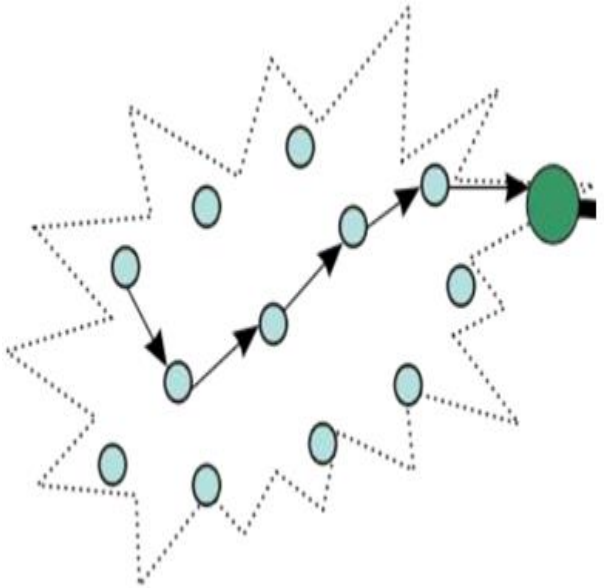
Wireless Sensor Networks

Wireless sensor network

- A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations
- Wireless sensors are limited in memory, computation power, bandwidth, and energy. Due to their small physical size, they can be embedded in the physical environment
- Low cost & energy implies low power CPU, radio with minimum bandwidth and range
- Ad-hoc deployment implies no maintenance or battery replacement

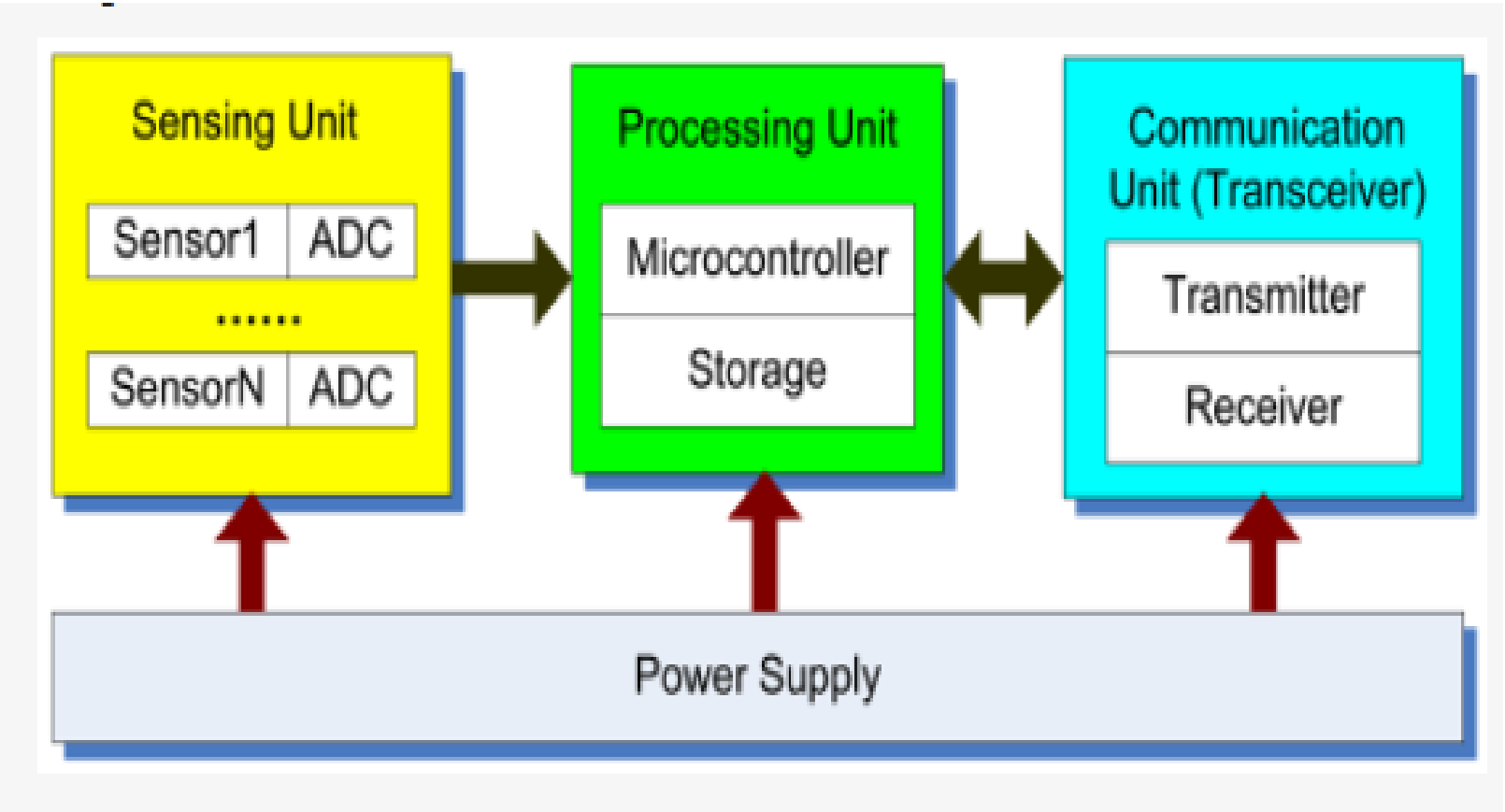
Sensor network

- Sensor
  - A transducer
  - converts physical phenomenon e.g. heat, light, motion, vibration, and sound into electrical signals
- Sensor node
  - basic unit in sensor network
  - contains on-board sensors, processor, memory, transceiver, and power supply



- Sensor network
  - consists of a large number of sensor nodes
  - nodes deployed either inside or very close to the sensed phenomenon

Hardware Architecture of sensor node



Characteristics of WSN

- Sensing and data processing are essential
- WSNs have many more nodes and are more densely deployed
- Hardware must be cheap; nodes are more prone to failures
- WSNs operate under very strict energy constraints
  - Sleep as much as possible.
  - Acquire data only if indispensable.
  - Use data fusion and compression.
  - Transmit and receive only if necessary. Receiving is just as costly as sending.
- WSN nodes are typically static
- The communication scheme is many-to-one (data collected at a base station) rather than peer-to-peer

Data Collection

- Centralized data collection puts extra burden on nodes close to the base station. Clever routing can alleviate that problem
- Clustering: data from groups of nodes are fused before being transmitted, so that fewer transmissions are needed
- Often getting measurements from a particular area is more important than getting data from each node
- Security and authenticity should be guaranteed. However, the CPUs on the sensing nodes cannot handle fancy encryption schemes.

Infrastructure vs. Ad-Hoc Networks

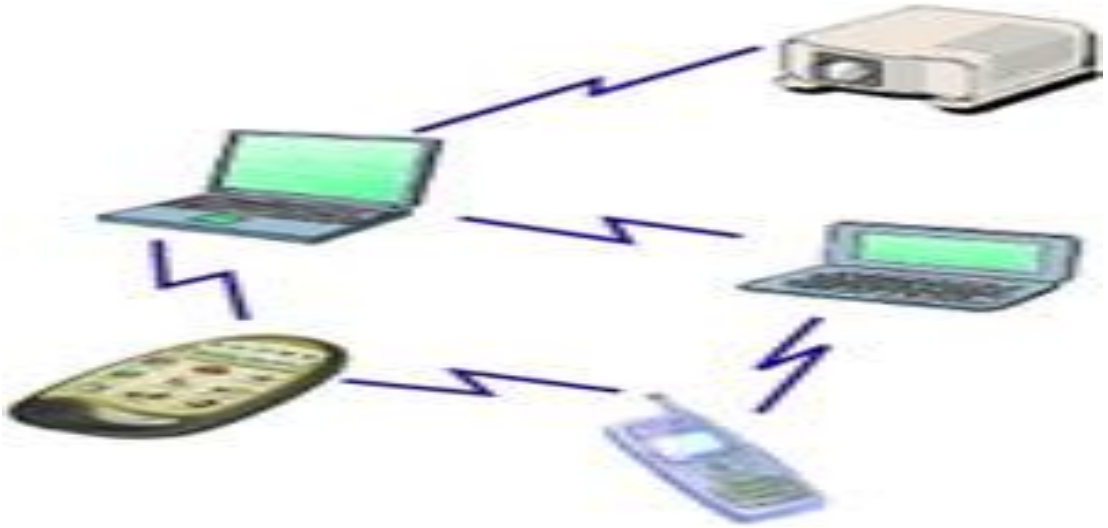
- Infrastructure network consists of wired network or fixed connectivity

Ad-hoc means '*for this purpose*'

- No need for infrastructure (like routers, cell towers, etc.)
- It can accommodate new devices at any time.
- MANET: Mobile Ad-Hoc Network
- WSN: Wireless sensor network

MANET

- MANET – (Mobile Ad-Hoc NETwork) a system of mobile nodes (laptops, sensors, etc.) interfacing without the assistance of centralized infrastructure (access points, bridges, etc.)



Ad Hoc Wireless Networks

- Large number of self-organizing static or mobile nodes that are possibly randomly deployed
- Near(est)-neighbor communication
- Wireless connections
  - Links are fragile, possibly asymmetric
  - Connectivity depends on power levels and fading
  - Interference is high for omnidirectional antennas
- WSNs are ad hoc networks (wireless nodes that self-organize into an infrastructure-less network).

Environment monitoring

Zebranet: a WSN to study the behavior of zebras

- Special GPS-equipped collars were attached to zebras
- Data exchanged with peer-to-peer info swaps
- Coming across a few zebras gives access to the data

Medical application

- Vital sign monitoring
- Accident recognition
- Monitoring the elderly

- Intel deployed a 130-node network to monitor the activity of residents in an elder care facility.
- Patient data is acquired with wearable sensing nodes (the “watch”)

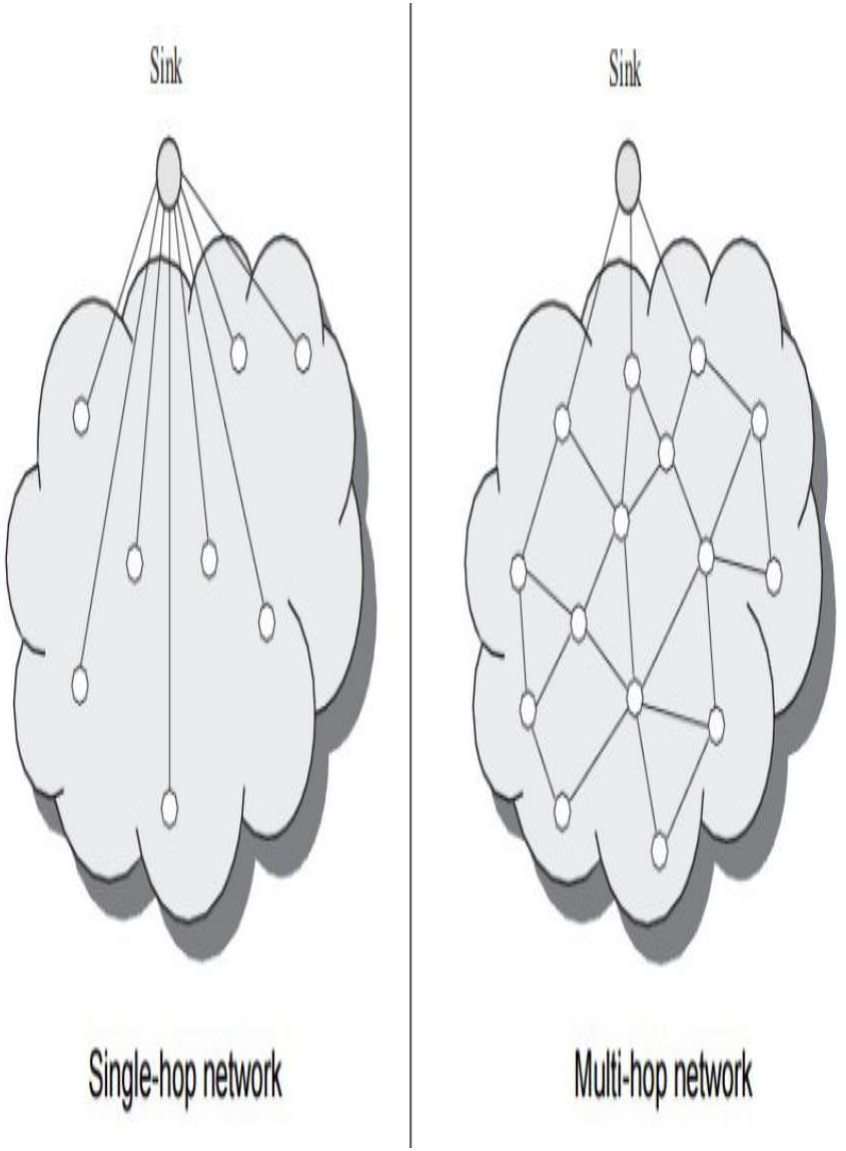
Data-dissemination Schemes

Direct communication with the base station

- Sensor nodes communicate with the base station directly.

Multi-hop Scheme

- Transmit through some other intermediate nodes.



WSN network Architecture

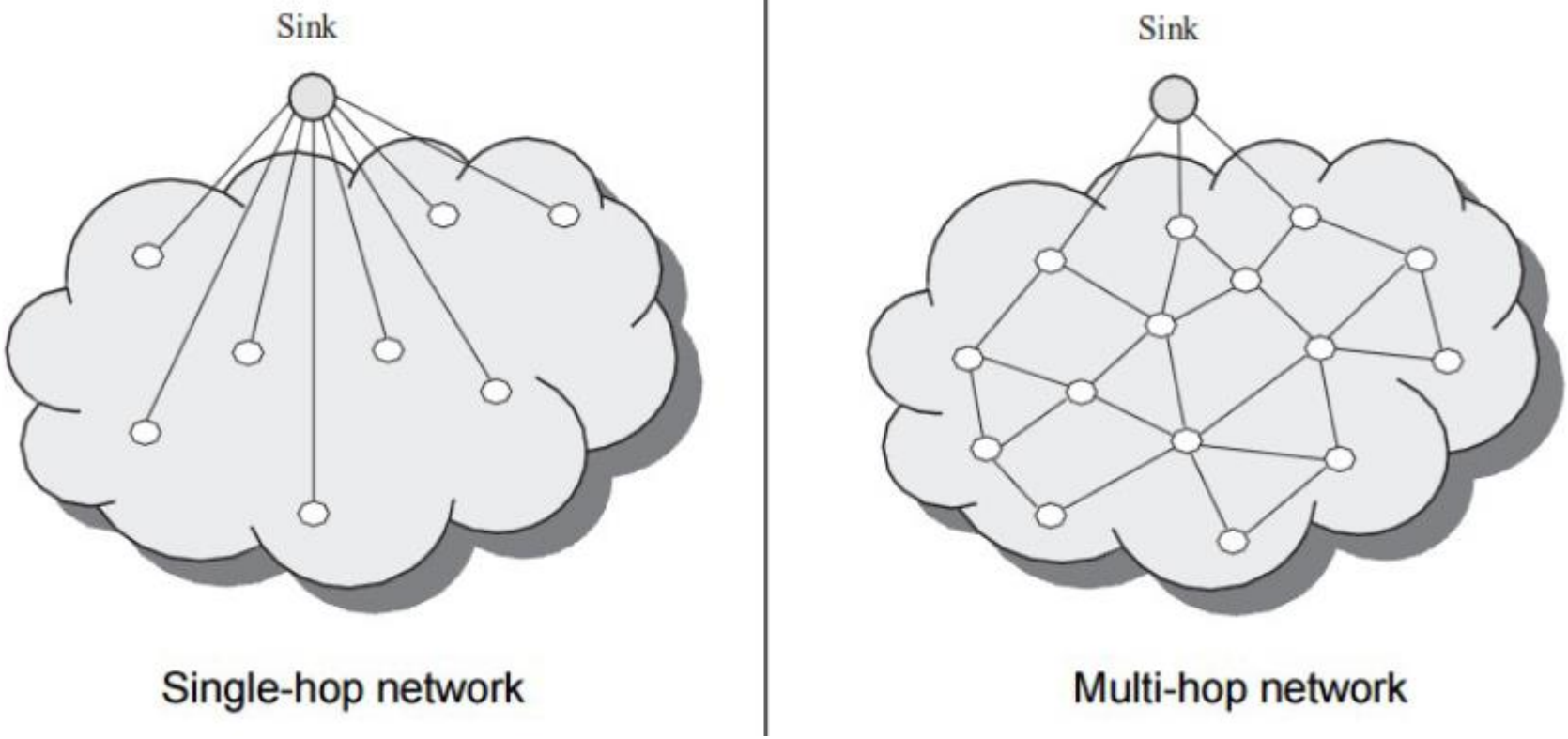
- Flat Architecture:

  Each node plays the same role in performing sensing task and all sensor nodes are peers

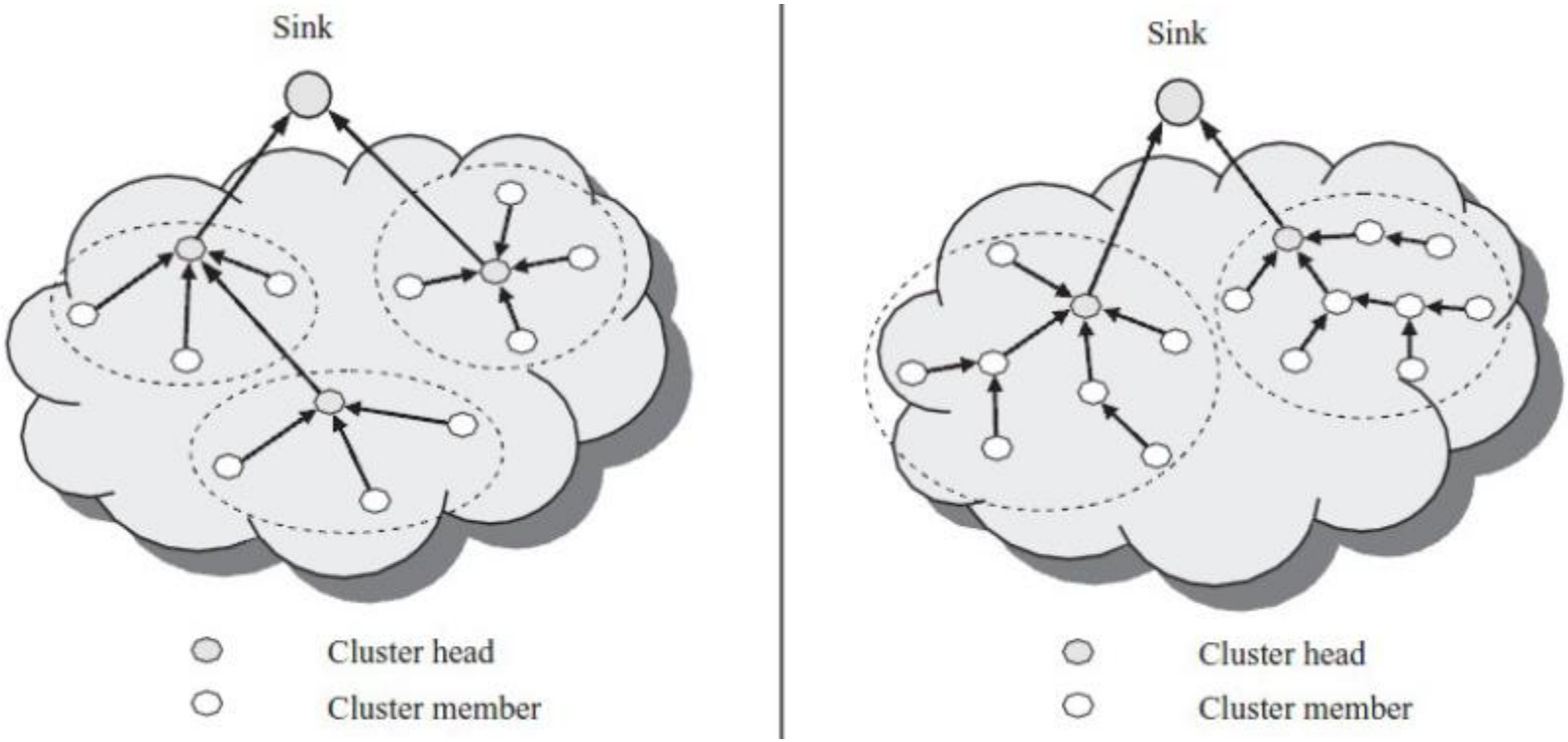
- Hierarchical Architecture:

  Sensor nodes are organized clusters, where the cluster members send their data to the sink

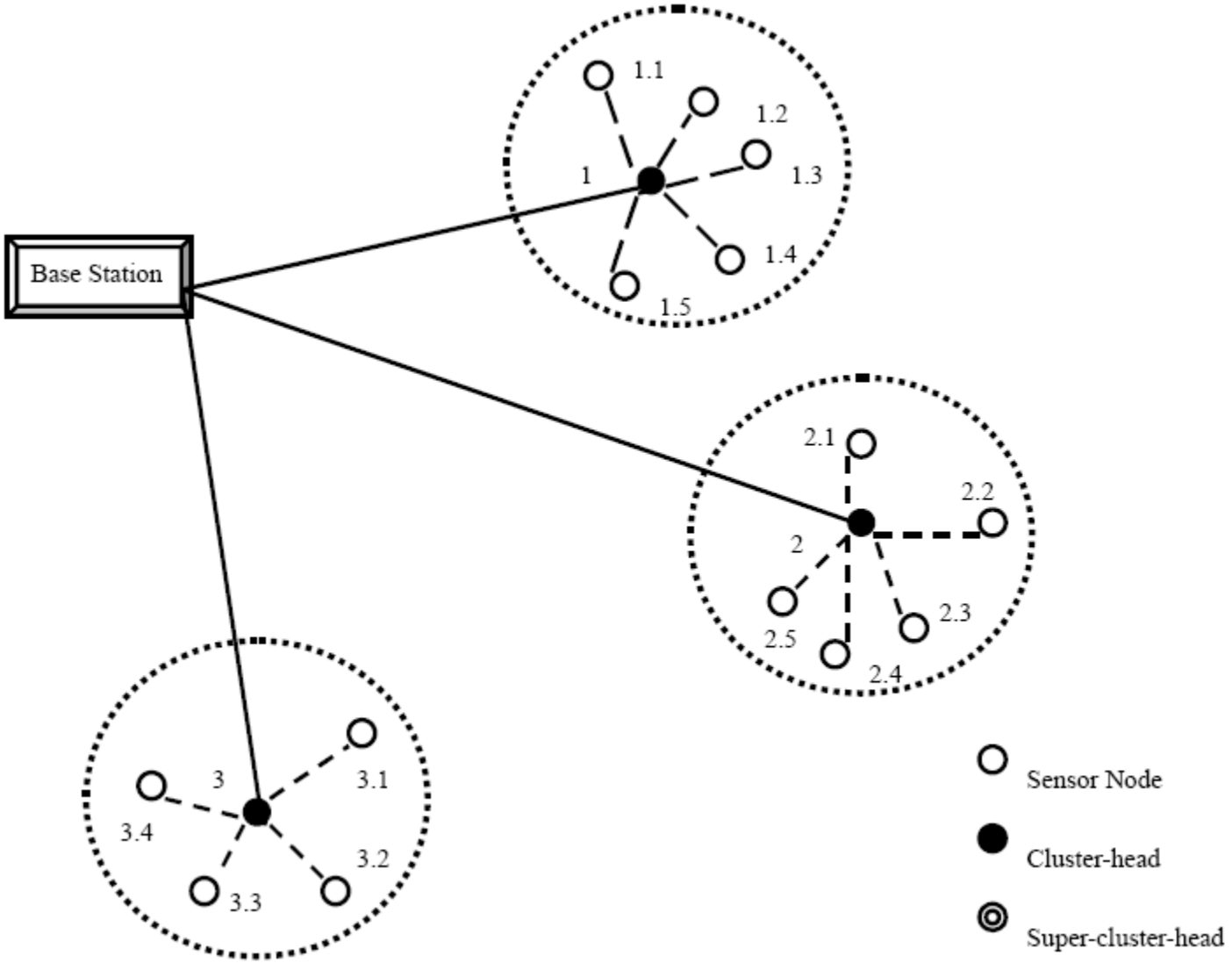
Flat Architecture



Hierarchical Architecture



Hierarchical Architecture

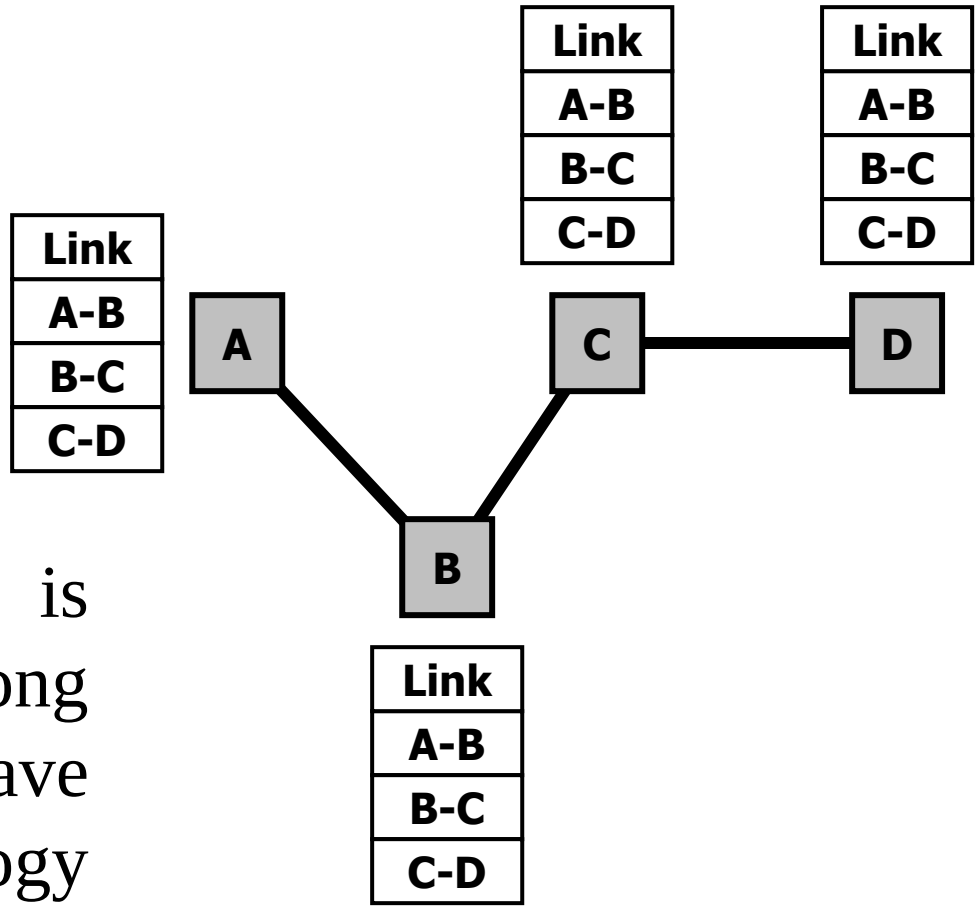


Ad-Hoc Routing Protocol

- An ad-hoc routing protocol is a convention that controls how nodes decide which way to route packets between computing devices in a mobile ad-hoc network
- Foundation in most protocols: neighbor discovery
  - Nodes send periodic announcements as broadcast packets (beacon messages, alive messages, …)
  - Can embed "neighbor table" into such messages; allows nodes to learn "2-hop neighborhood"
- Popular types of routing protocols:
  - Proactive
  - Reactive
  - Geographic

Proactive: "Link-State" Algorithms

- Each node shares its link information so that all nodes can build a map of the full network topology

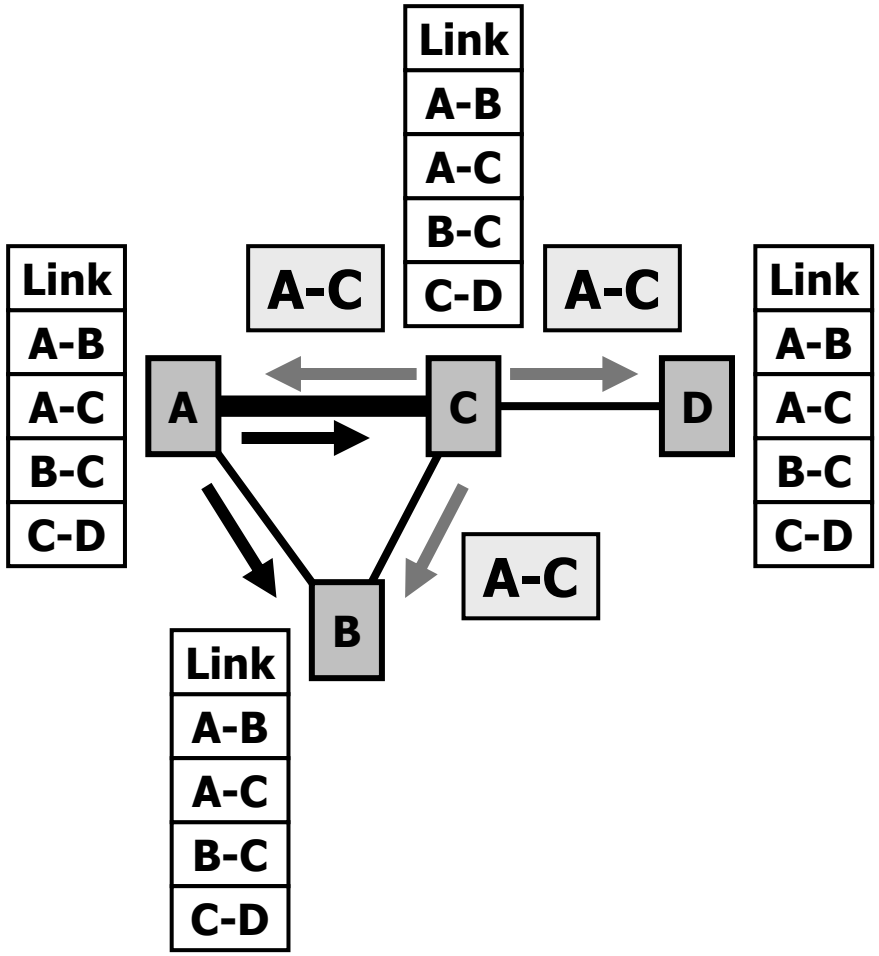


- Assuming the topology is stable for a sufficiently long period, all nodes will have the same topology information

Proactive: "Link-State" Algorithms

- Link information is updated when a link changes state (goes up or down)
  - by sending small "hello" packets to neighbors

- Nodes A and C propagate the existence of link A-C to their neighbors and, eventually, to the entire network

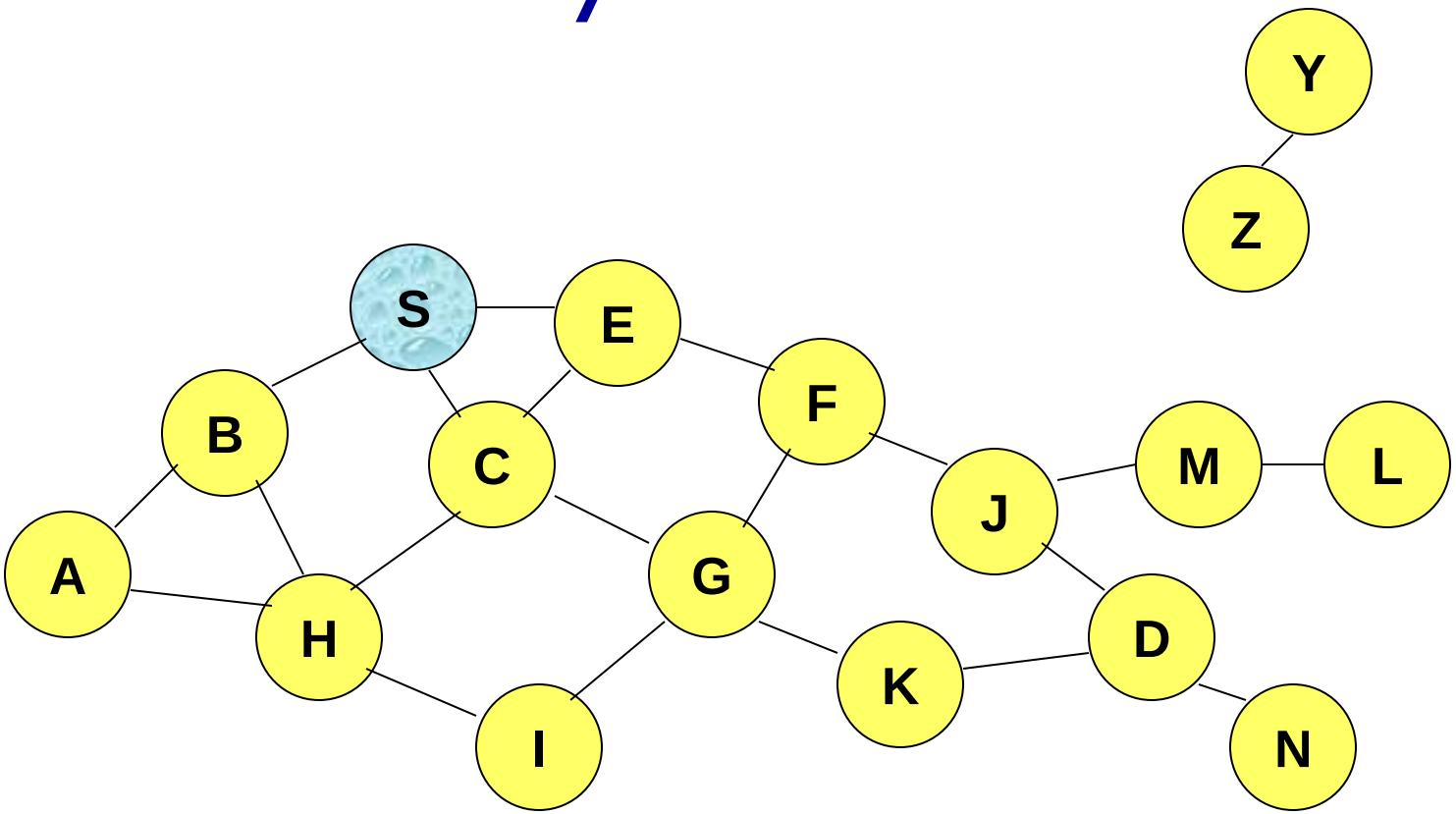


Reactive: DSR

Dynamic **S**ource **R**outing

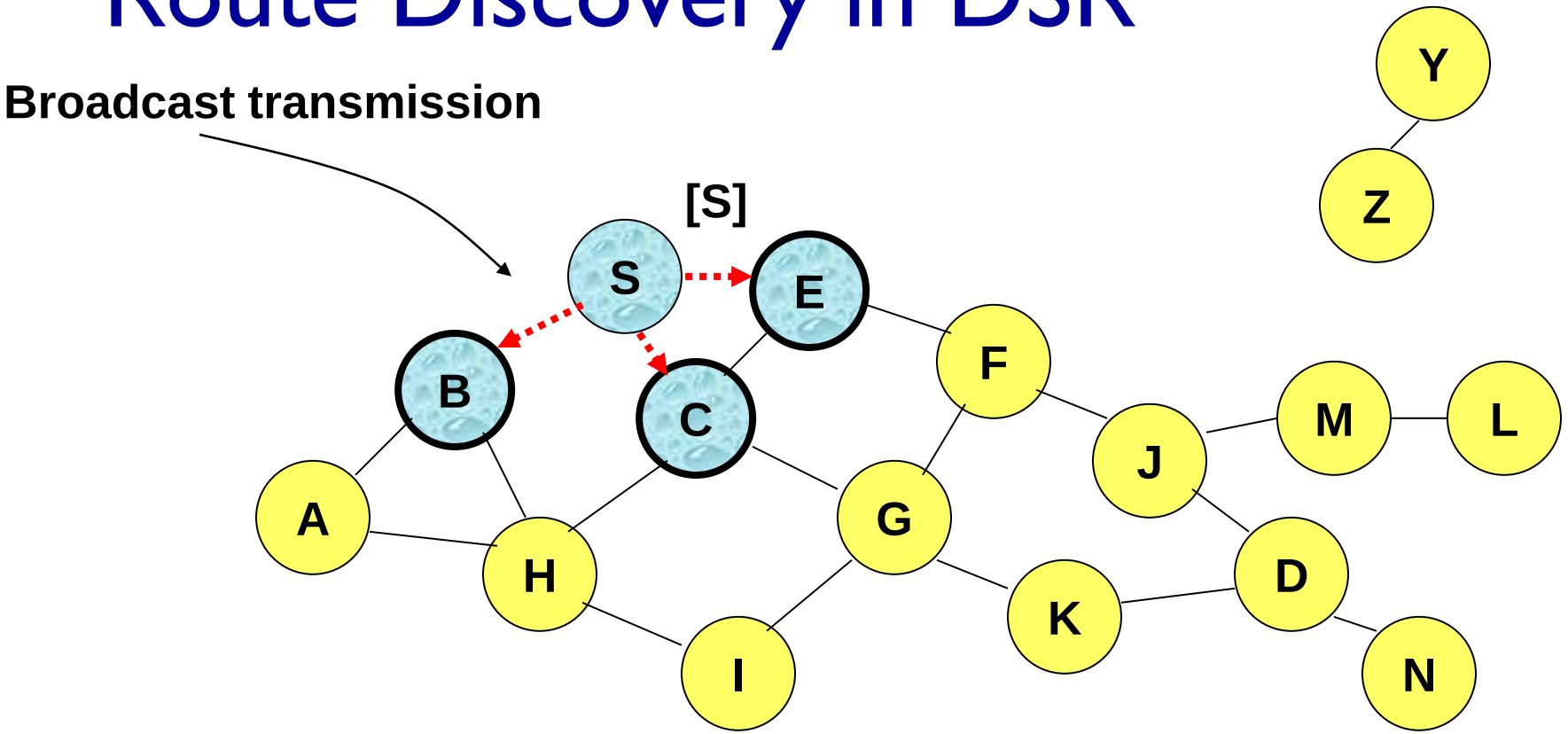
- Search for route when needed only
  - Search using **Route Request (RREQ)** broadcasts
  - Response using **Route Reply (RREP)** message
- Every message along route contains entire path to help intermediate nodes to decide what to do with message

Route Discovery in DSR



Represents a node that has received RREQ for D from S

Route Discovery in DSR

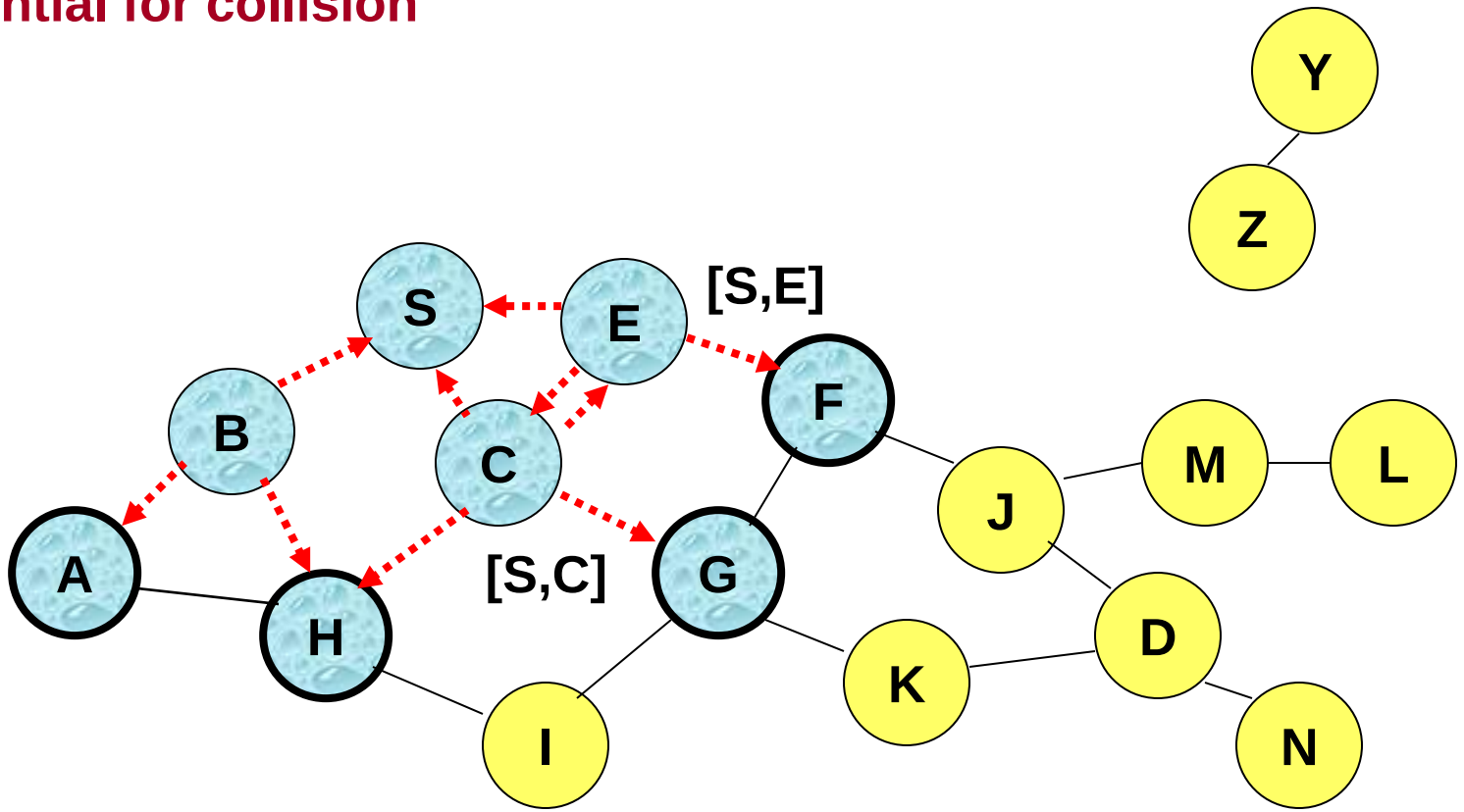


Represents transmission of RREQ

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

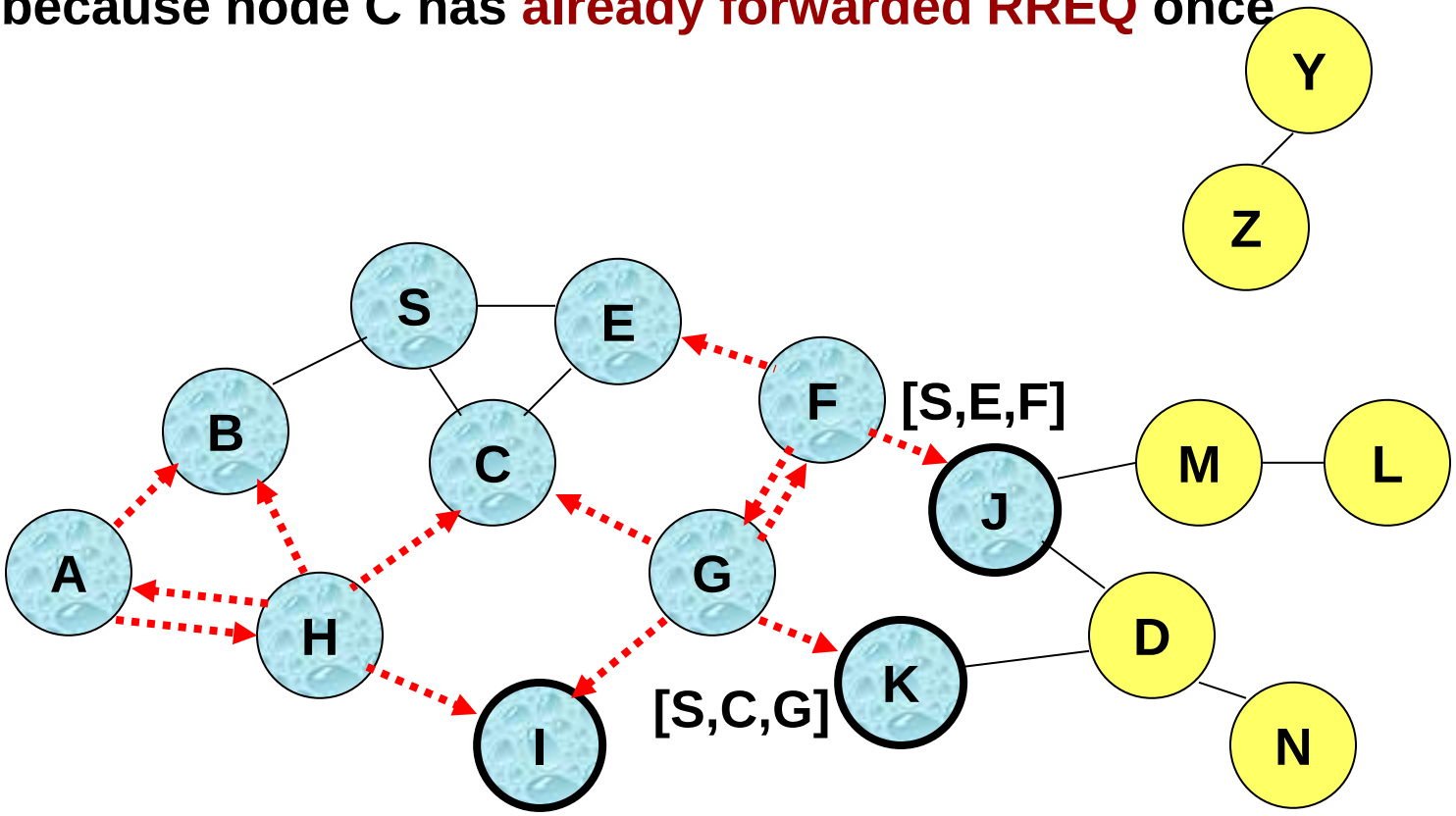
Route Discovery in DSR

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



Route Discovery in DSR

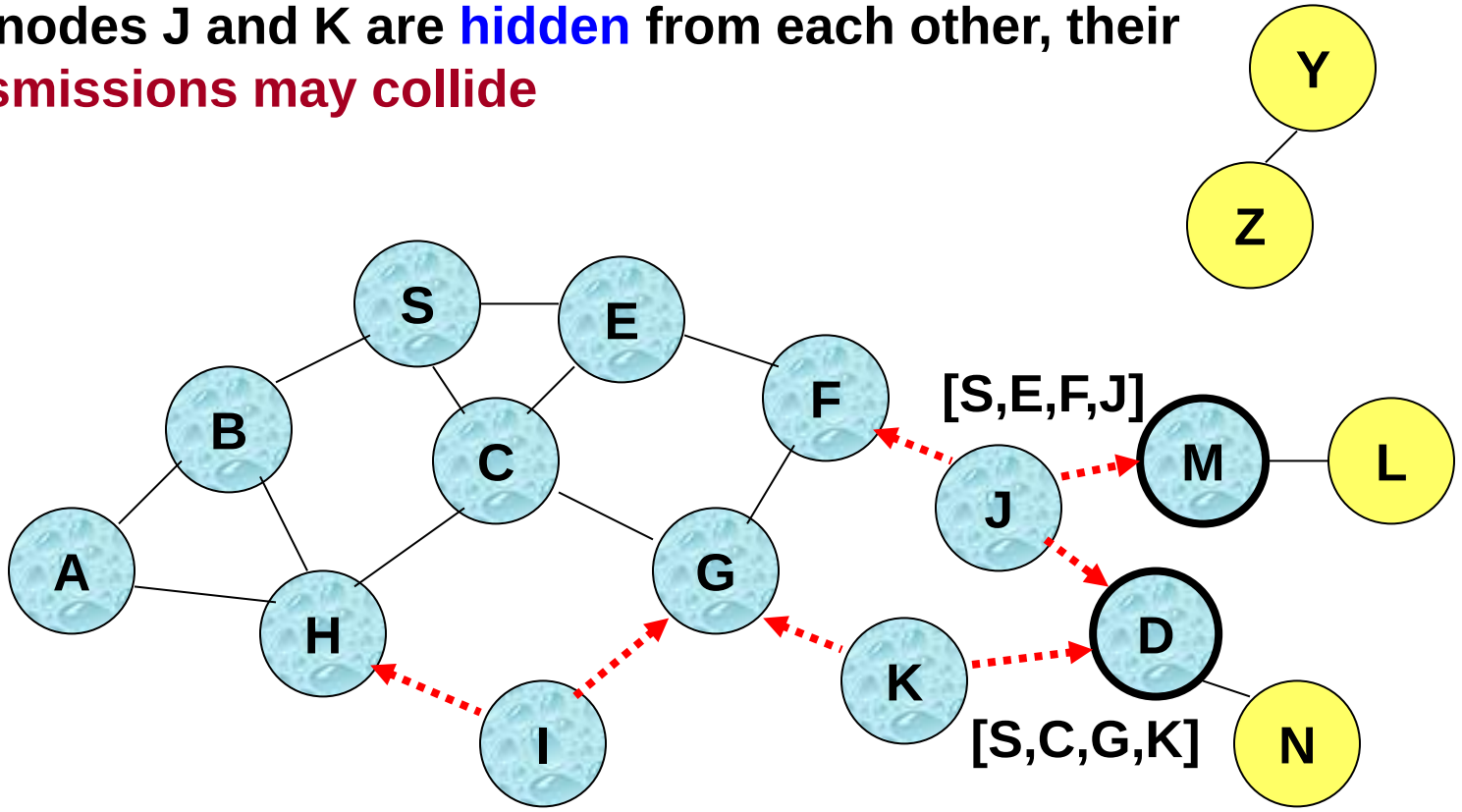
Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once



Route Discovery in DSR

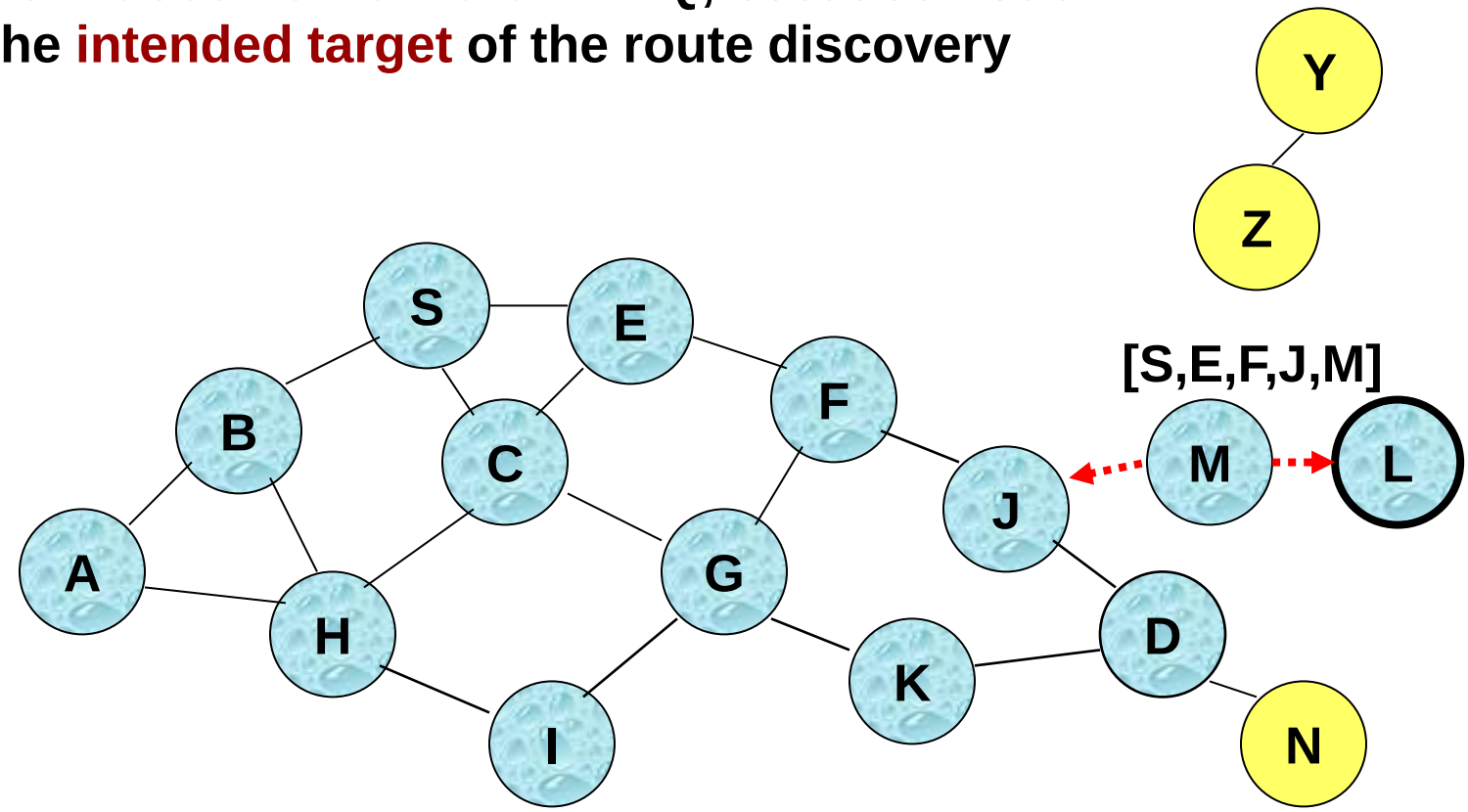
Nodes J and K both broadcast RREQ to node D

Since nodes J and K are hidden from each other, their transmissions may collide

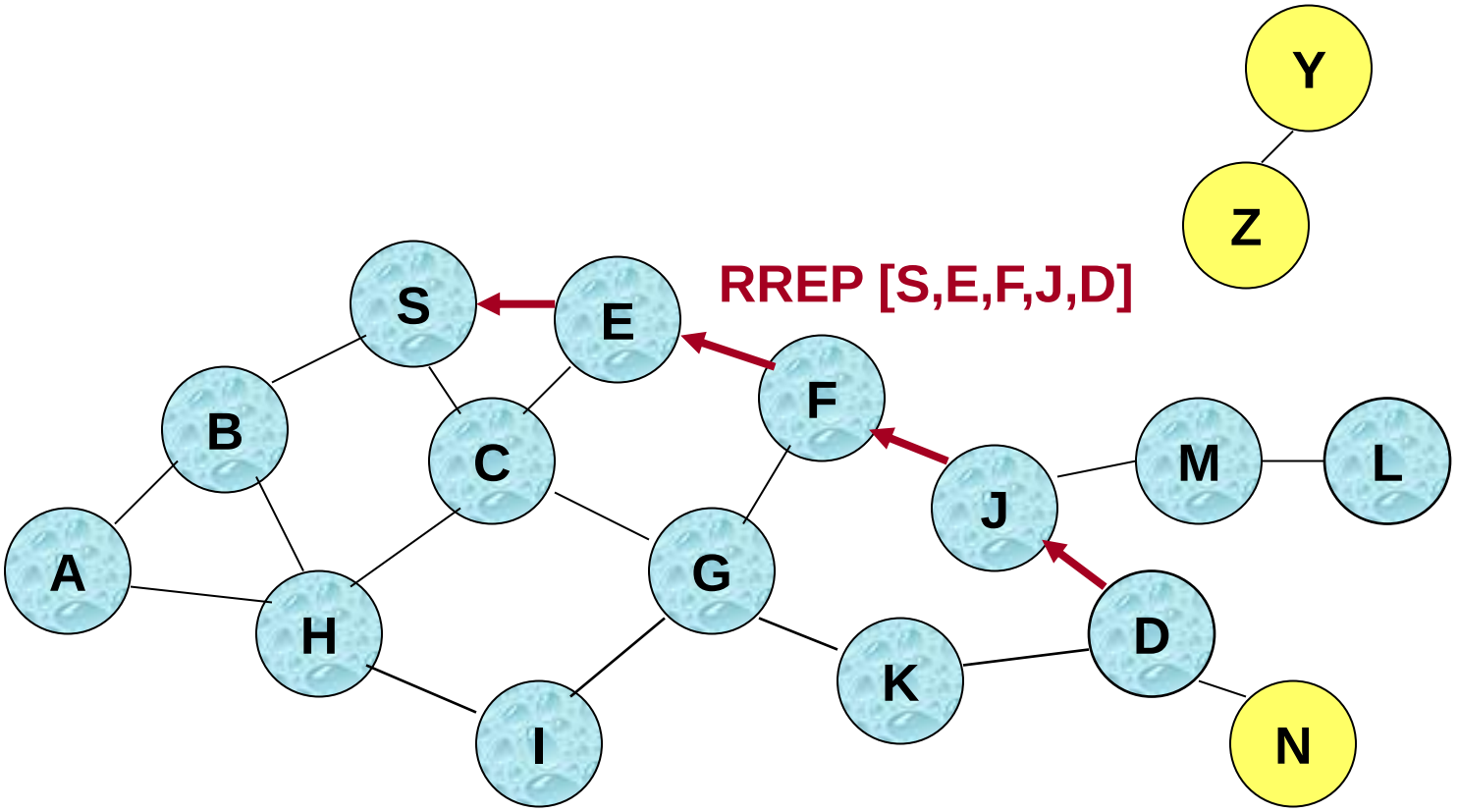


Route Discovery in DSR

- **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

Route Reply in DSR

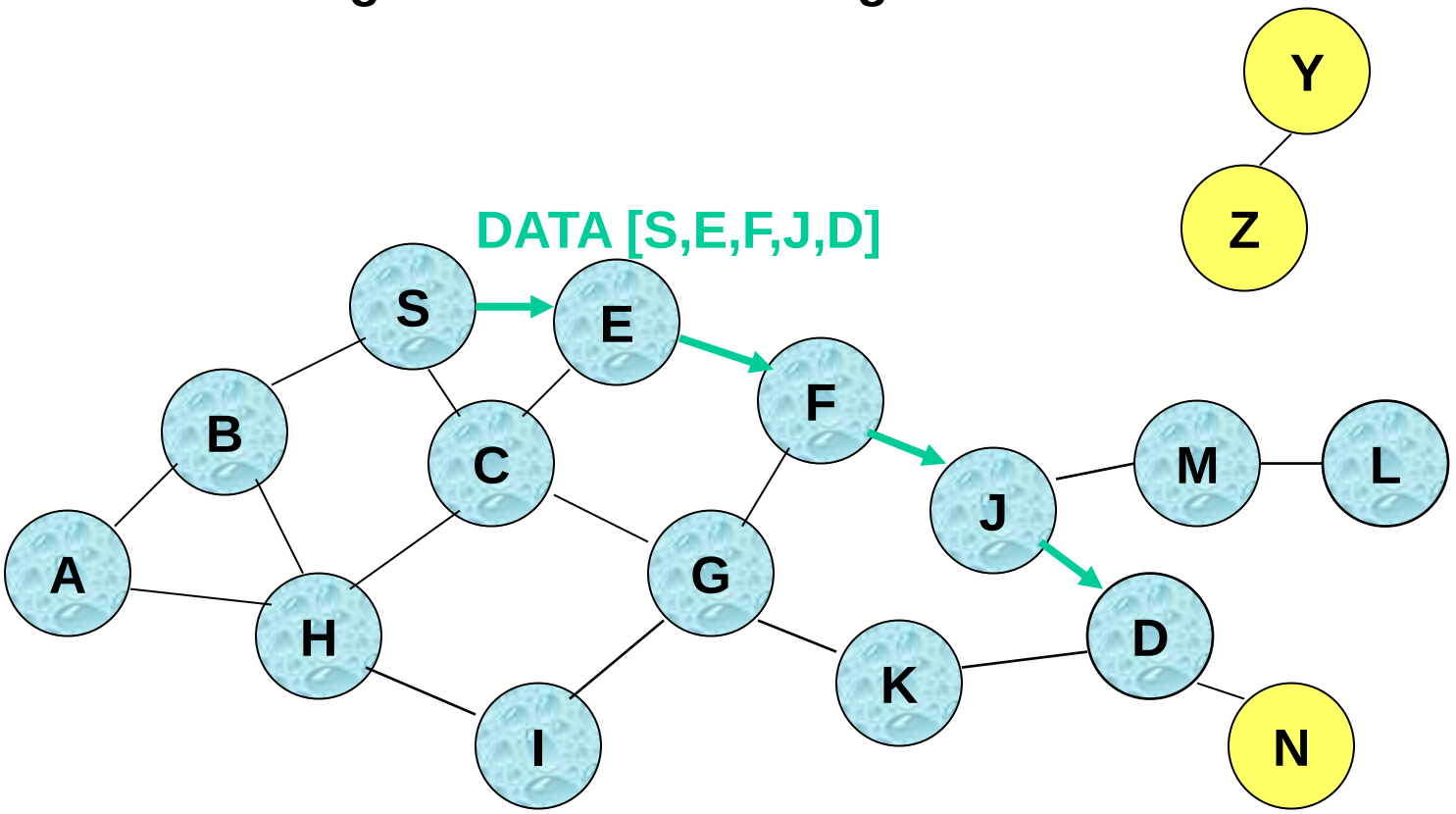
- Route Reply can be sent by reversing the route in Route Request (RREQ) only if links are guaranteed to be bidirectional
- One way to ensure this is to check, if the received RREQ was on a link that is known to be bi-directional, e.g.
  - If IEEE 802.11 MAC is used to send data, then links have to be bi-directional (since Ack is used)
- If unidirectional (asymmetric) links are allowed, then RREP may need a route discovery for S from node D
  - Route discovery not needed -> If 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.

Route Reply in 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



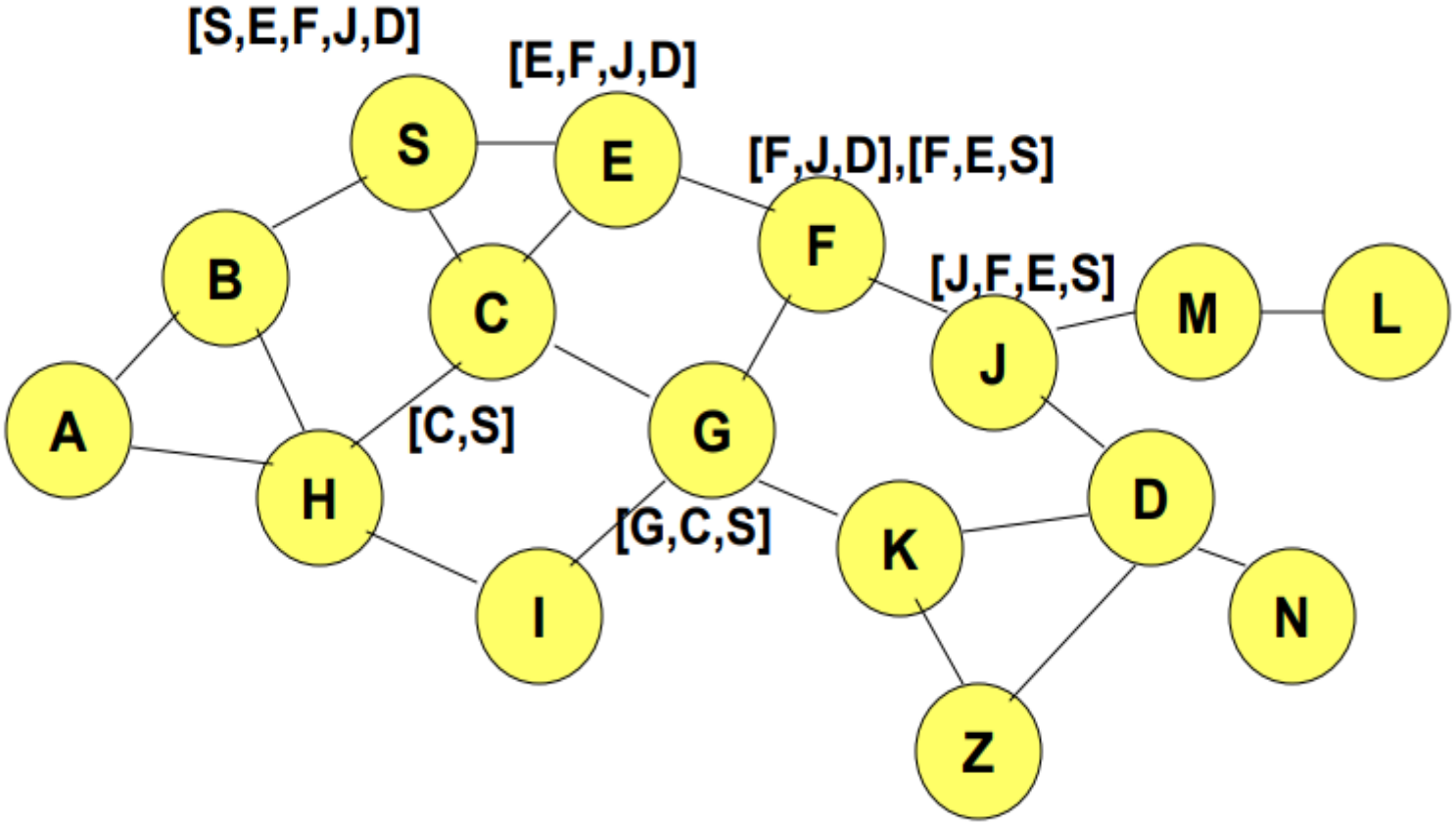
DSR Optimization: Route Caching

- Each node caches a new route it learns by any means
- When node S finds route [S,E,F,J,D] to node D, node S also learns route [S,E,F] to node F
- When node K receives Route Request [S,C,G] destined for node D, node K learns route [K,G,C,S] to node S
- When node F forwards Route Reply RREP [D,J,F, E,S], 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

DSR Optimization: Route Caching

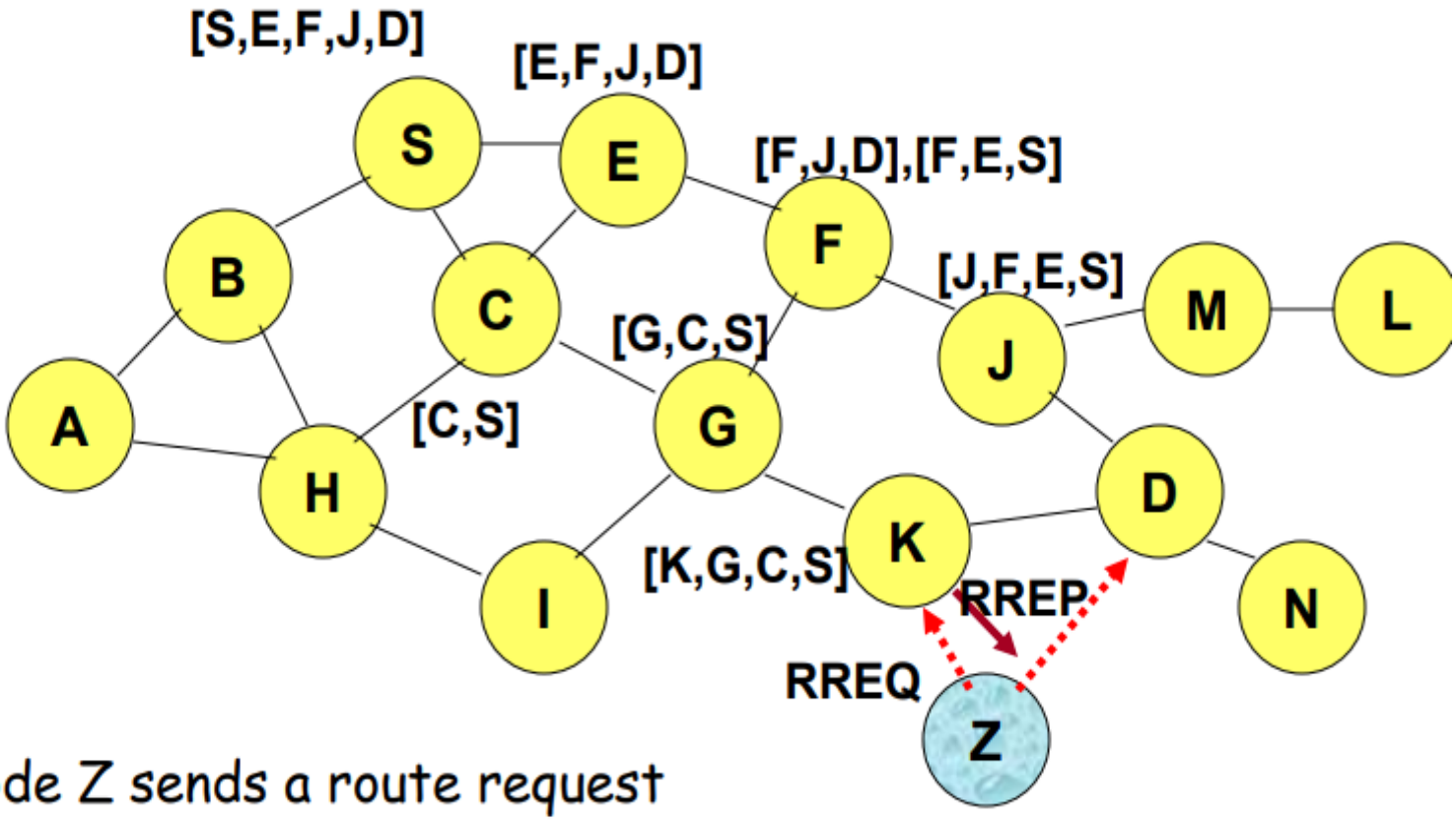
- When node S learns that a route to node D is broken,
  - Can use another route from its local cache, if such a route to D exists in its cache.
  - Otherwise, node S initiates route discovery by sending a route request
- Node X on receiving a Route Request for some node D can send a Route Reply if node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



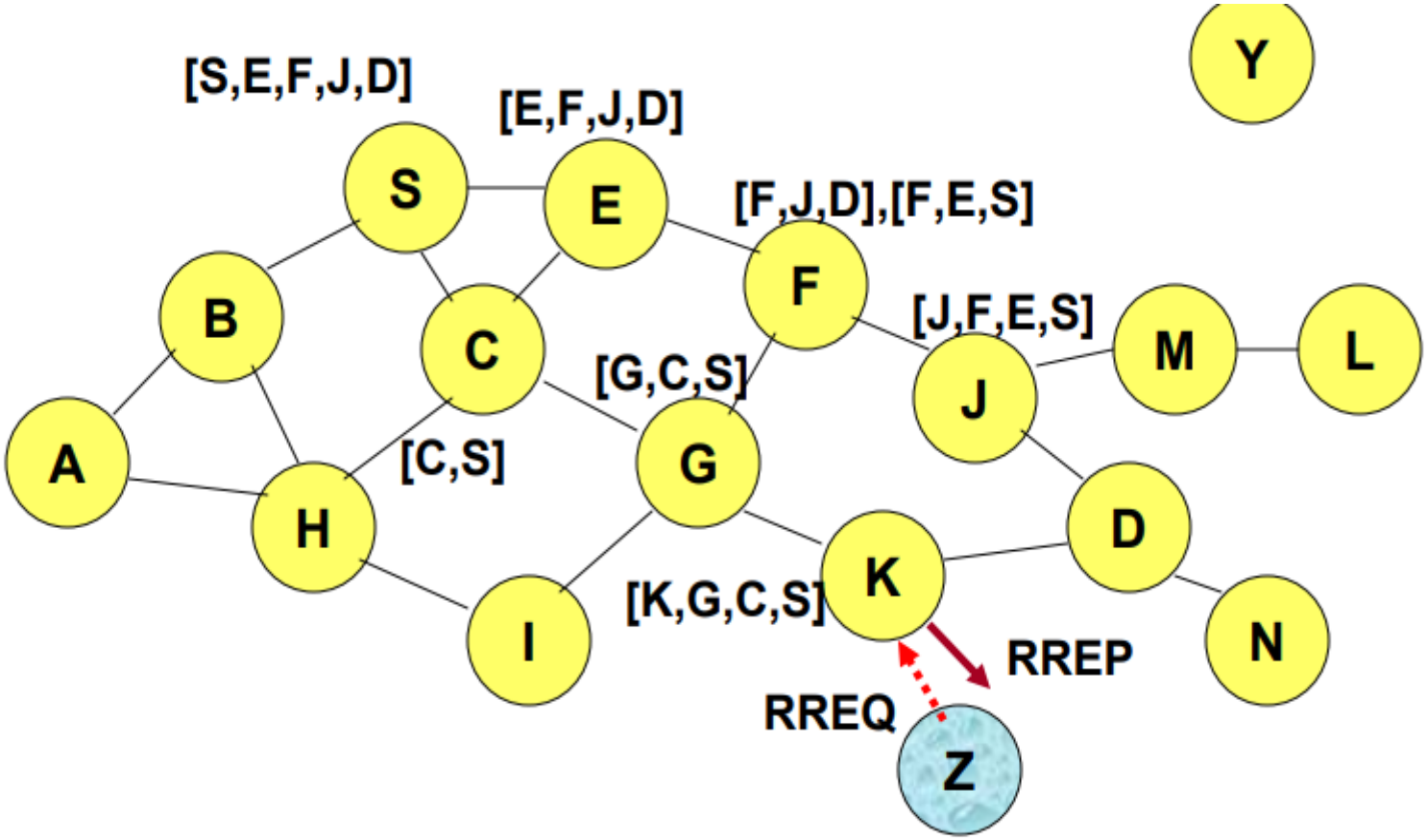
[P,Q,R] Represents cached route at a node
(DSR maintains the cached routes in a tree format)

Route Caching benefits: speed up of Route Discovery



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

Route Caching benefits: Reduction in propagation of RREQs



- Route Reply (RREP) from node K limits flooding of RREQ.

DSR : Explore the following

- Duplication of Route hops
- Route Maintenance
  - Preventing Route Reply Storms
  - Route Request hop limits
  - Packet Salvaging
  - Automatic Route Shortening
  - Increased spreading of Route Error messages

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
- Increased contention if too many route replies come back due to nodes replying using their local cache
  - Route Reply Storm problem

Proactive vs Reactive

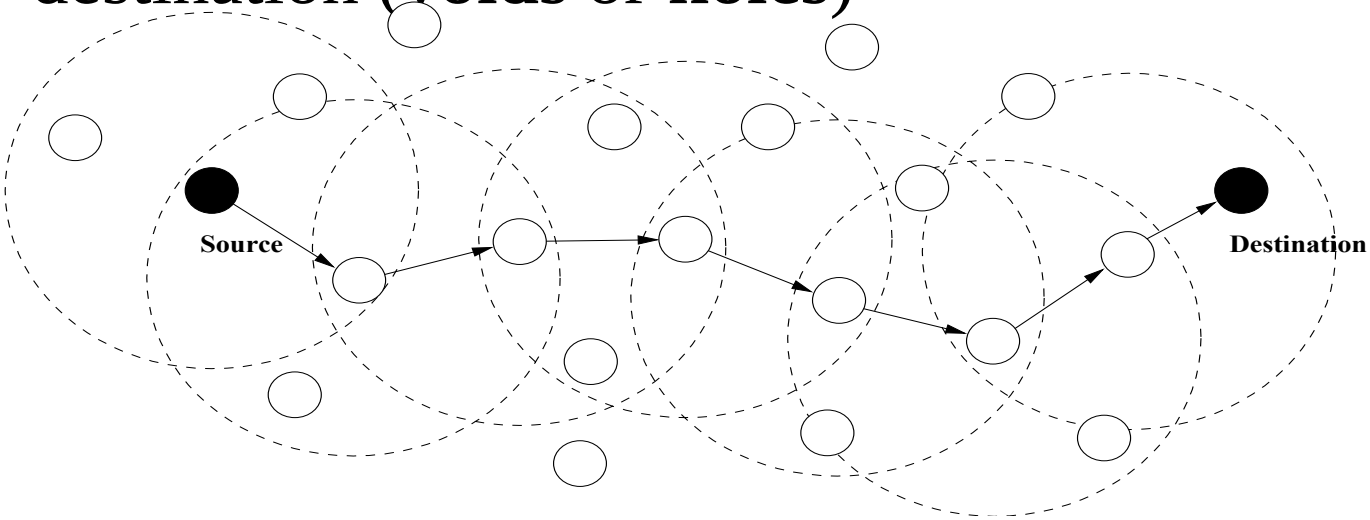
- Reactive:
  - Only establish/maintain routes between nodes needed them (in contrast: tables store ALL routes)
  - Store entire route in each message; message size grows with route length
  - Route requests cause “flooding”
- Proactive:
  - Route information always available; no need to search for route (but route information can be outdated)
  - Continuous exchange of route change updates

Geographic Routing

- Nodes use location information to make routing decisions
  - sender must know the locations of itself, the destination, and its neighbors
  - location information can be queried or obtained from a **location broker**
  - location information can come from GPS (Global Positioning System) or some other form of positioning technology

Unicast Location-Based Routing

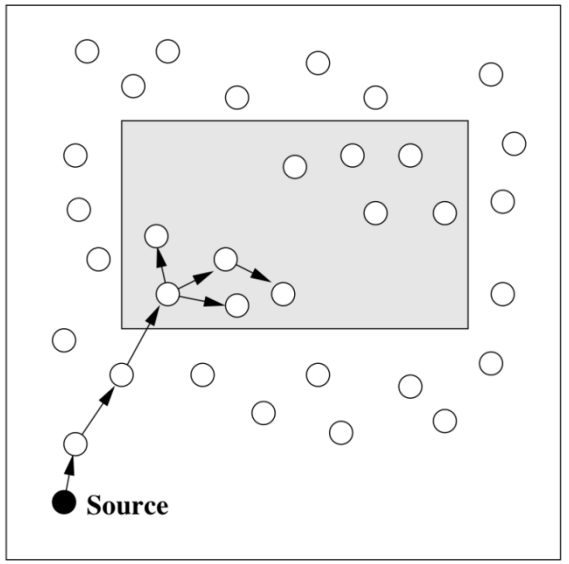
- One single destination
- Each forwarding node makes localized decision based on the location of the destination and the node's neighbors (**greedy forwarding**)
- **Challenge:** packet may arrive at a node without neighbors that could bring packet closer to the destination (**voids** or **holes**)



Geocasting

- Packet is sent to all or some nodes within specific geographic region
- **Example:** query sent to all sensors within geographic area of interest

- **Routing challenge:**
  - propagate a packet near the target region (similar to unicast routing)
  - distribute packet within the target region (similar to flooding)



Design Challenges

- Heterogeneity
  - The devices deployed may be of various types and need to collaborate with each other.
- Distributed Processing
  - The algorithms need to be centralized as the processing is carried out on different nodes.
- Low Bandwidth Communication
  - The data should be transferred efficiently between sensors

Design Challenges

- Large Scale Coordination
  - The sensors need to coordinate with each other to produce required results.
- Utilization of Sensors
  - The sensors should be utilized in a ways that produce the maximum performance and use less energy.
- Real Time Computation
  - The computation should be done quickly as new data is always being generated.

Applications of WSN

- Military and national security application
- Environment monitoring
- Medical application
- Home and Office Applications
- Automotive Applications