher latency because a route from X to Y will be found only when X attempts to send to Y
- **Overhead of route discovery/maintenance**
  - Reactive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

Routing Protocols Description

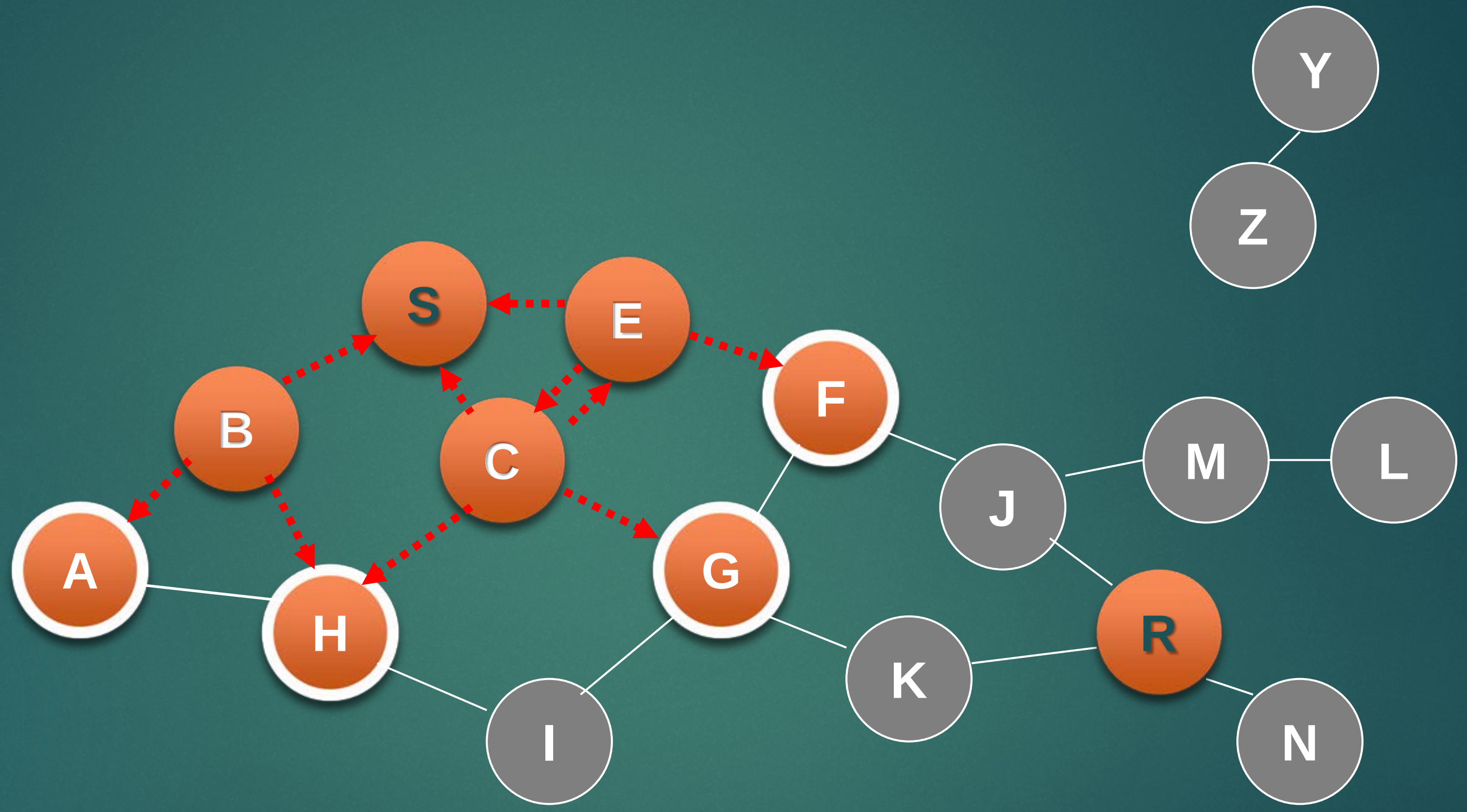
Flooding for Data Delivery



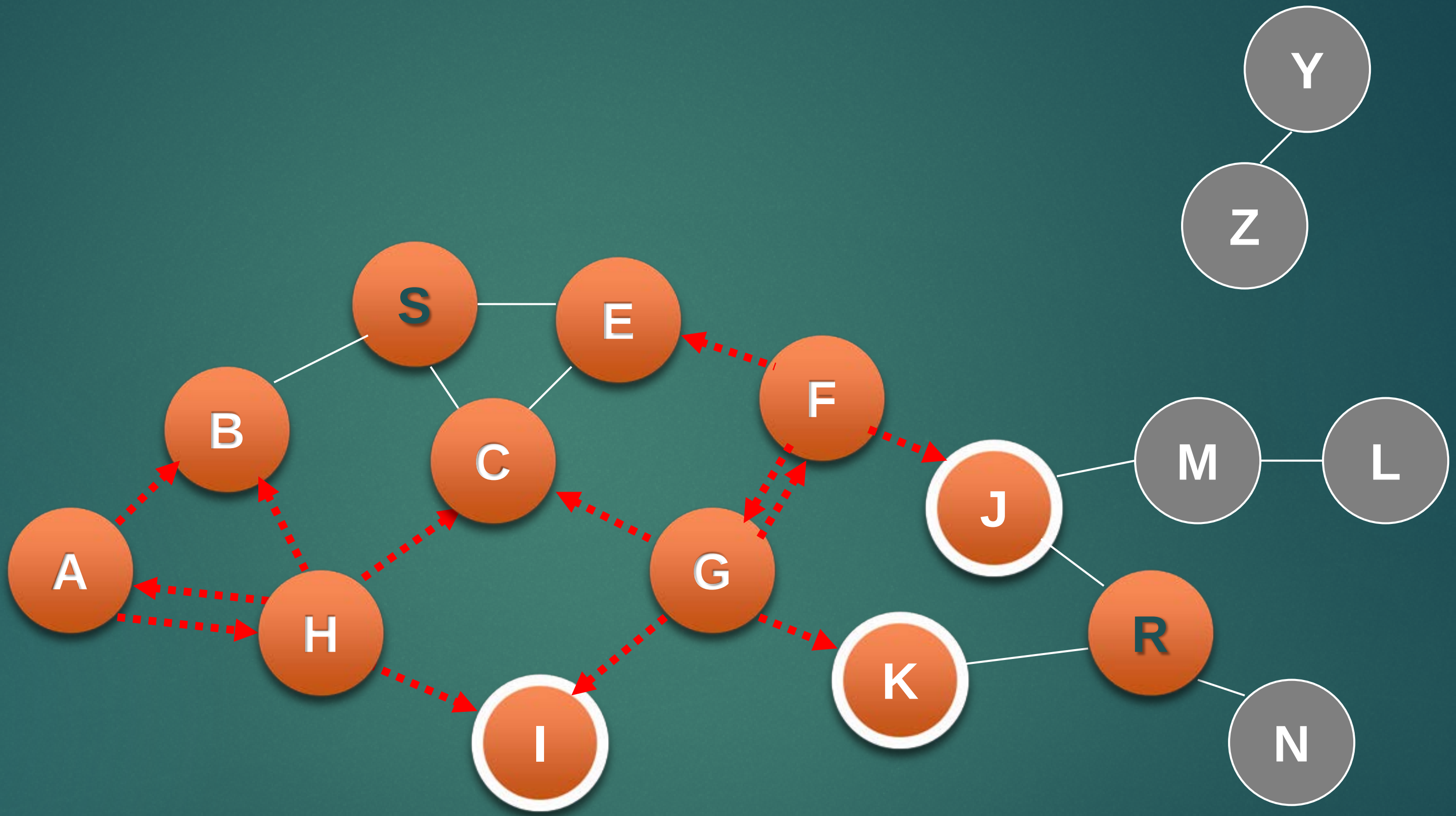
Flooding for Data Delivery



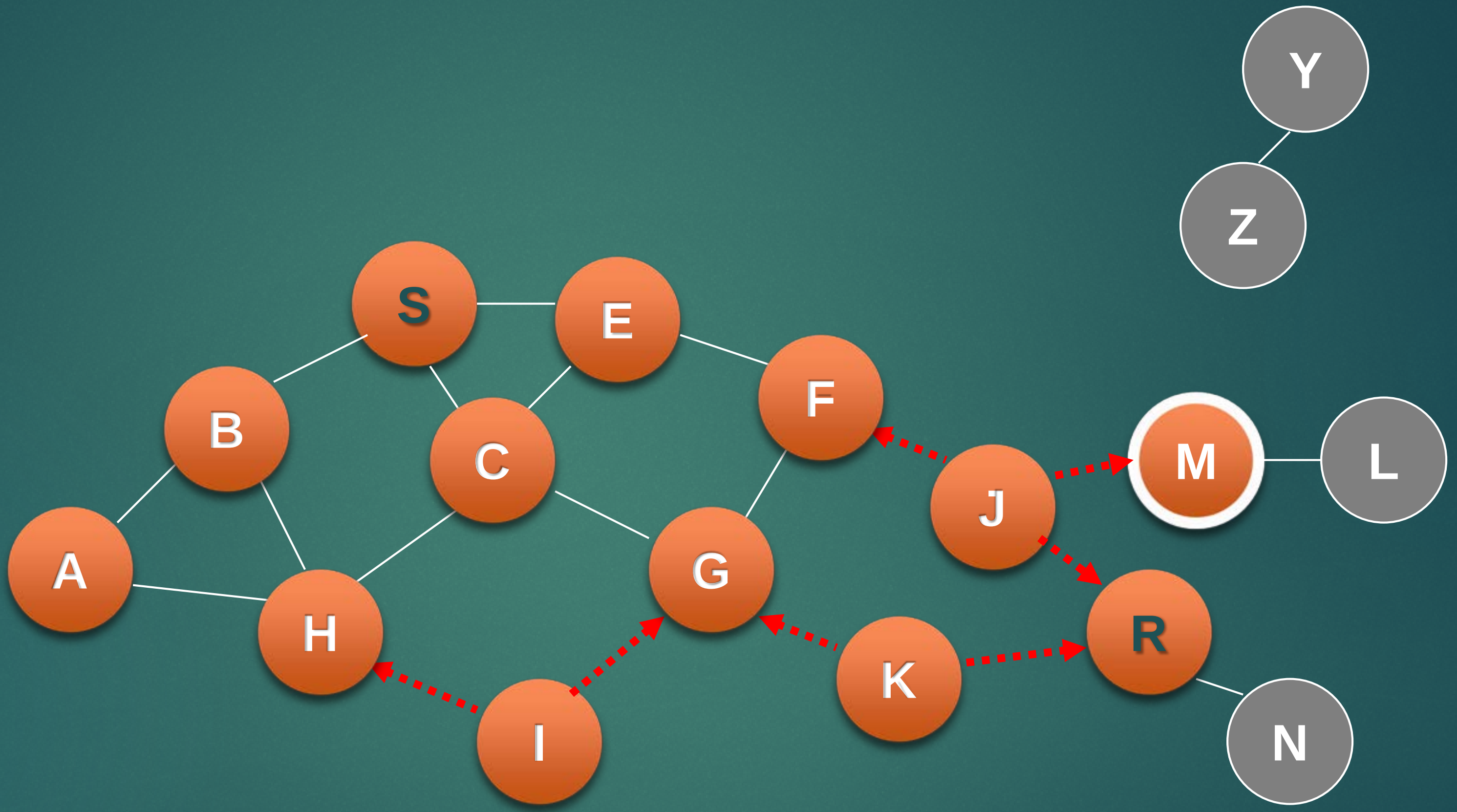
Flooding for Data Delivery



Flooding for Data Delivery

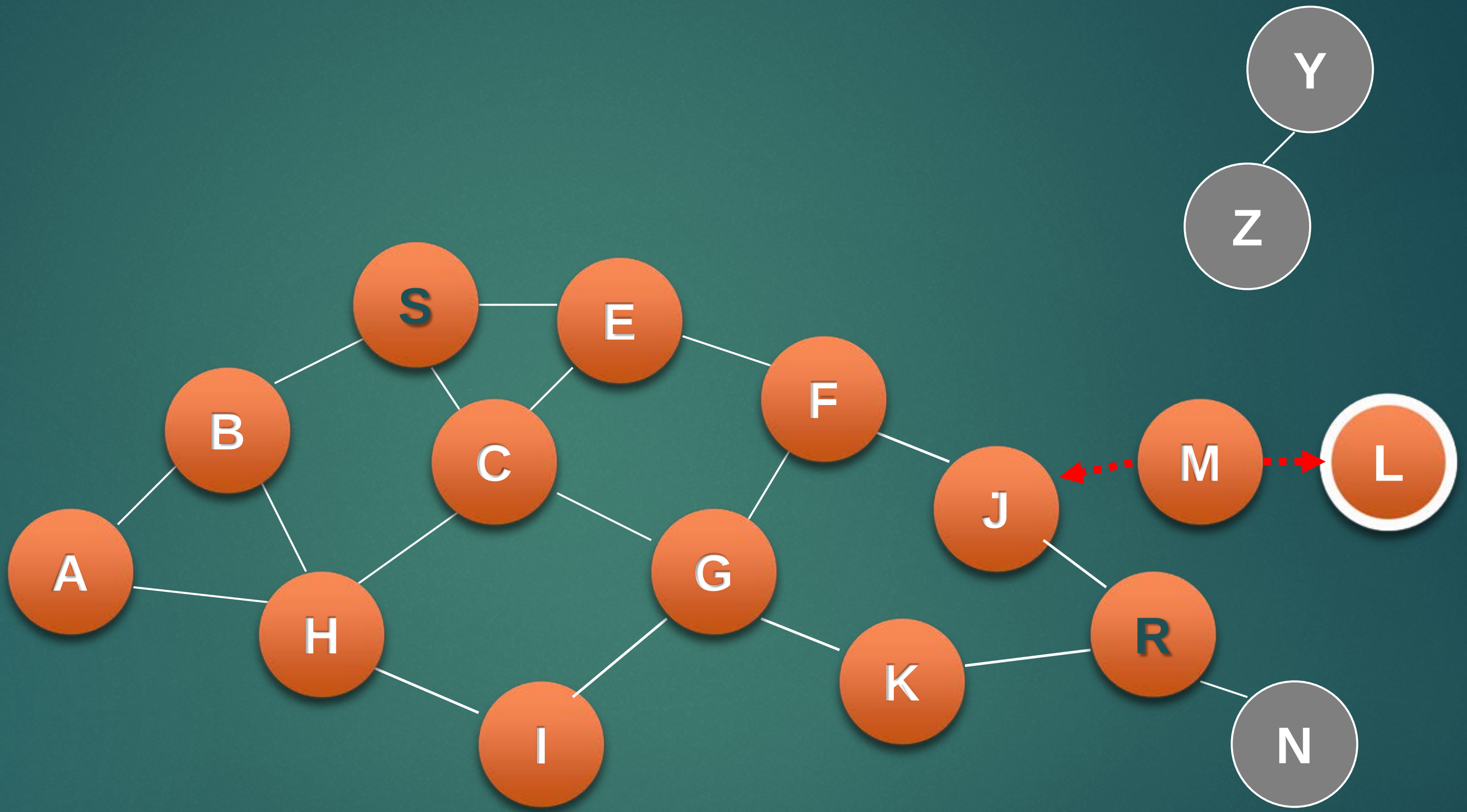


Flooding for Data Delivery

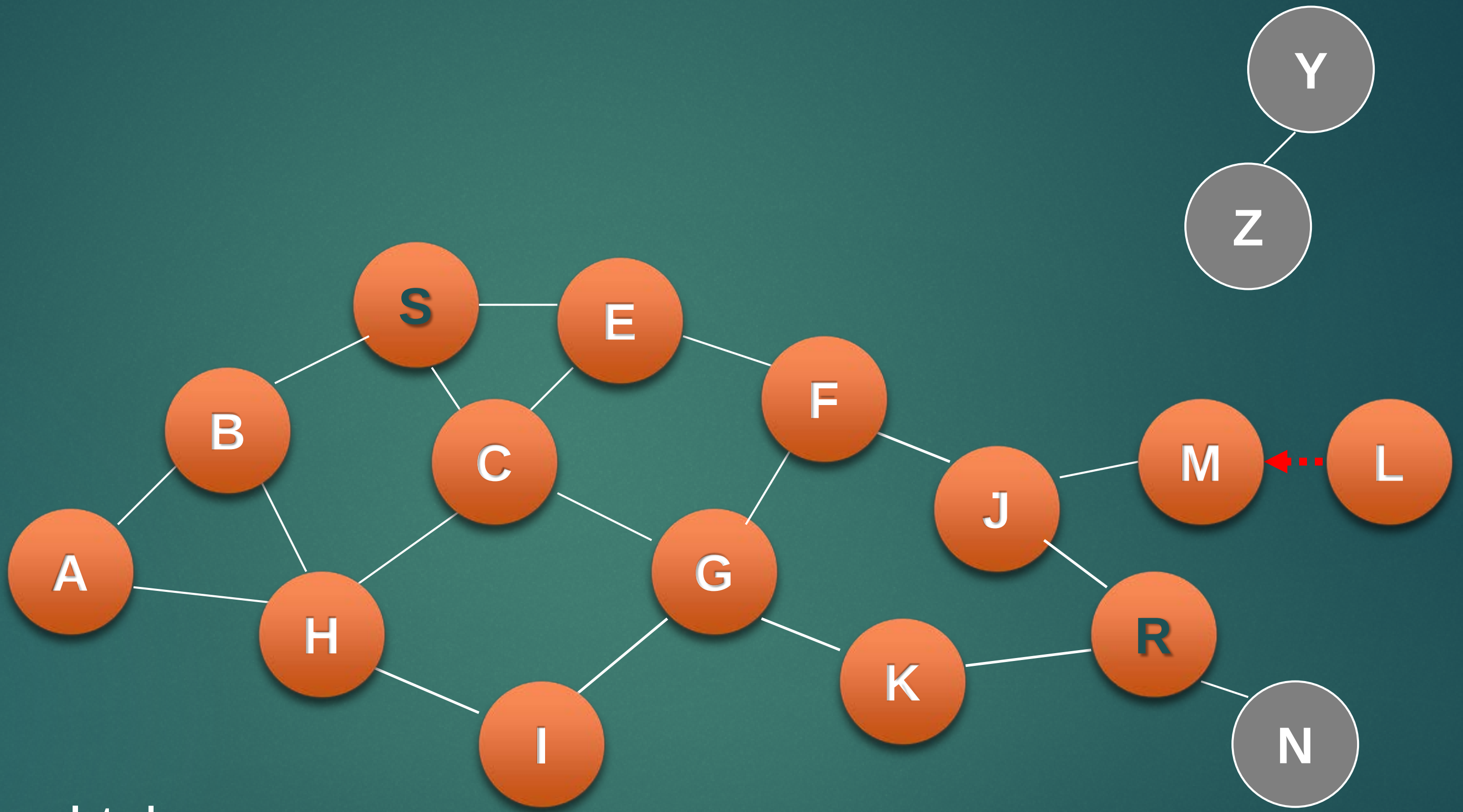


- Nodes J and K both broadcast packet P to node R
- Since nodes J and K are hidden from each other, their transmissions may collide
  => Packet P may not be delivered to node R at all, despite the use of flooding

Flooding for Data Delivery



Flooding for Data Delivery



- Flooding completed
- Nodes unreachable from S do not receive packet
- 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
- Efficient than other protocols when rate of information transmission is low enough
  - overhead of explicit route discovery/maintenance incurred is higher
  - small data packets
  - infrequent transfers
  - many topology changes occur between consecutive packet transmissions
- Potentially higher reliability of data delivery

Flooding for Data Delivery: Disadvantages

- High overhead
  - Data packets may be delivered to too many nodes who do not need to receive them
- Lower reliability of data delivery
  - If Broadcasting is unreliable (ie. 802.11 MAC)

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)

Dynamic Source Routing (DSR)

- Source routing: entire path to destination supplied by source in packet header
  - Utilizes extension header following standard IP header to carry protocol information (route to destination, etc.)

DSR Protocol Activities

- **Route discovery**
  - Undertaken when source needs a route to a destination
- **Route maintenance**
  - Detect network topology changes
  - Used when link breaks, rendering specified path unusable
- **Routing (easy!)**

Details

- Intermediate nodes cache overheard routes
  - “Eavesdrop” on routes contained in headers
  - Reduces need for route discovery
- Intermediate node may return Route Reply to source if it already has a path stored
  - Encourages “expanding ring” search for route

Details (cont.)

- Destination may need to discover route to source to deliver Route Reply
  - piggyback Route Reply onto new Route Request to prevent “infinite loop”
- Route Request *duplicate rejection*:
  - Source includes identification number in Route Request
  - Partial path inspected for “loop”

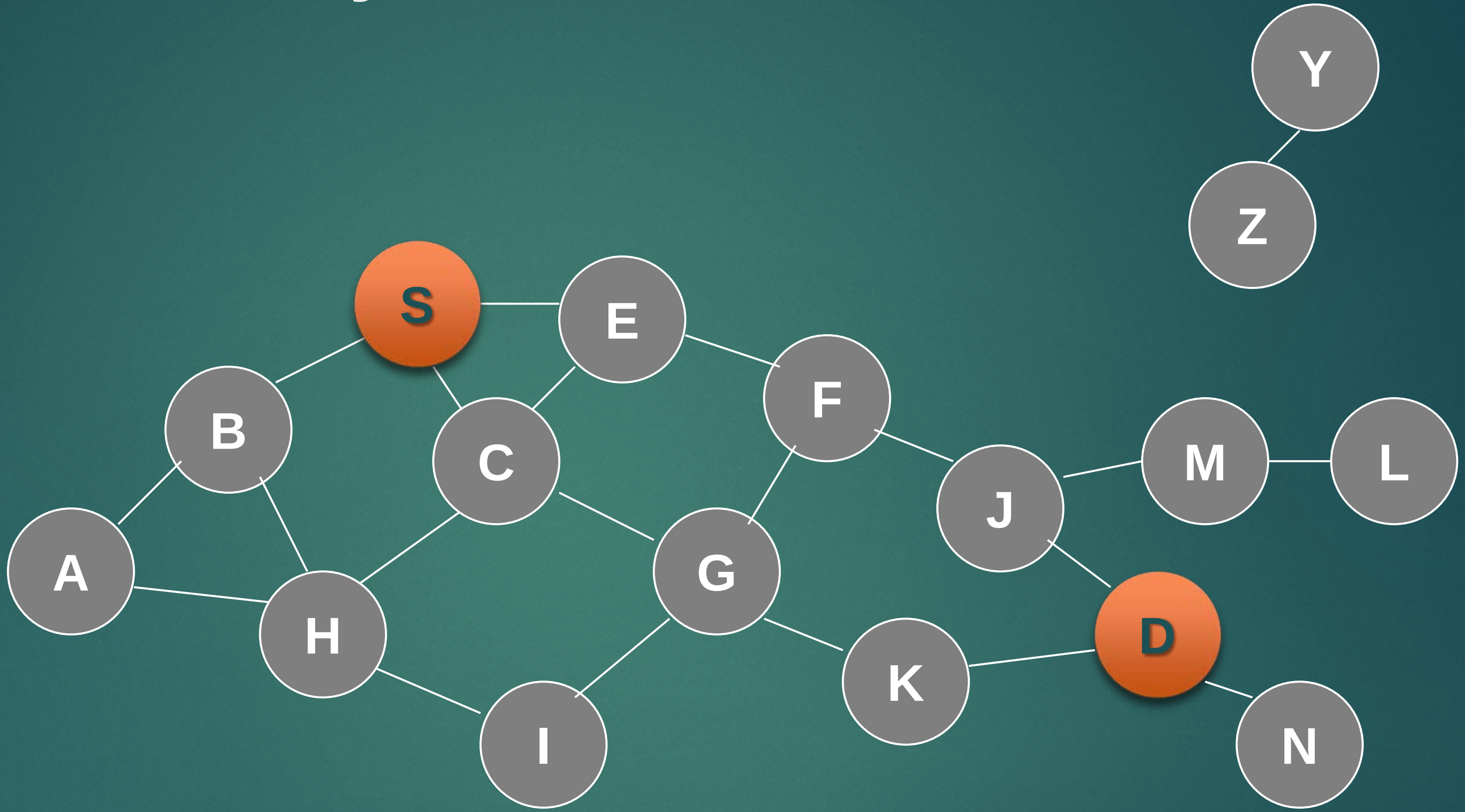
Route Maintenance

- Used when link breakage occurs
- Link breakage may be detected using link-layer ACKs, "passive ACKs", DSR ACK request
- Route Error message sent to source of message being forwarded when break detected
- Intermediate nodes "eavesdrop", adjust cached routes
- Source deletes route; tries another if one cached, or issues new Route Request
  - Piggybacks Route Error on new Route Request to clear intermediate nodes' route caches, prevent return of invalid route

Issues

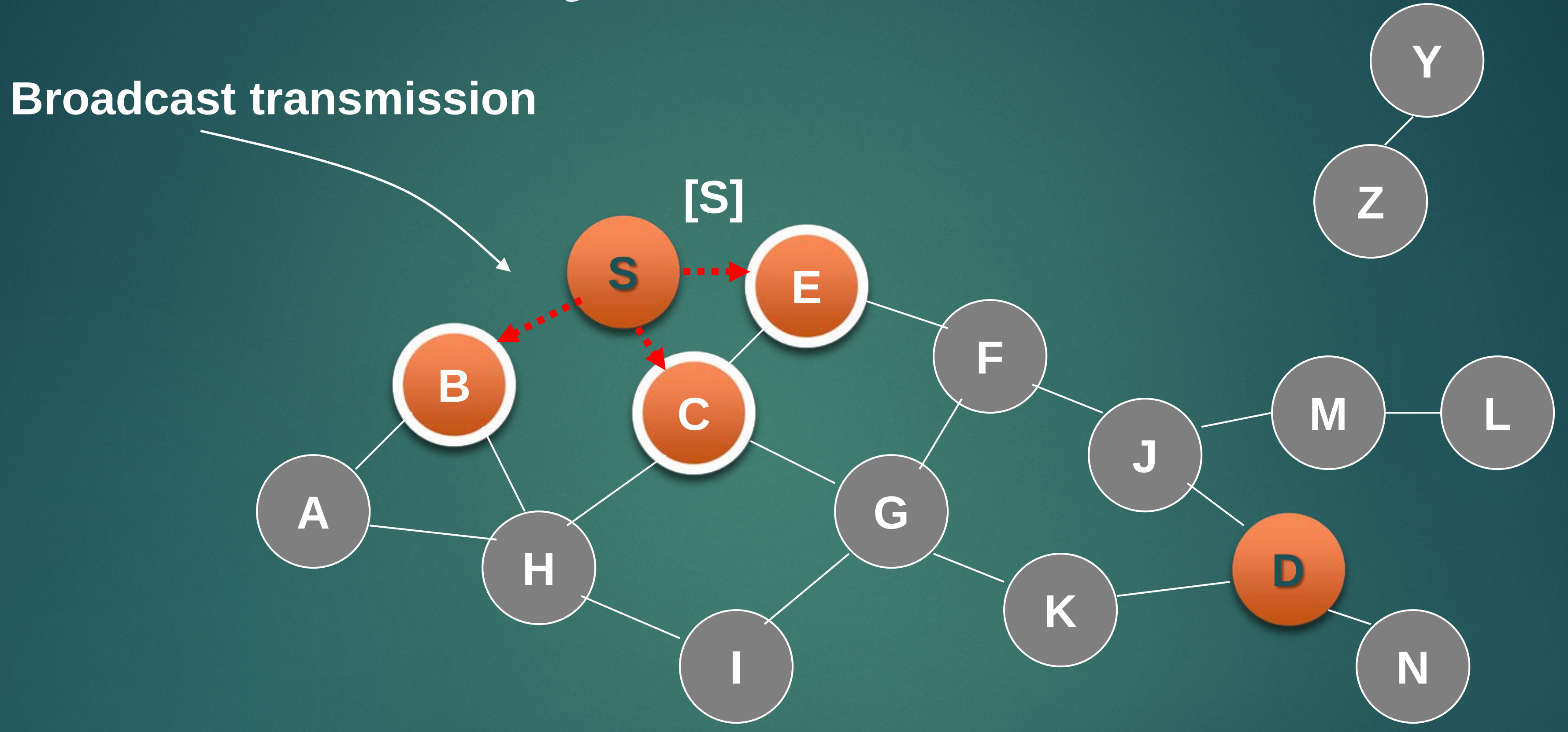
- Scalability
  - Discovery messages broadcast throughout network
- Broadcast / Multicast
  - Use Route Request packets with data included
    - Duplicate rejection mechanisms prevent “storms”
  - Multicast treated as broadcast; no multicast-tree operation defined
    - Scalability issues

Route Discovery in DSR



Represents a node that has received RREQ for D from S

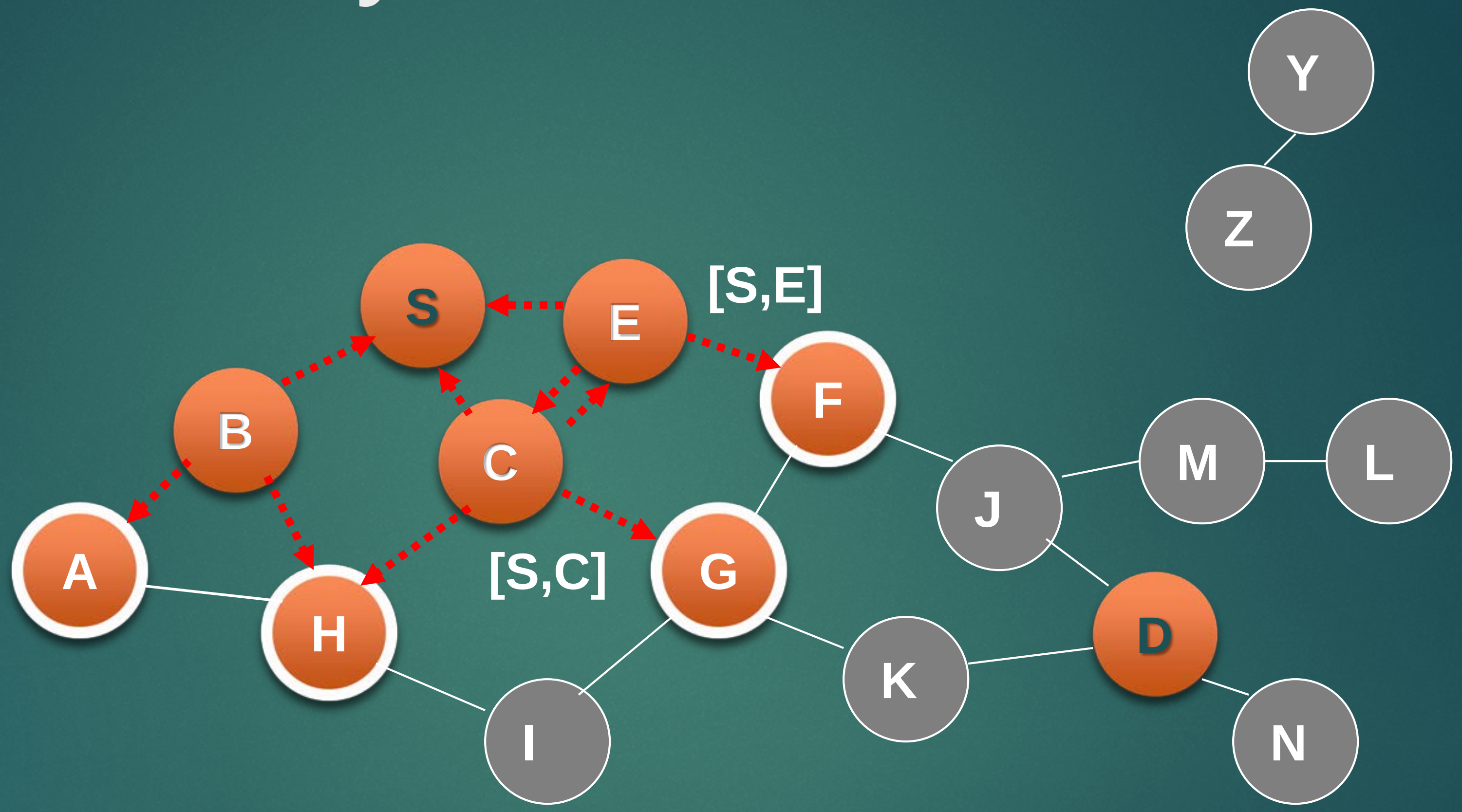
Route Discovery in DSR



Represents transmission of RREQ

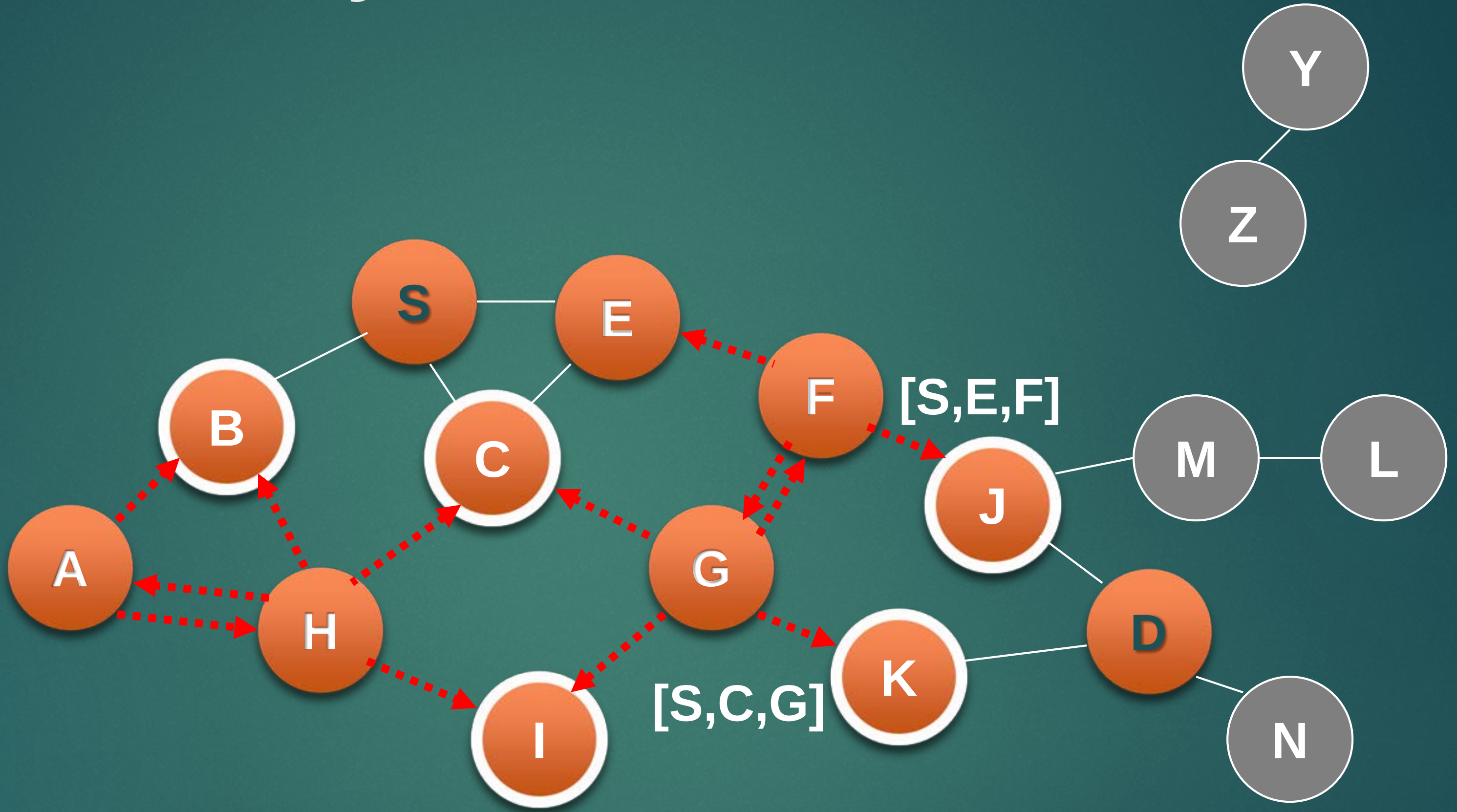
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



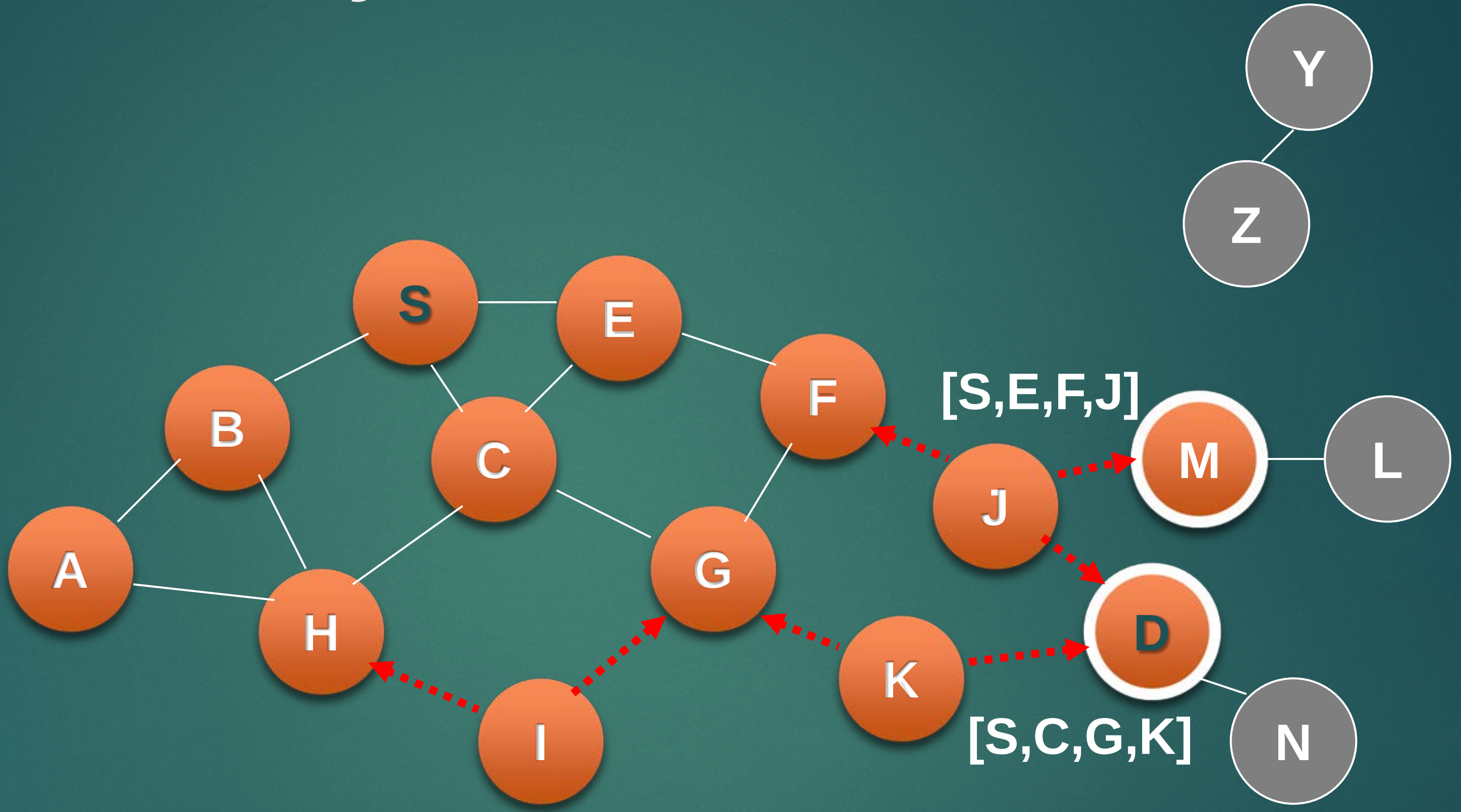
- Node H receives packet RREQ from two neighbors: potential for collision

Route Discovery in DSR



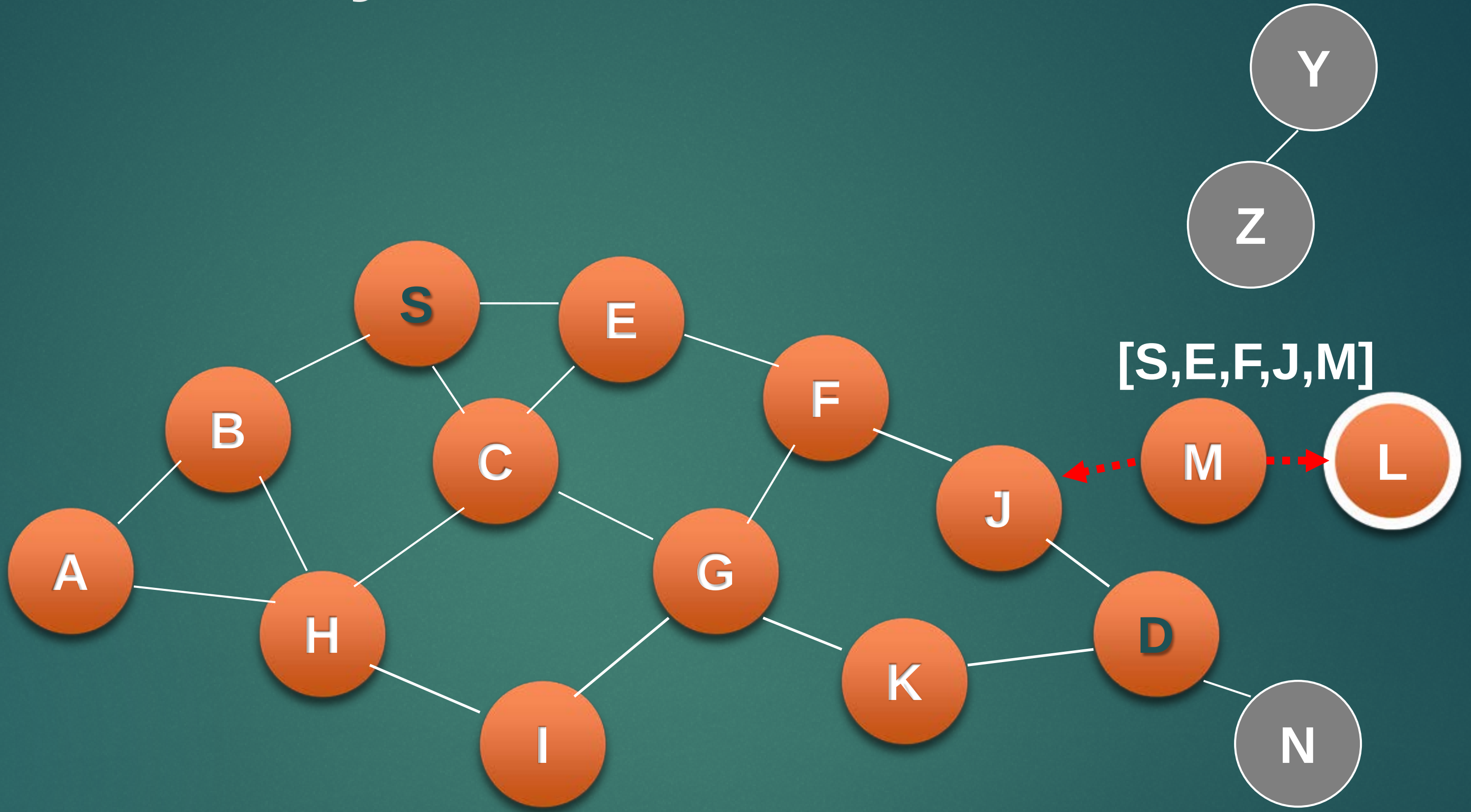
• Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

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 <u>intended target</u> of the route discovery

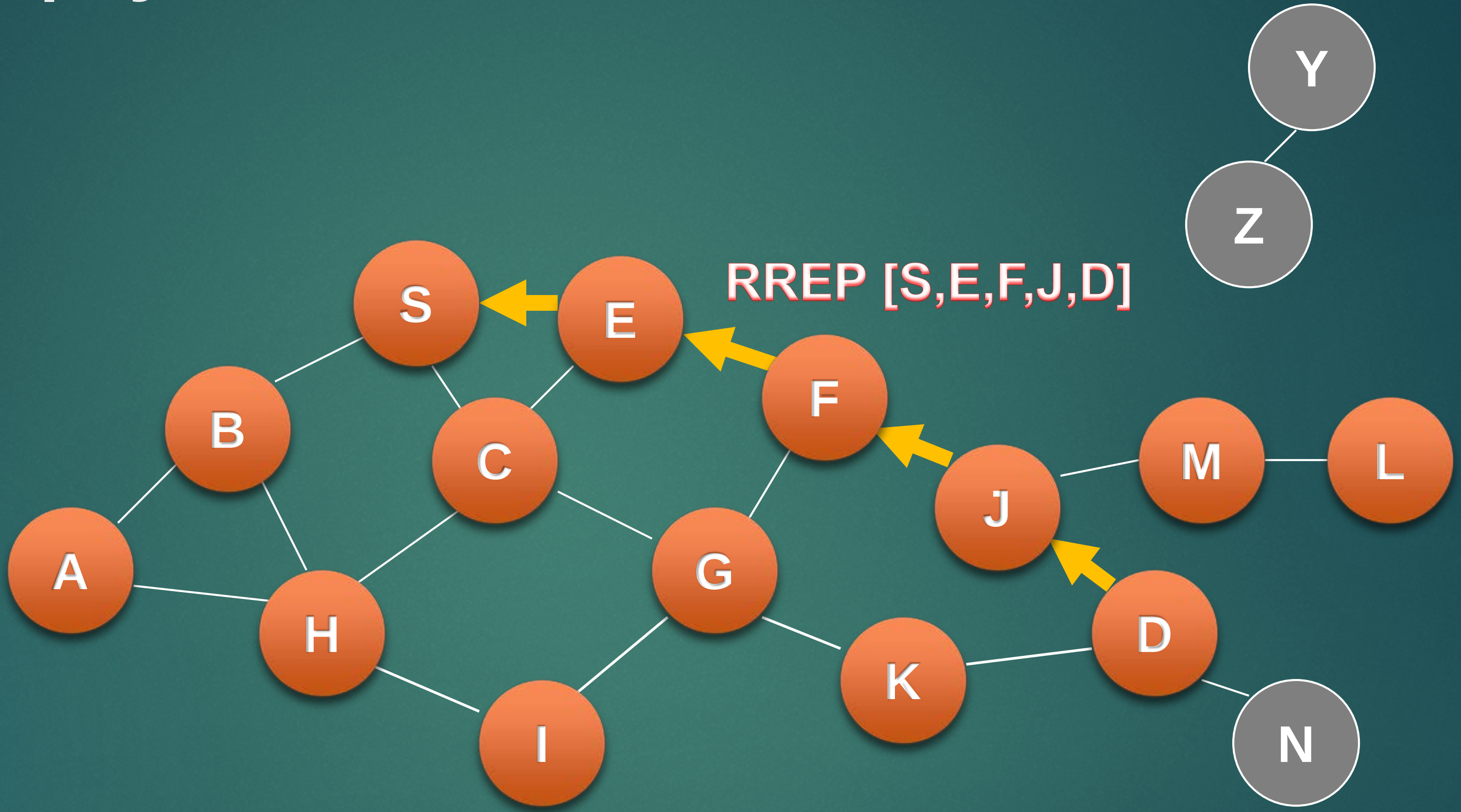
Route Reply in DSR

- 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)

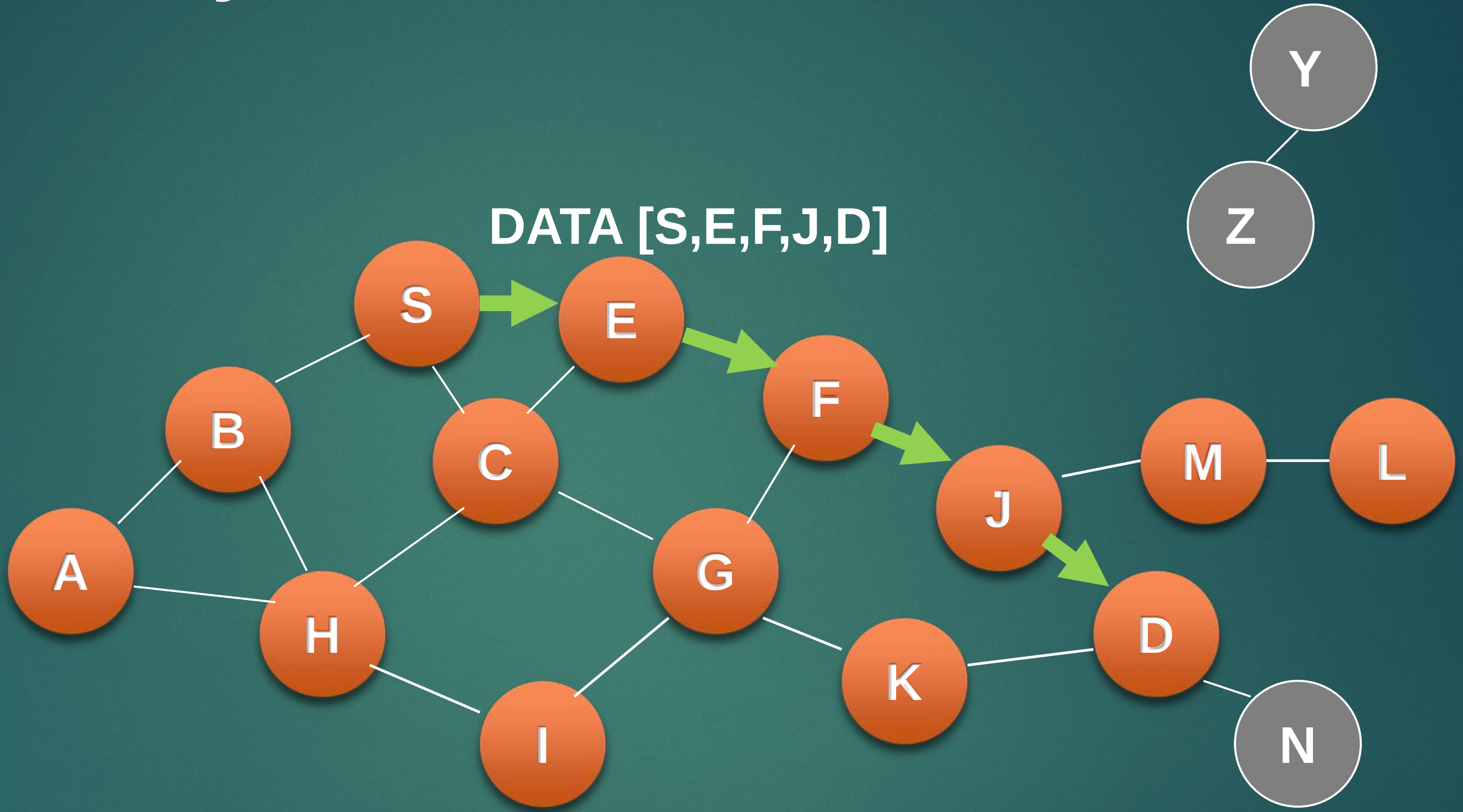
- Node S on receiving RREP, caches the route included in the RREP
- When node S sends a data packet to D, the entire route is included in the packet header
  - hence the name **source routing**
- Intermediate nodes use the source route included in a packet to determine to whom a packet should be forwarded

Route Reply in DSR



• Node D sends back a Reply (RREP) to S with the path
NOTE: If node D does not know a rout back to S it might be necessary to start it’s own rout discovery to S.

Data Delivery in DSR



Packet header size grows with route length

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
- 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

DSR: Disadvantages

- An intermediate node may send Route Reply using a stale cached route, thus polluting other caches
  - Solution – Cached Route invalidation (root lifetime estimation)
- Increased contention, too many route replies using their local cache node caches
  - Route Reply Storm problem
  - Solution – preventing a node from sending RREP if it hears another RREP with a shorter route

Ad-hoc On-demand Distance Vector Routing

- “Hop-by-hop” protocol: intermediate nodes use lookup table to determine next hop based on destination

- Utilizes only standard IP header

AODV Protocol Activities

- Route discovery
  - Undertaken whenever a node needs a “next hop” to forward a packet to a destination
- Route maintenance
  - Used when link breaks, rendering next hop unusable
- Routing (easy!)

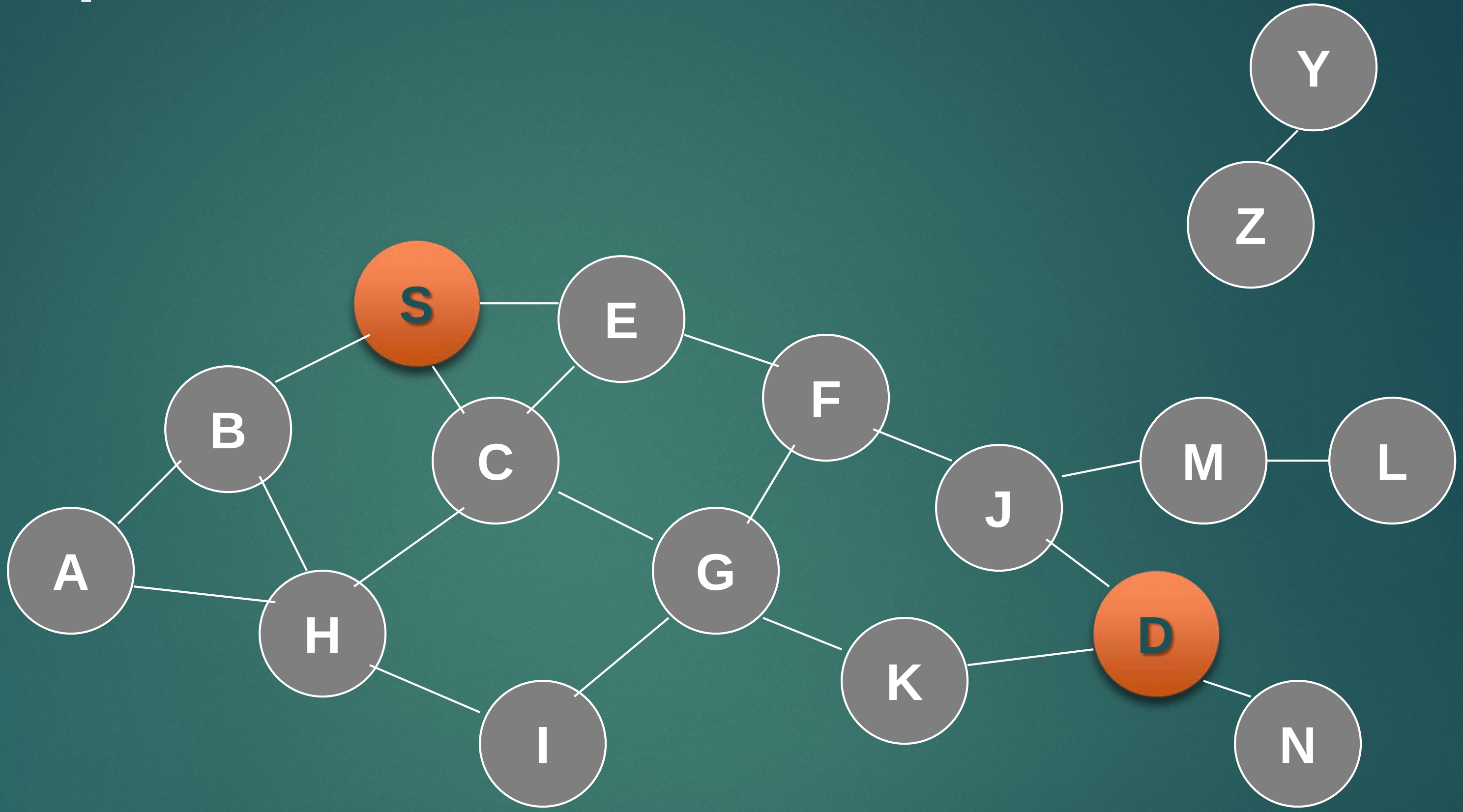
Route Discovery

- Route Request:
  - Source broadcasts Route Request (RREQ) message for specified destination
  - Intermediate node Forward message toward destination
- Route Reply
  - Destination unicasts Route Reply *msg* to source
  - Intermediate node create next-hop entry for destination and forward the reply
  - If source receives multiple replies, uses one with lowest hop count

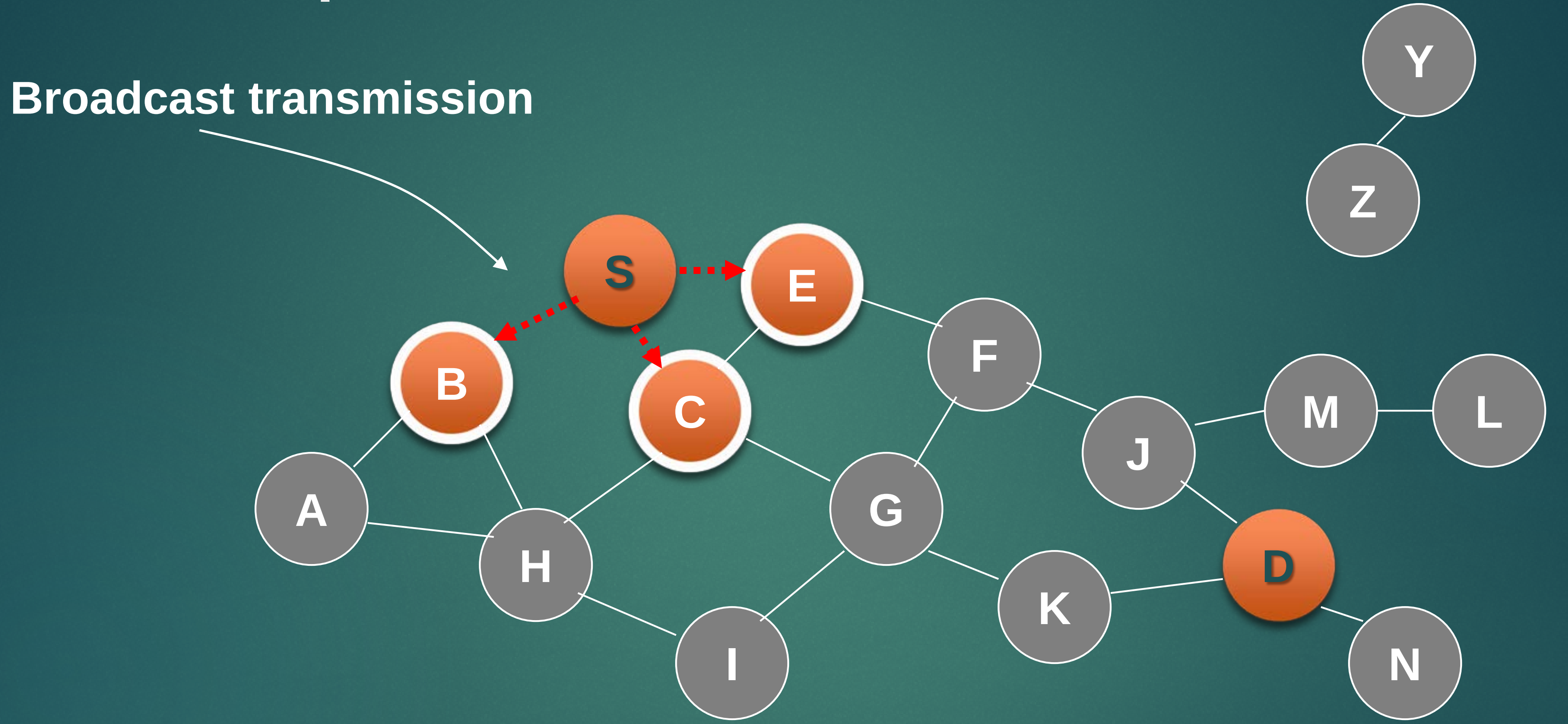
Route Maintenance

- Used when link breakage occurs
- Detecting node may attempt “local repair”
- Route Error (RERR) message generated
  - Contains list of unreachable destinations
  - Sent to “precursors”: neighbors who recently sent packet which was forwarded over broken link
    - Propagated recursively

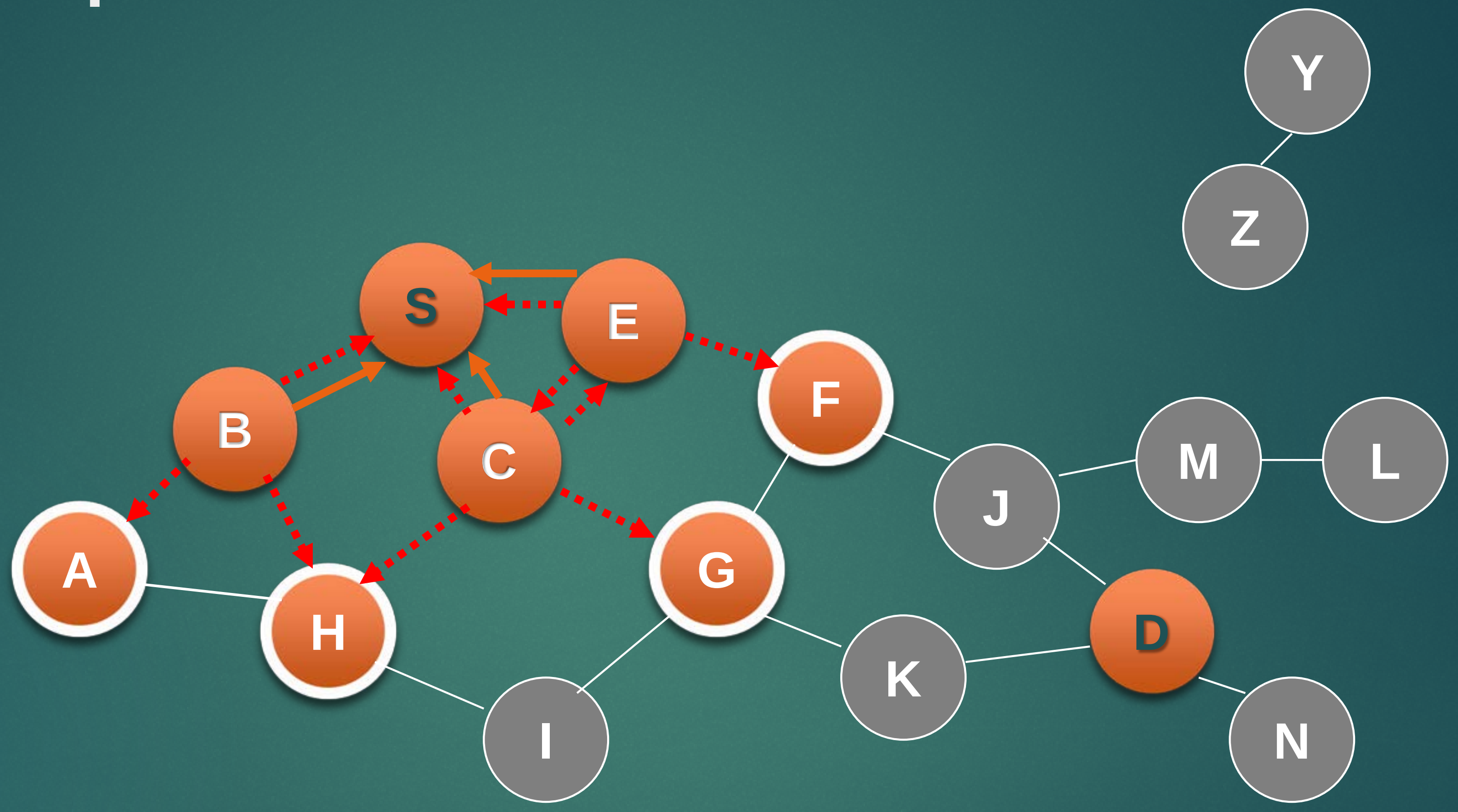
Route Requests in AODV



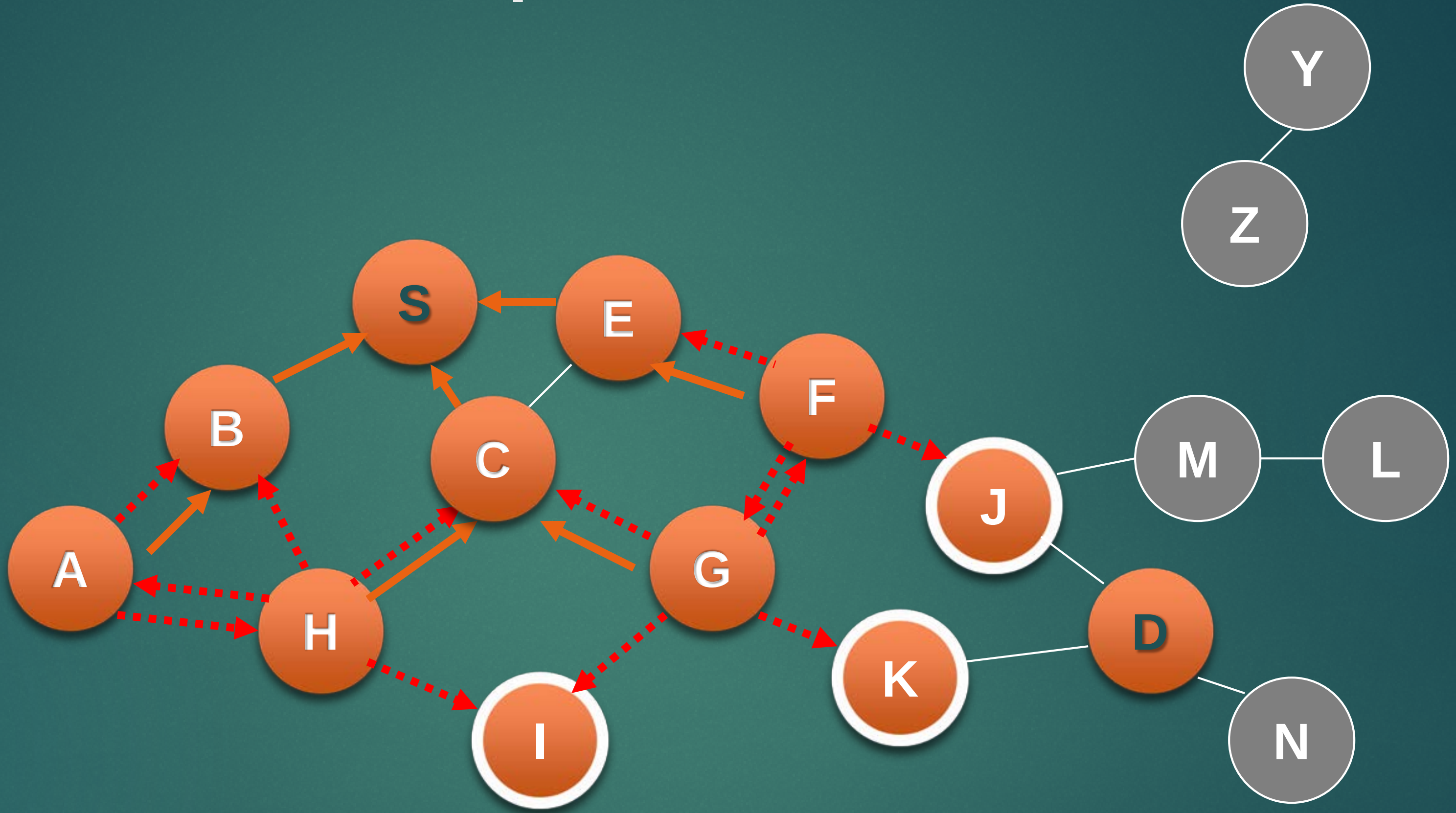
Route Requests in AODV



Route Requests in AODV

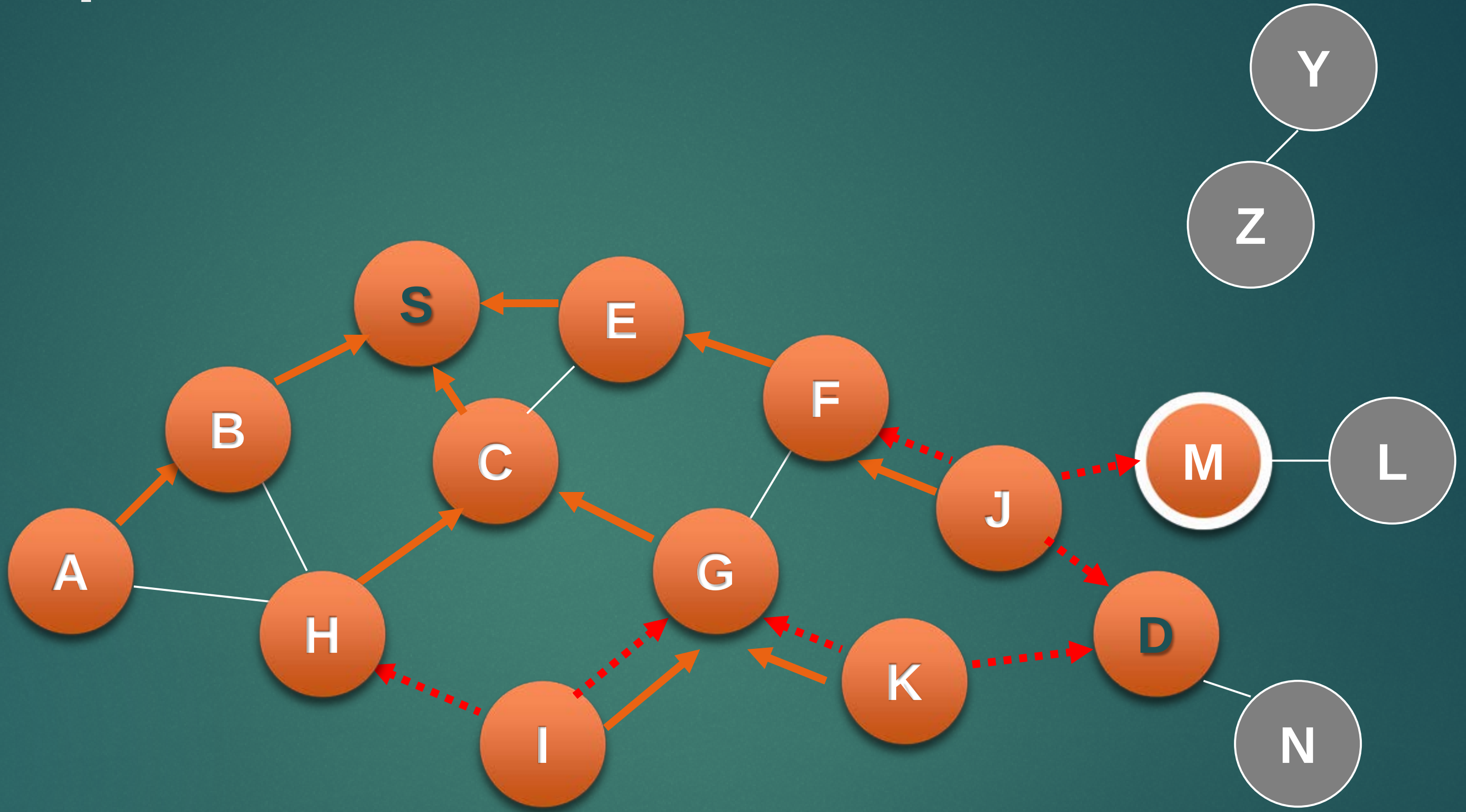


Reverse Path Setup in AODV

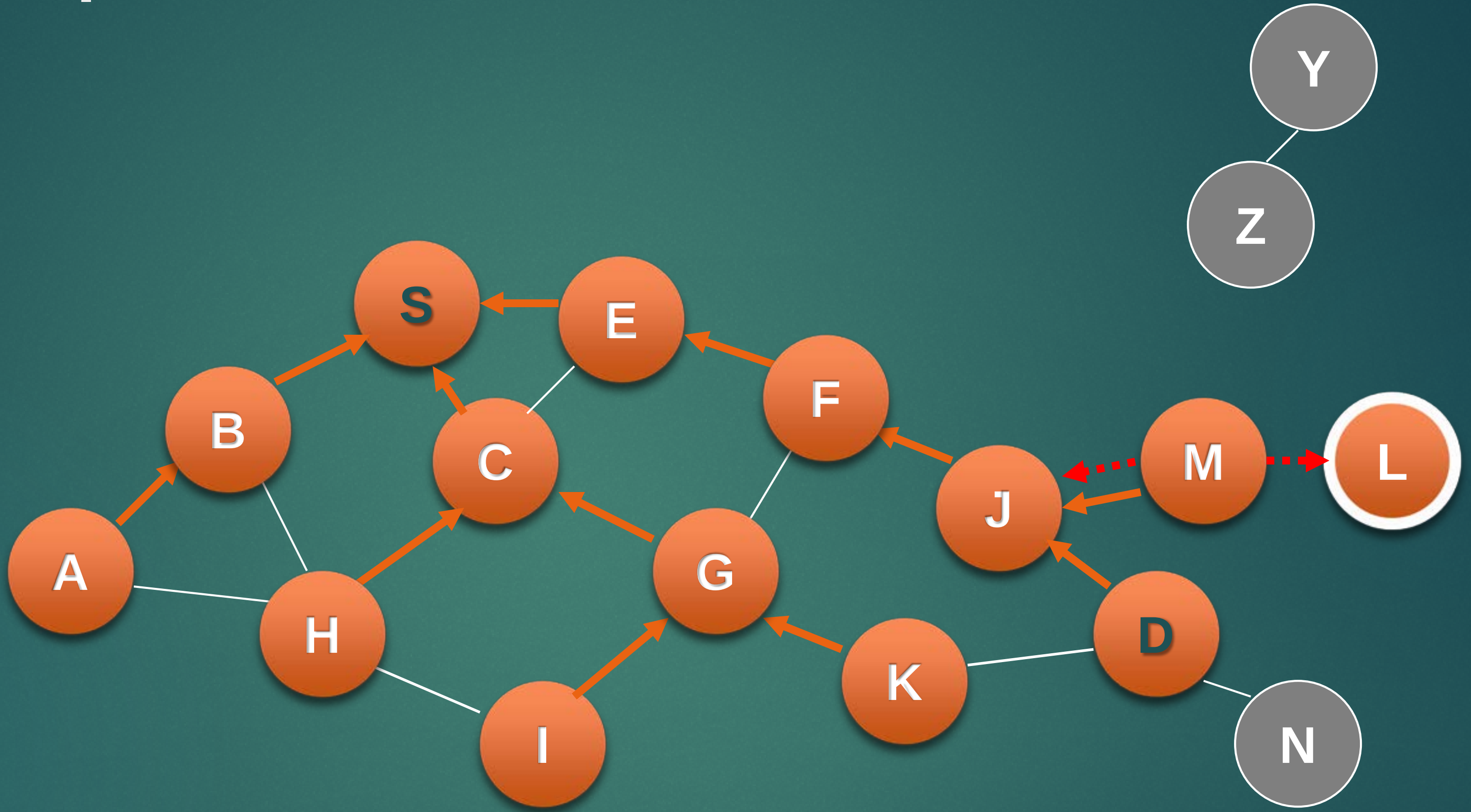


- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

Route Requests in AODV

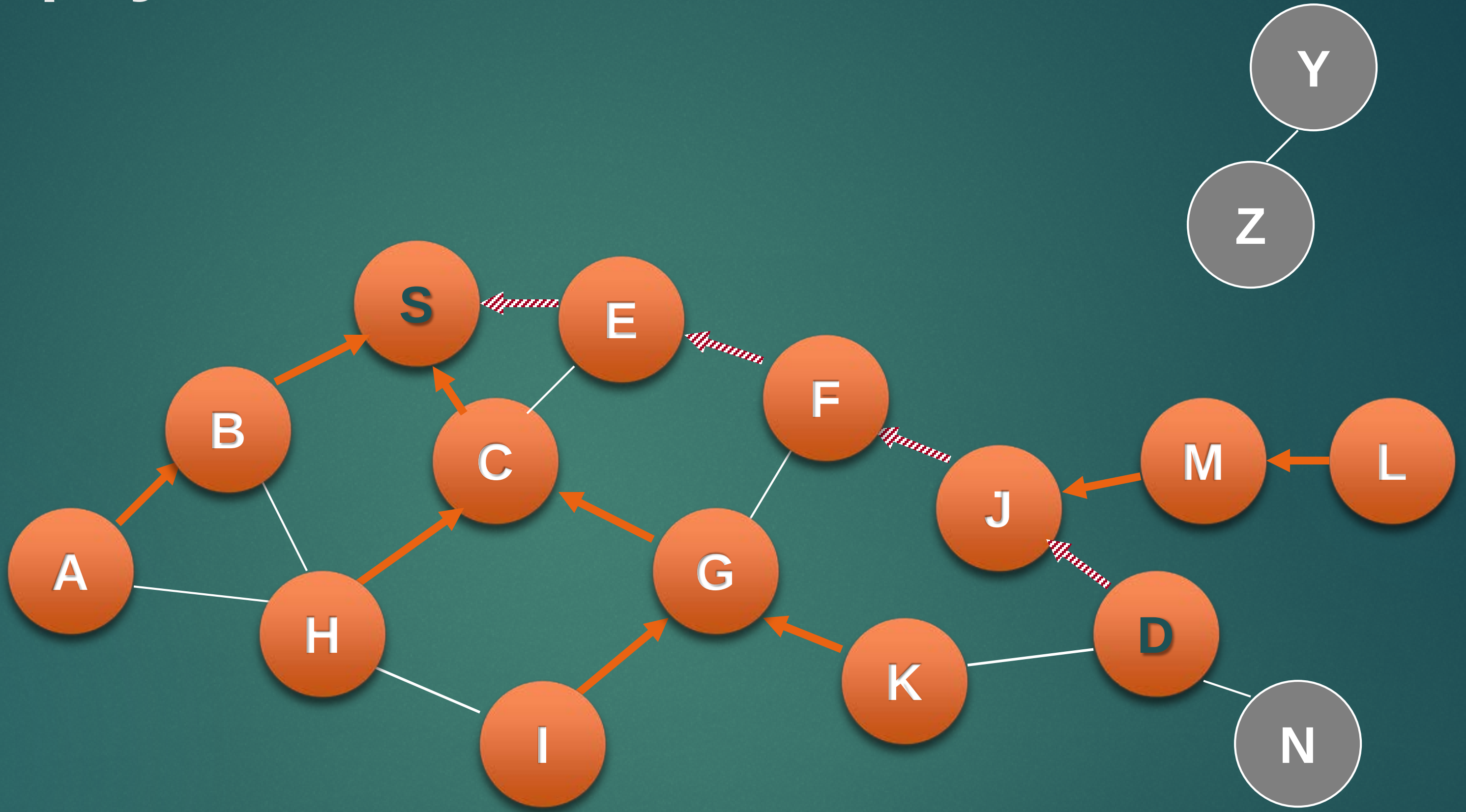


Route Requests in AODV



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

Route Reply in AODV

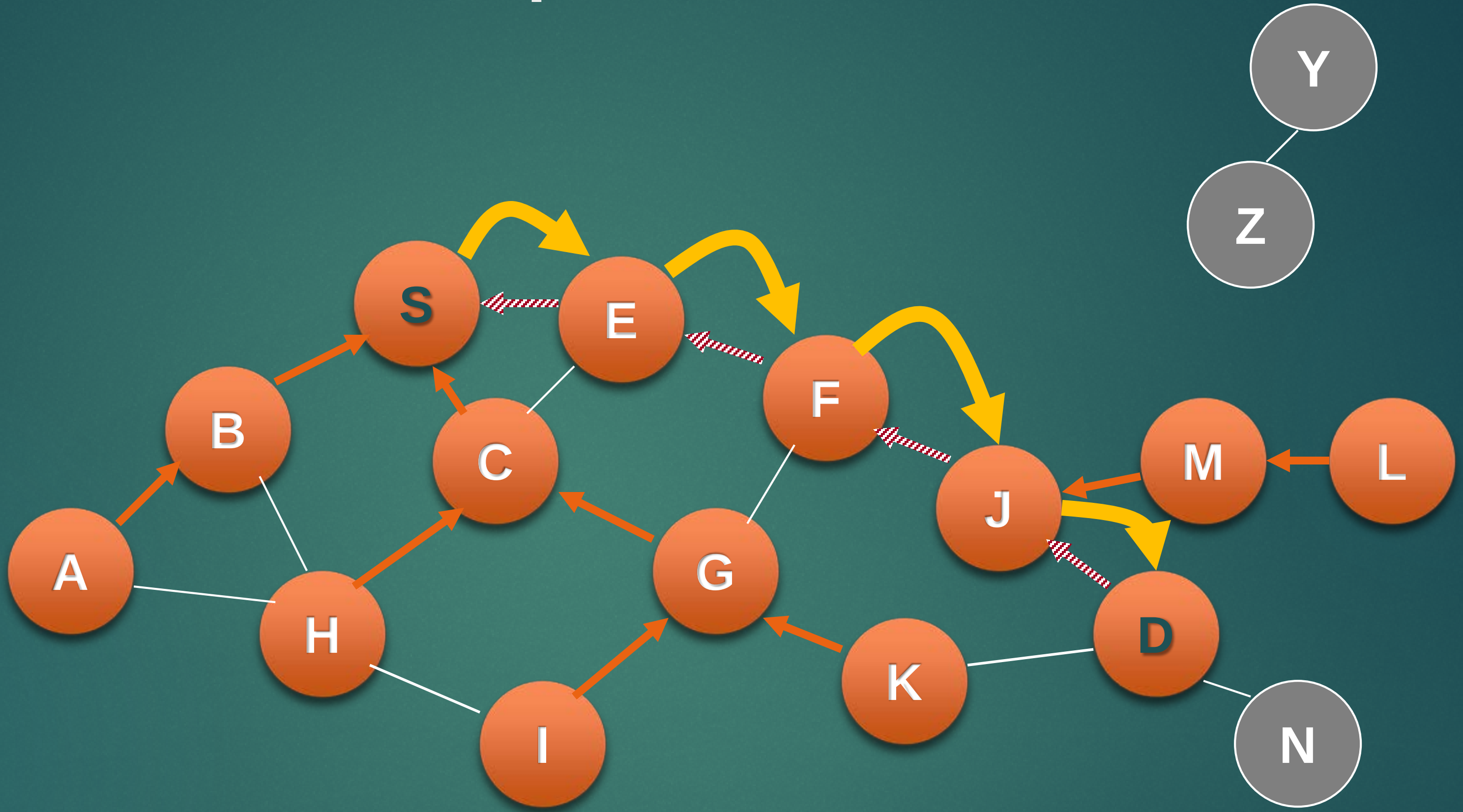


Represents links on path taken by RREP

Route Reply in AODV

- An *intermediate node (not the destination)* may also send a Route Reply (RREP) provided that it knows a more recent path than the one previously known to sender S
- To determine whether the path known to an intermediate node is more recent, ***destination sequence numbers*** are used
- The likelihood that an intermediate node will send a Route Reply when using AODV is not as high as DSR

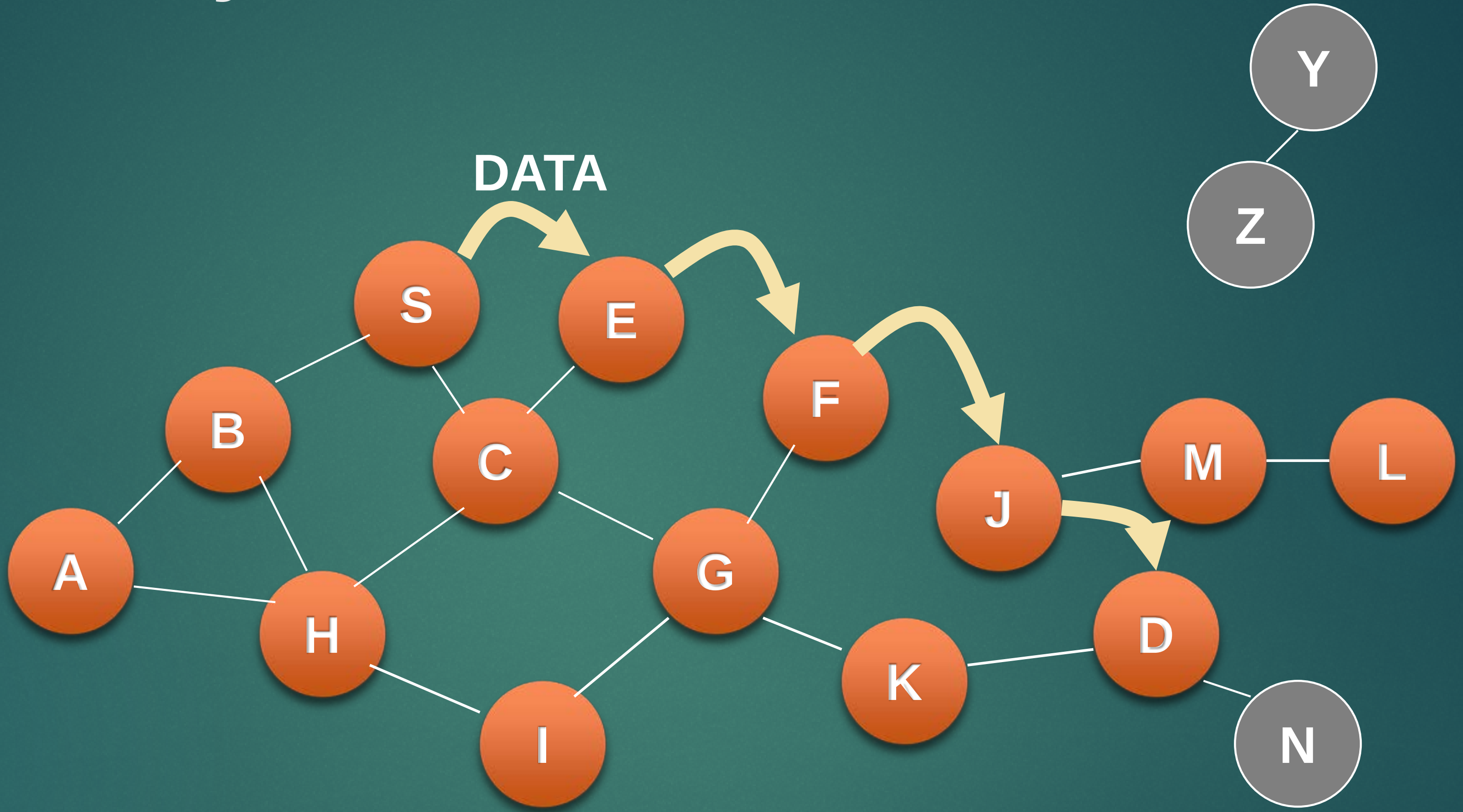
Forward Path Setup in AODV



Forward links are setup when RREP travels along the reverse path

Represents a link on the forward path

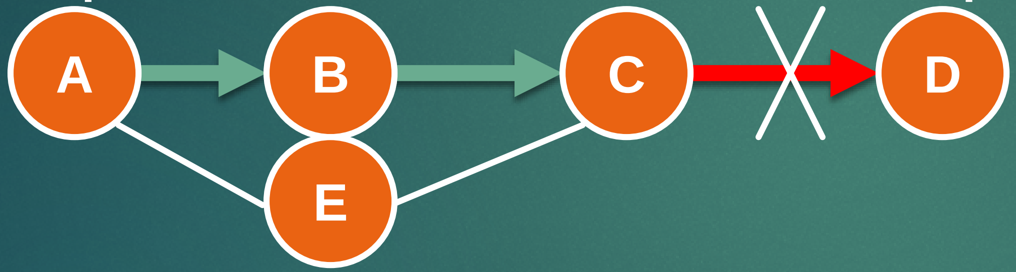
Data Delivery in AODV



- Routing table entries used to forward data packet.
- **Route is <u>not</u> included in packet header.**

Why Sequence Numbers in AODV

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



  - 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)

Summary: AODV

- 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
  - DSR may maintain several routes for a single destination
- Unused routes expire even if topology does not change

Overview / Comparizon

On-Demand	AODV	DSR
Overall complexity	Medium	Medium
Overhead	Low	Medium
Loop-free	Yes	Yes
Beaconing requirements	No	No
Multiple route support	No	Yes
Routes maintained in	Route table	Route cache
Route reconfiguration methodology	Erase route; notify source	Erase route; notify source
Routing metric	Freshest and shortest path	Shortest path

Hybrid Protocols

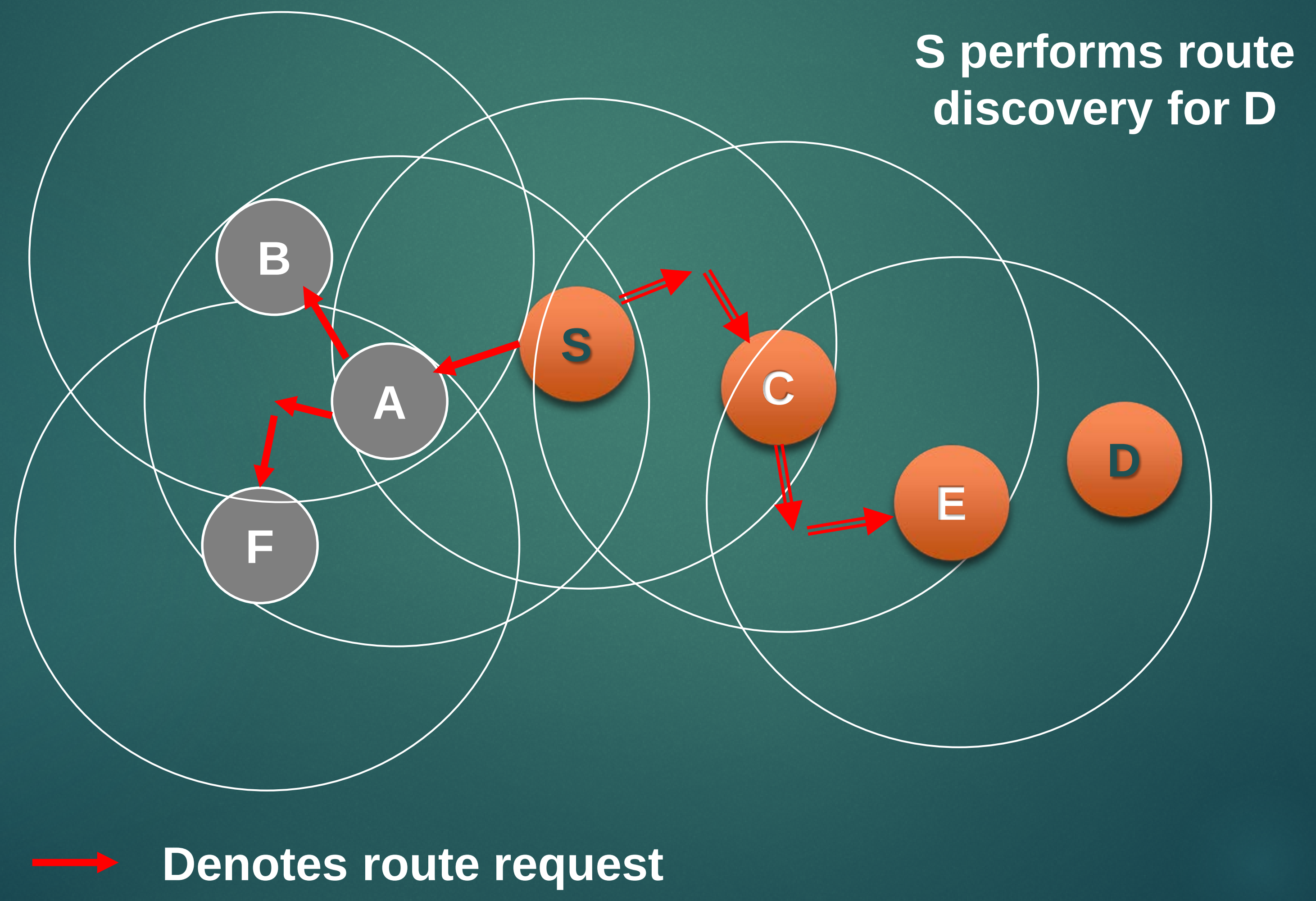
Zone Routing Protocol (ZRP)

Zone routing protocol combines

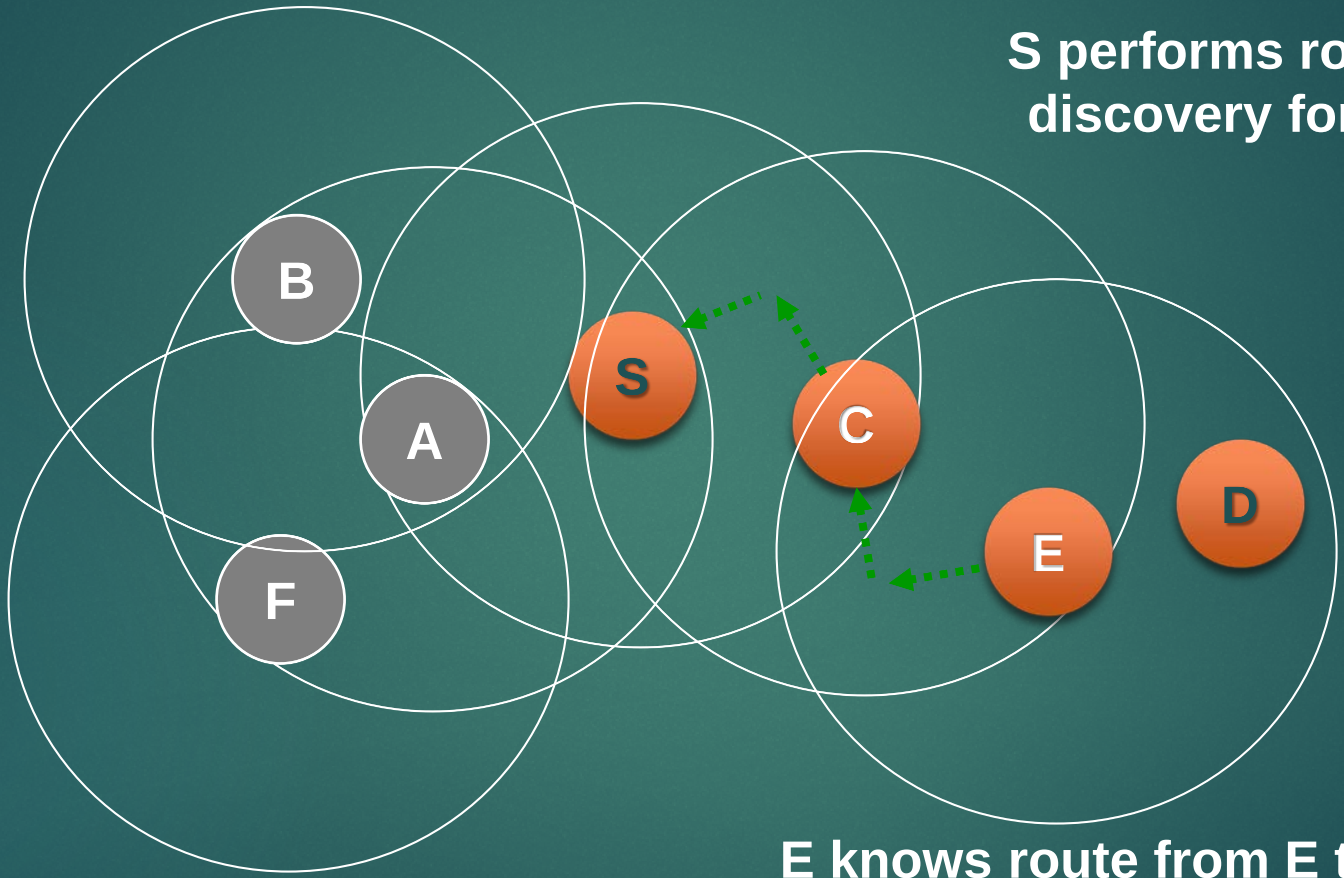
- Proactive protocol: which pro-actively updates network state and maintains route regardless of whether any data traffic exists or not

- Reactive protocol: which only determines route to a destination if there is some data to be sent to the destination

ZRP: Example with Zone Radius = d = 2



ZRP: Example with $d = 2$

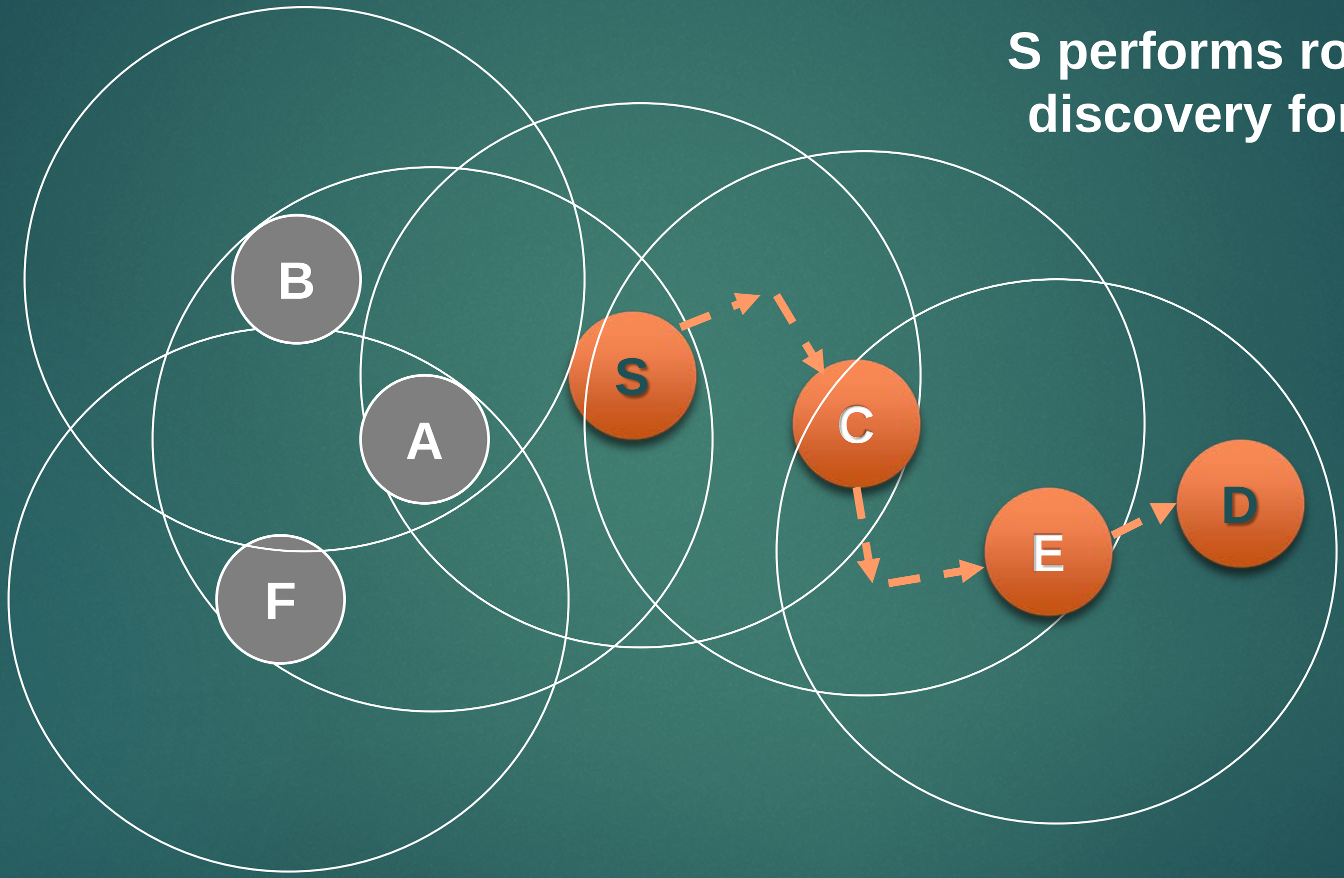


S performs route discovery for D

E knows route from E to D, so route request need not be forwarded to D from E

Denotes route reply

ZRP: Example with *d* = 2



S performs route discovery for D

Denotes route taken by Data

thank you!

Questions?