MANETs and Dynamic Source Routing Protocol

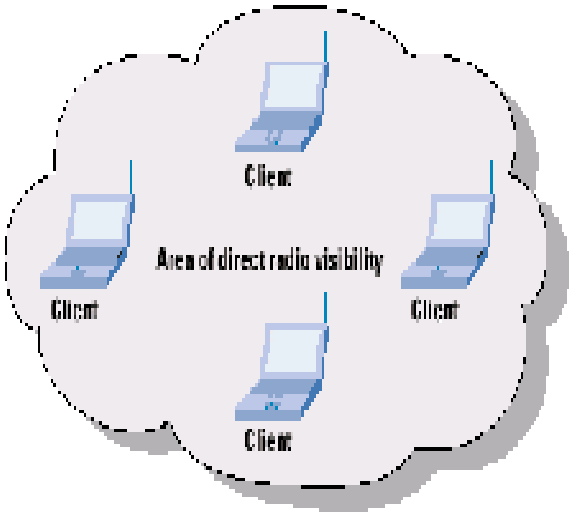
Diwakar Yagaysen

CSE, BBDNITM, Lucknow

Mobile Ad Hoc Networks (MANET)

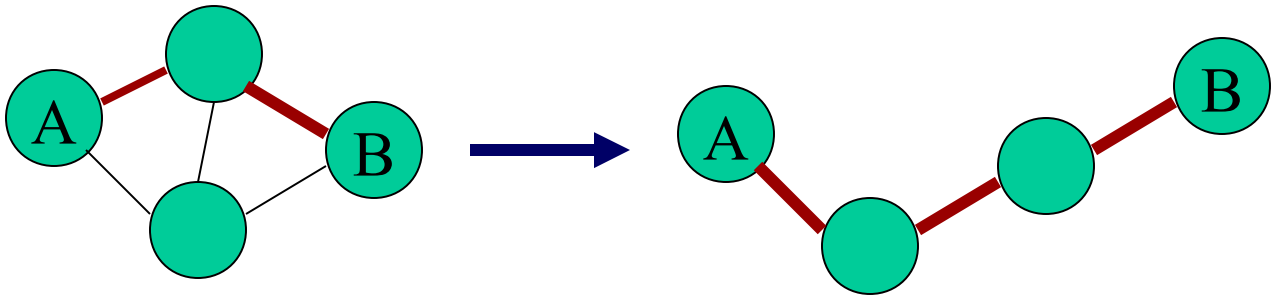
- Information exchange in a network of mobile and wireless nodes without any infrastructural support.
- Such networks are often called ad hoc networks to emphasize that they do not depend on infrastructural support.
- A mobile ad-hoc network is a mobile, multi-hop wireless network which is capable of autonomous operation.
- The purpose of an ad hoc network is to set up (possibly) a short-lived network for a collection of nodes.

- Characteristics
  - Energy constrained nodes
  - Bandwidth constrained
  - Variable capacity wireless links
  - Dynamic topology



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.

Why Ad Hoc Networks ?

- Setting up of fixed access points and backbone infrastructure is not always viable
  - Infrastructure may not be present in a disaster area or war zone
  - Infrastructure may not be practical for short-range radios; Bluetooth (range ~ 10m)

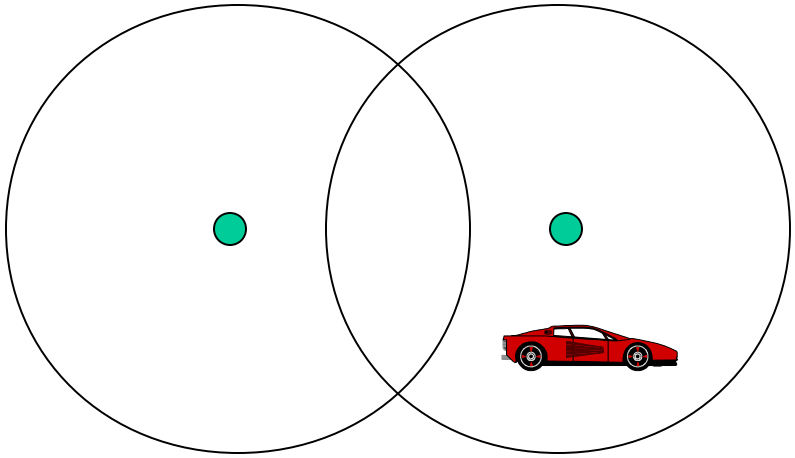
- Ad hoc networks:
  - Do not need backbone infrastructure support
  - Are easy to deploy
  - Useful when infrastructure is absent, destroyed or impractical

Wireless Networks

- Need: Access computing and communication services, on the move
- Infrastructure-based Networks
  - traditional cellular systems (base station infrastructure)
- Wireless LANs
  - Infrared (IrDA) or radio links (Wavelan)
  - very flexible within the reception area; ad-hoc networks possible
  - low bandwidth compared to wired networks (1-1000 Mbit/s)
- Ad hoc Networks
  - useful when infrastructure not available, impractical, or expensive
  - military applications, rescue, home networking

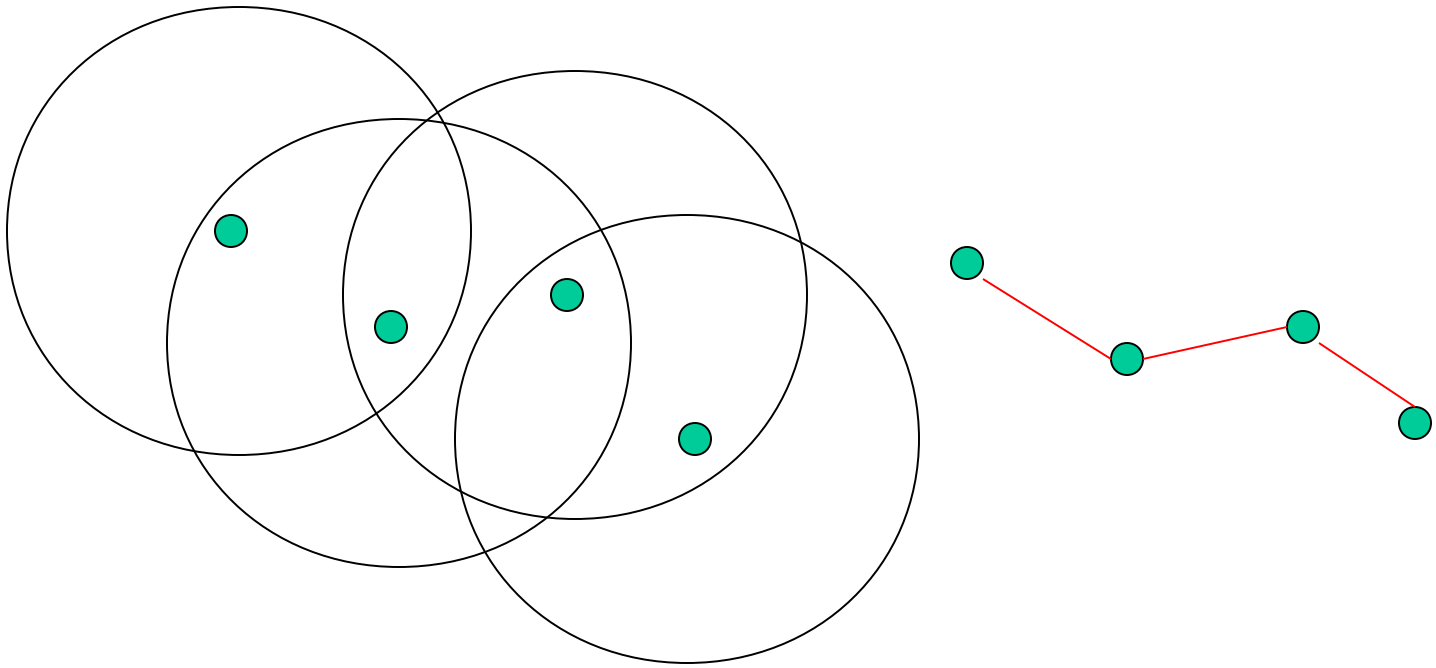
Cellular Wireless

- Single hop wireless connectivity to the wired world
  - Space divided into cells
  - A base station is responsible to communicate with hosts in its cell
  - Mobile hosts can change cells while communicating
  - Hand-off occurs when a mobile host starts communicating via a new base station



Multi-Hop Wireless

- May need to traverse multiple links to reach destination



- Mobility causes route changes

Routing in MANET

- No base station. No fixed infrastructure.
- Traditional fixed networks routing schemes are not effective.
  - E.g. Link state and distance vector routing algorithms
- MANET nodes cooperate to provide routing service.
  - A node communicates directly with nodes in wireless range.
  - For all other destinations, a dynamically determined multi-hop route through other nodes.
  - Rely on each other to forward packets to their destination.

Taxonomy - MANET routing

- Communication model
  - What is the wireless communication model?
- Structure
  - Are all nodes treated uniformly?
  - How are distinguished nodes selected?
- State information
  - Is network scale topology information obtained at each node?
- Scheduling
  - Is the route information always maintained at each destination?

Taxonomy – Communication model

- Multi-channel communication
  - Combine channel assignment and routing functionality
  - Generally used in TDMA or CSMA based networks
  - E.g. Clusterhead Gateway Switched Routing

- Single channel communication
  - Generally CSMA/CA oriented protocols
  - Vary in the extent to which they rely on specific link-layer behaviors like failure detection, traffic information etc.
  - E.g. Dynamic Source Routing, Global State Routing

Taxonomy - Structure

- Uniform protocols
  - No hierarchical structure.
  - Send and respond to routing control messages the same way.
  - Save resource cost in maintaining high-level structure
  - Scalability may become an issue

- Non-Uniform protocols
  - Reduces no. of nodes participating in a route computation.
  - Improve scalability
  - Reduce communication overhead.
  - Support use of greater computational complexity.

Taxonomy – Structure (contd.)

- Further categories of non-uniform protocols
  - Neighbor selection protocol
    - Some nodes take on distinguished role.
    - No negotiation process. No consensus with neighbors.
    - Not affected by non-local topological changes.
  - Partitioning protocol
    - Nodes negotiate a topological partitioning into clusters.
    - Distributed operation. No central topology manager.
    - Roles could be “cluster-head” or “gateway” between two clusters.

Taxonomy – State Information

- Topology based Protocols
  - Exchange large scale (complete) topology information
  - Variants of link-state protocols
    - Less frequent data exchange
    - Apply expensive computation to a few nodes.

- Destination based Protocols
  - Exchange local topology information (e.g. 1 or 2-hop)
  - Most are variants of distance-vector protocols.
  - Others avoid exchange of distance information.
    - Maintain information only for “active” destination.

Taxonomy – Scheduling

- **Proactive protocols**
  - Traditional distributed shortest-path protocols
  - Maintain routes between every host pair at all times
  - Exchange route information
    - Periodically
    - In response to topology change
  - Minimizes delay in obtaining a route
  - Consumes significant network resources due to periodic updates, i.e., High routing overhead
  - Example: DSDV (destination sequenced distance vector)

- **Reactive protocols**
  - Determine route if and when needed
  - Source initiates route discovery
  - 2 step process
    - Route Discovery
    - Route Maintenance
  - Route discovery is expensive

- **Hybrid protocols**
  - Adaptive; Combination of proactive and reactive
  - Example: DSR (dynamic source routing)
  - Example : ZRP (zone routing protocol)

Many Applications

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

Challenges in Mobile Environments

- Limitations of the Wireless Network
  - packet loss due to transmission errors
  - variable capacity links
  - frequent disconnections/partitions
  - limited communication bandwidth
  - Broadcast nature of the communications
- Limitations Imposed by Mobility
  - dynamically changing topologies/routes
  - lack of mobility awareness by system/applications
- Limitations of the Mobile Computer
  - short battery lifetime
  - limited capacities

Effect of mobility on the protocol stack

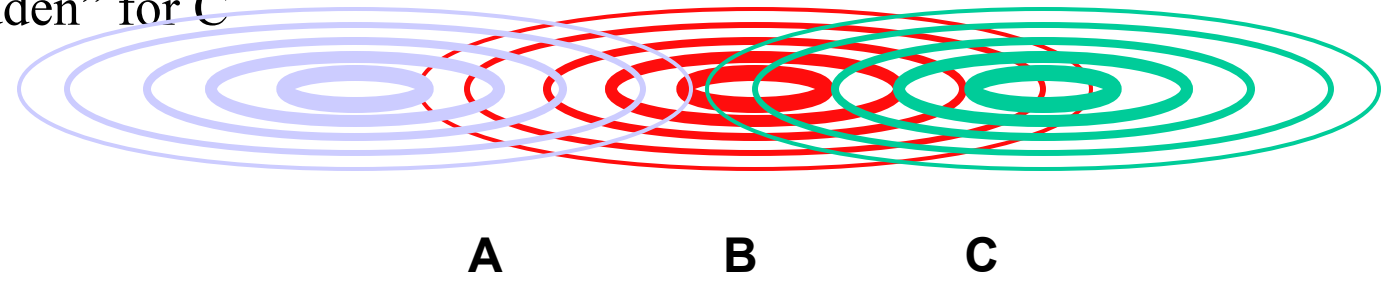
- Application
  - new applications and adaptations
- Transport
  - congestion and flow control
- Network
  - addressing and routing
- Link
  - media access and handoff
- Physical
  - transmission errors and interference

Medium Access Control in MANET

- Can we apply media access methods from fixed networks?
- Example CSMA/CD
  - **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection
  - send as soon as the medium is free, listen into the medium if a collision occurs (original method in IEEE 802.3)
- Medium access problems in wireless networks
  - signal strength decreases proportional to the square of the distance
  - sender would apply **C**arrier **S**ense (CS) and **C**ollision **D**etection (CD), but the collisions happen at the receiver
  - sender may not “hear” the collision, i.e., CD does not work
  - CS might not work, e.g. if a terminal is “hidden”

Hidden and Exposed Terminals

- Hidden terminals
  - A sends to B, C cannot receive A
  - C wants to send to B, C senses a “free” medium (CS fails)
  - collision at B, A cannot receive the collision (CD fails)
  - A is “hidden” for C

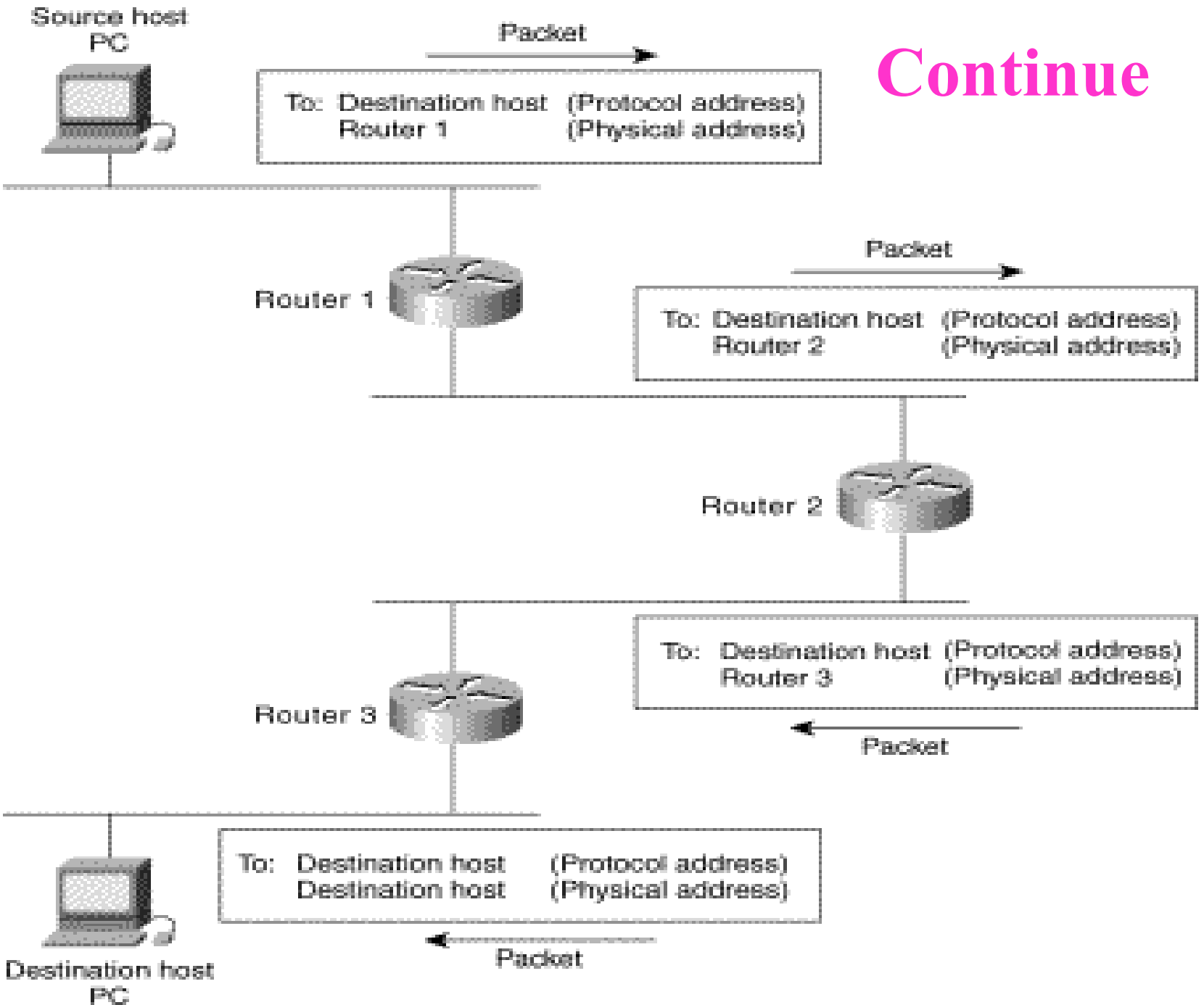


- Exposed terminals
  - B sends to A, C wants to send to another terminal (not A or B)
  - C senses carrier, finds medium in use and has to wait
  - A is outside the radio range of C, therefore waiting is not necessary
  - C is “exposed” to B

Routing

- *A **router** receives a packet from a network and passes it to another network.*
- *At the Router a Routing Table is maintained which may be Static or Dynamic.*
- *A router is usually attached to several networks. When it receives a packet, to which network should it pass the packet? The decision is based on optimization: which of the available pathways is the optimum pathway?*
- *Routing* is the act of moving information across an internetwork from a source to a destination.
- Along the way, at least one intermediate node typically is encountered.
- Routing involves two basic activities: determining optimal routing paths and transporting information groups (typically called packets) through an internetwork.

Continue


Source host
PC
Packet
To: Destination host (Protocol address)
Router 1 (Physical address)
Router 1
Packet
To: Destination host (Protocol address)
Router 2 (Physical address)
Router 2
To: Destination host (Protocol address)
Router 3 (Physical address)
Packet
Router 3
To: Destination host (Protocol address)
Destination host (Physical address)
Packet
Destination host
PC

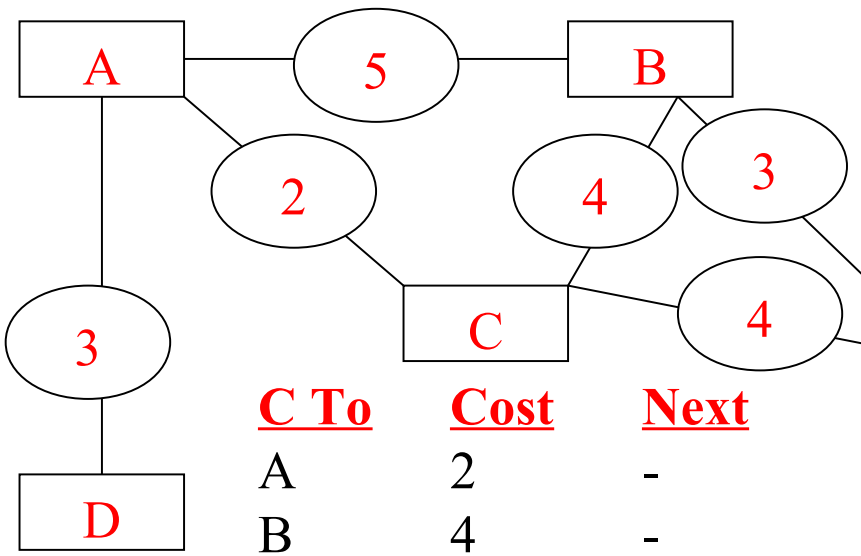
Routing Example

A To	Cost	Next
A	0	-
B	5	-
C	2	-
D	3	-
E	6	C

A's Table

D To	Cost	Next
A	3	-
B	8	A
C	5	A
D	0	-
E	9	A

D's Table



C To	Cost	Next
A	2	-
B	4	-
C	0	-
D	5	A
E	4	-

C's Table

B To	Cost	Next
A	5	-
B	0	-
C	4	-
D	8	A
E	3	-

B's Table

E To	Cost	Next
A	6	C
B	3	-
C	4	-
D	9	C
E	0	-

E's Table

Continue

- Routing is often contrasted with bridging, which might seem to accomplish precisely the same thing to the casual observer.
- The primary difference between the two is that bridging occurs at Layer 2 (the data link layer) of the OSI reference model, whereas routing occurs at Layer 3 (the network layer).
- This distinction provides routing and bridging with different information to use in the process of moving information from source to destination, so the two functions accomplish their tasks in different ways.

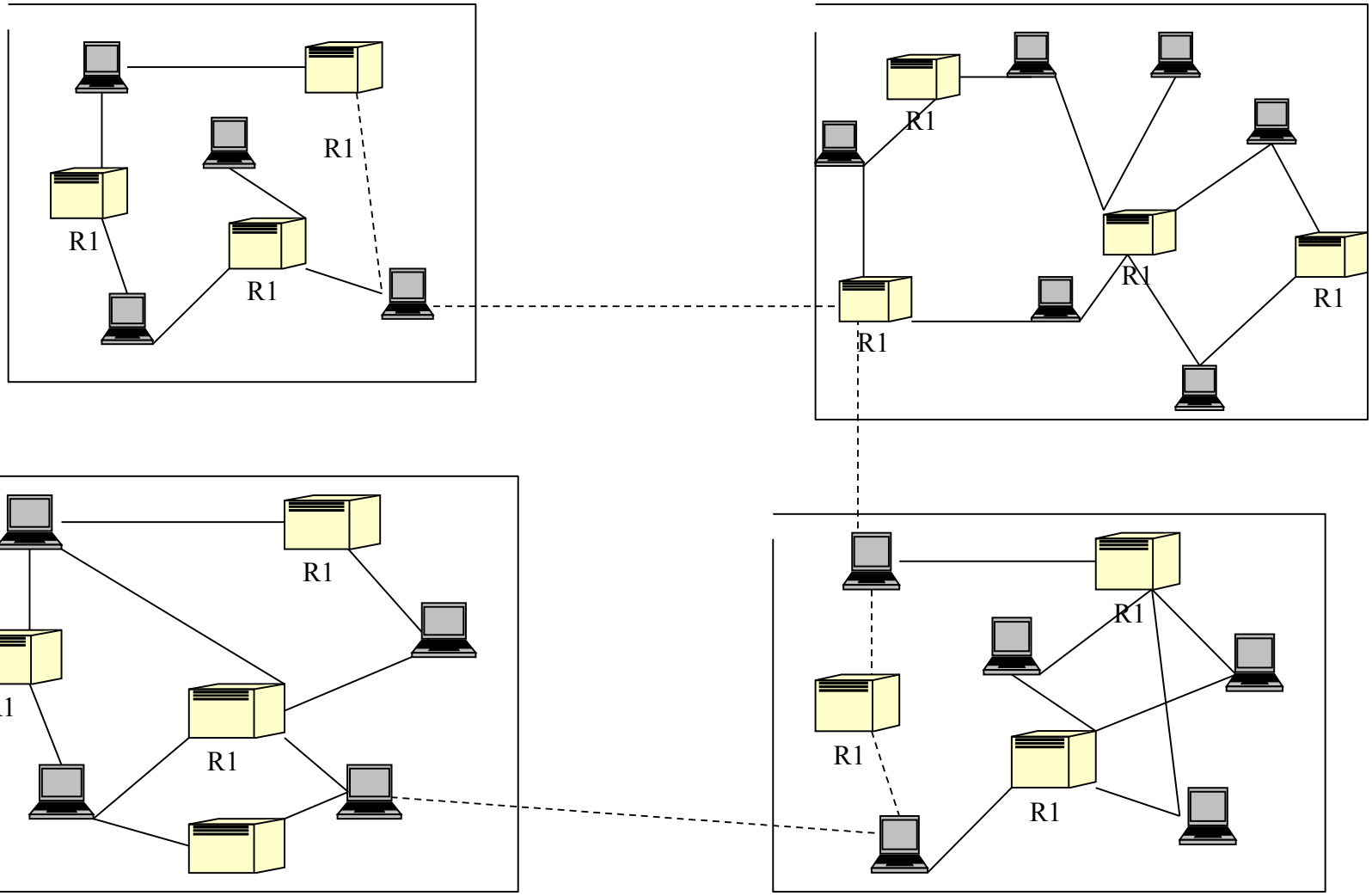
Continue

- The International Organization for Standardization (ISO) has developed a hierarchical terminology that is useful in describing routing.
- Using this terminology, network devices without the capability to forward packets between subnetworks are called *end systems (ESs)*, whereas network devices with these capabilities are called *intermediate systems (ISs)*.
- ISs are further divided into those that can communicate within routing domains (*intradomain ISs*) and those that communicate both within and between routing domains (*interdomain ISs*).

Continue

- A **routing domain** generally is considered a portion of an internetwork under common administrative authority that is regulated by a particular set of administrative guidelines.
- An **autonomous system (AS)** is a group of networks and routers under the authority of a single administration.
- Routing inside an autonomous system is referred to as intradomain routing.
- Routing between autonomous systems is referred to as interdomain routing. Each autonomous system can choose one or more intradomain routing protocols to handle routing inside the autonomous systems.

Autonomous Systems



Routing and Mobility

- Finding a path from a source to a destination
- Issues
  - Frequent route changes
    - amount of data transferred between route changes may be much smaller than traditional networks
  - Route changes may be related to host movement
  - Low bandwidth links
- Goal of routing protocols
  - decrease routing-related overhead
  - find short routes
  - find “stable” routes (despite mobility)

Protocol Trade-offs

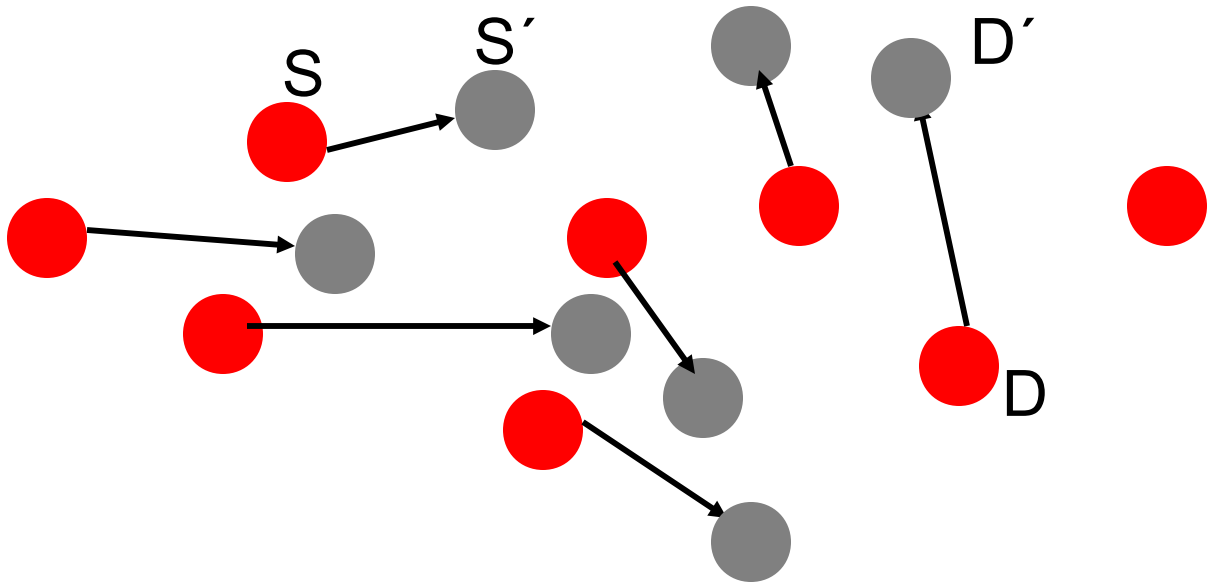
- Reactive protocols
  - Lower overhead since routes are determined on demand
  - Significant delay in route determination
  - Employ flooding (global search)
  - Control traffic may be bursty

- Which approach achieves a better trade-off depends on the traffic and mobility patterns

Reactive Routing Protocols

Dynamic Source Routing (DSR)

The Routing Problem

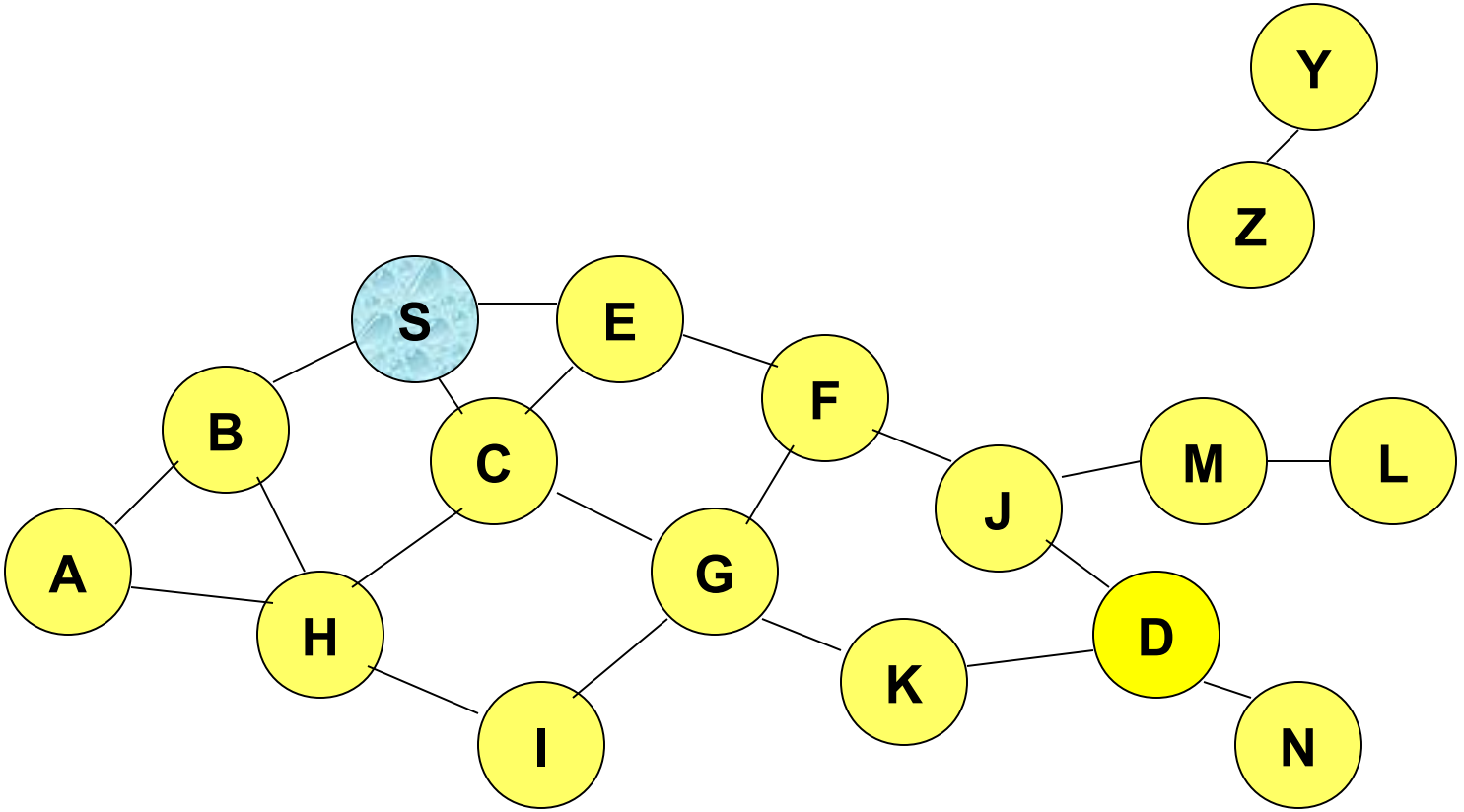


- The routing problem is to find a route from S to D when some or all of the nodes are mobile.

Dynamic Source Routing (DSR)

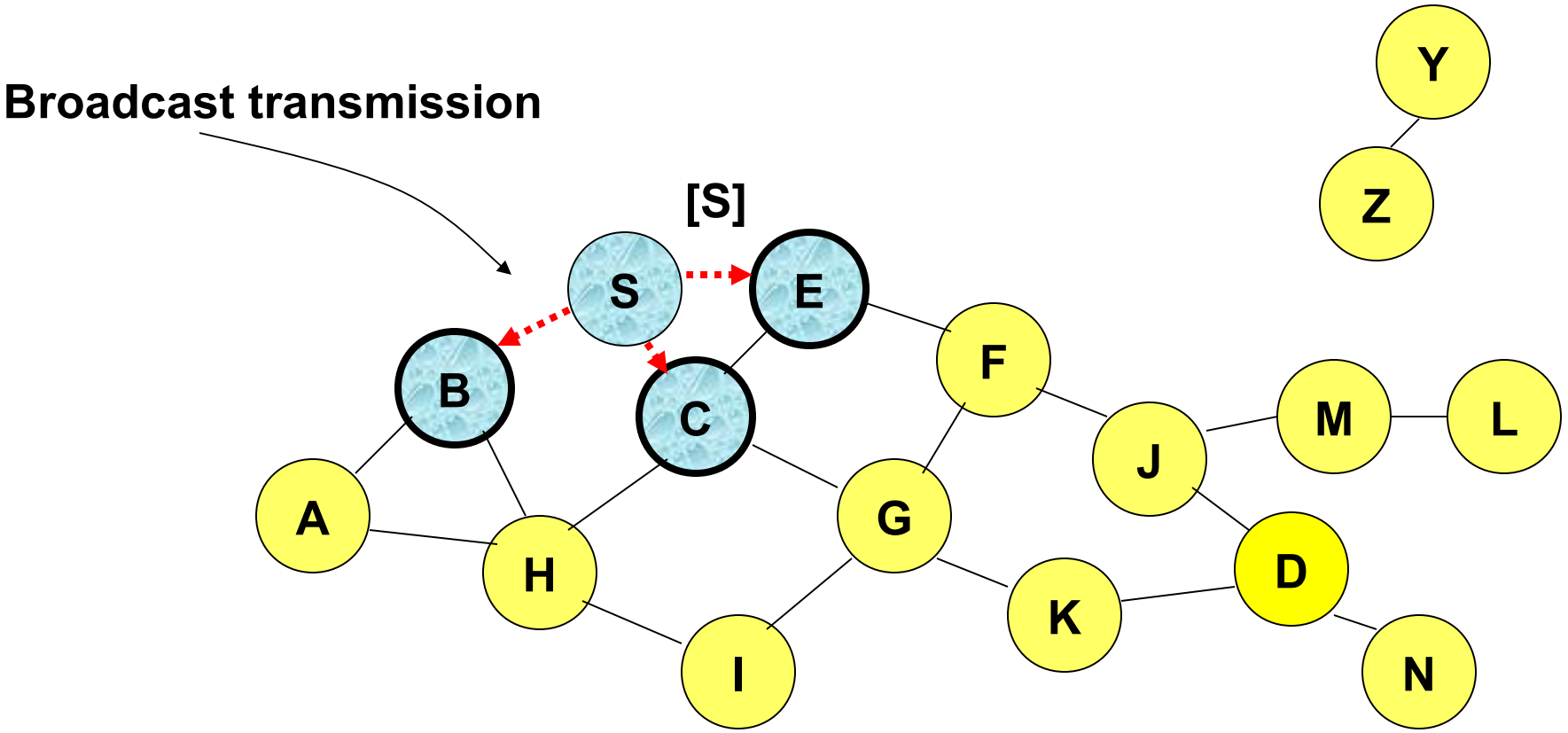
- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a route discovery
- Source node S floods Route Request (RREQ)
- Each node *appends own identifier* when forwarding RREQ

Route Discovery in DSR



Represents a node that has received RREQ for D from S

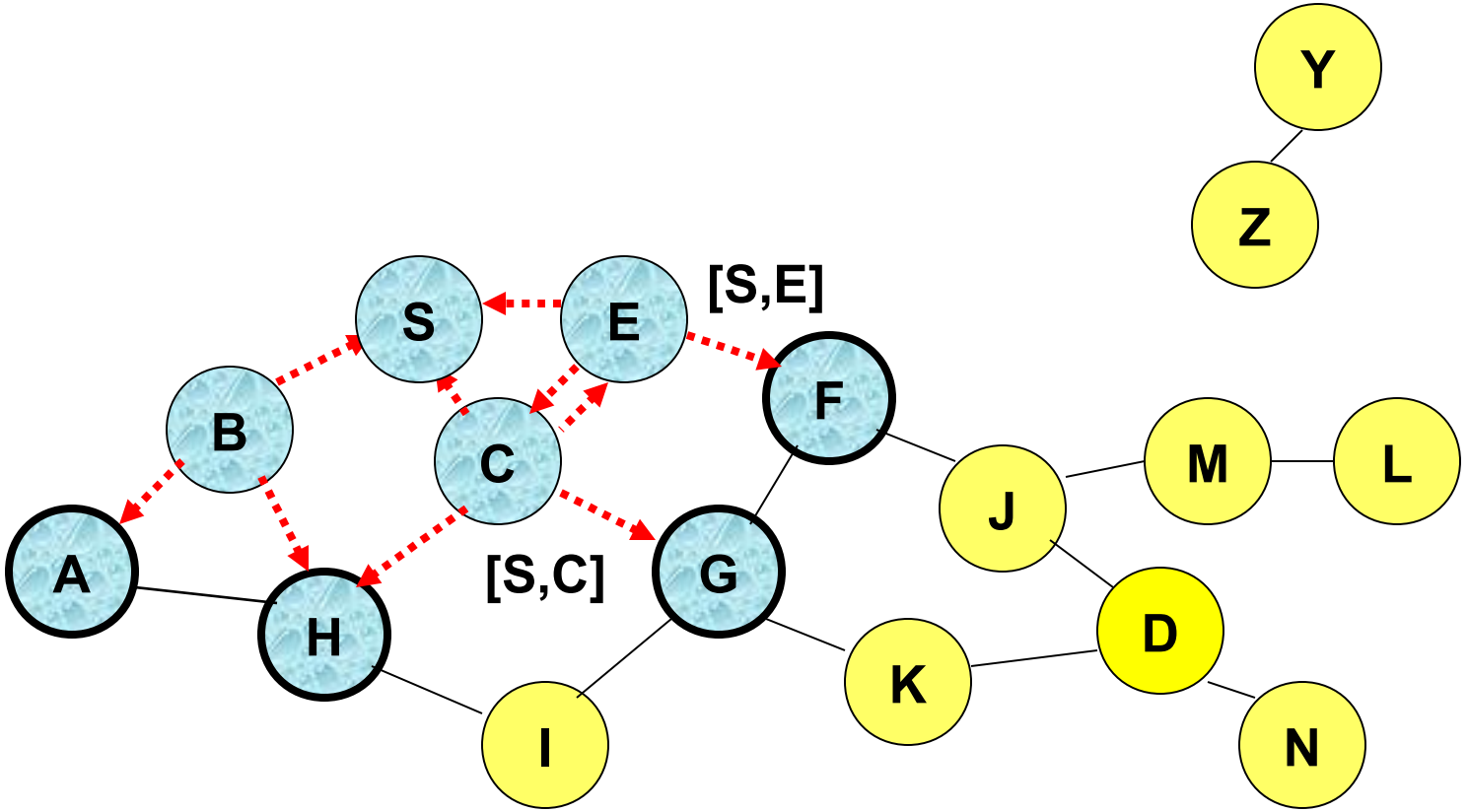
Route Discovery in DSR



Represents transmission of RREQ

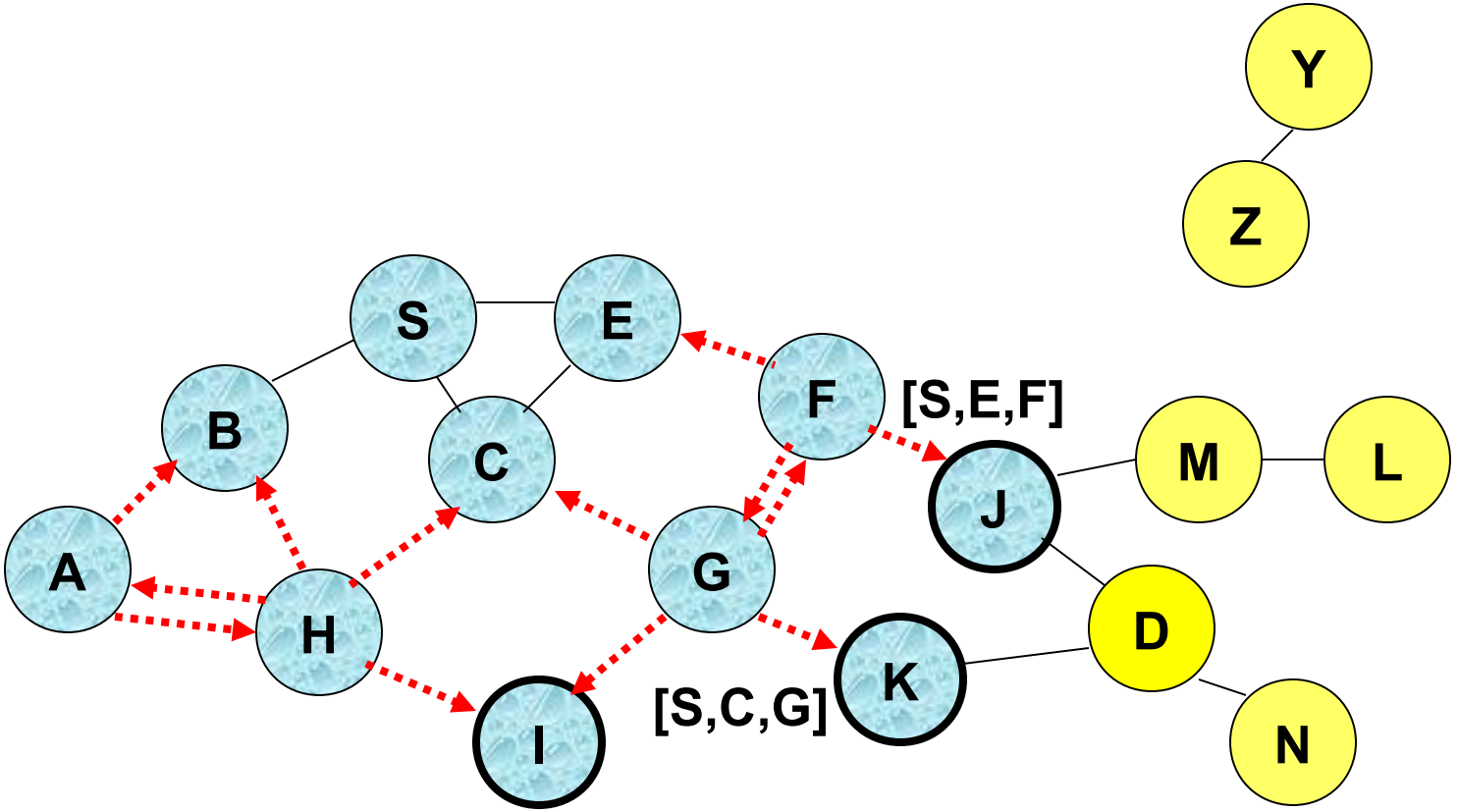
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



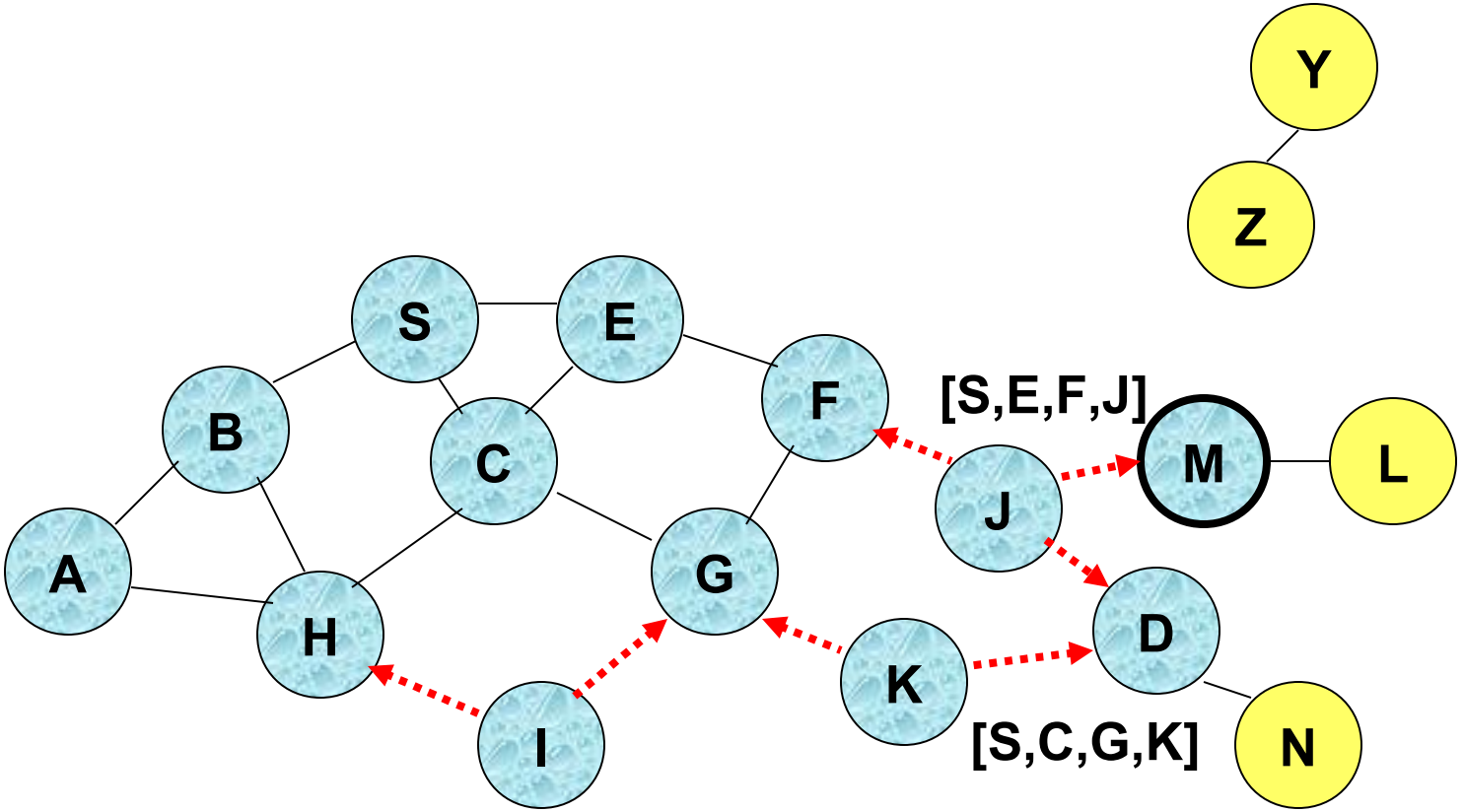
- **Node H receives packet RREQ from two neighbors:**
  potential for collision

Route Discovery in DSR



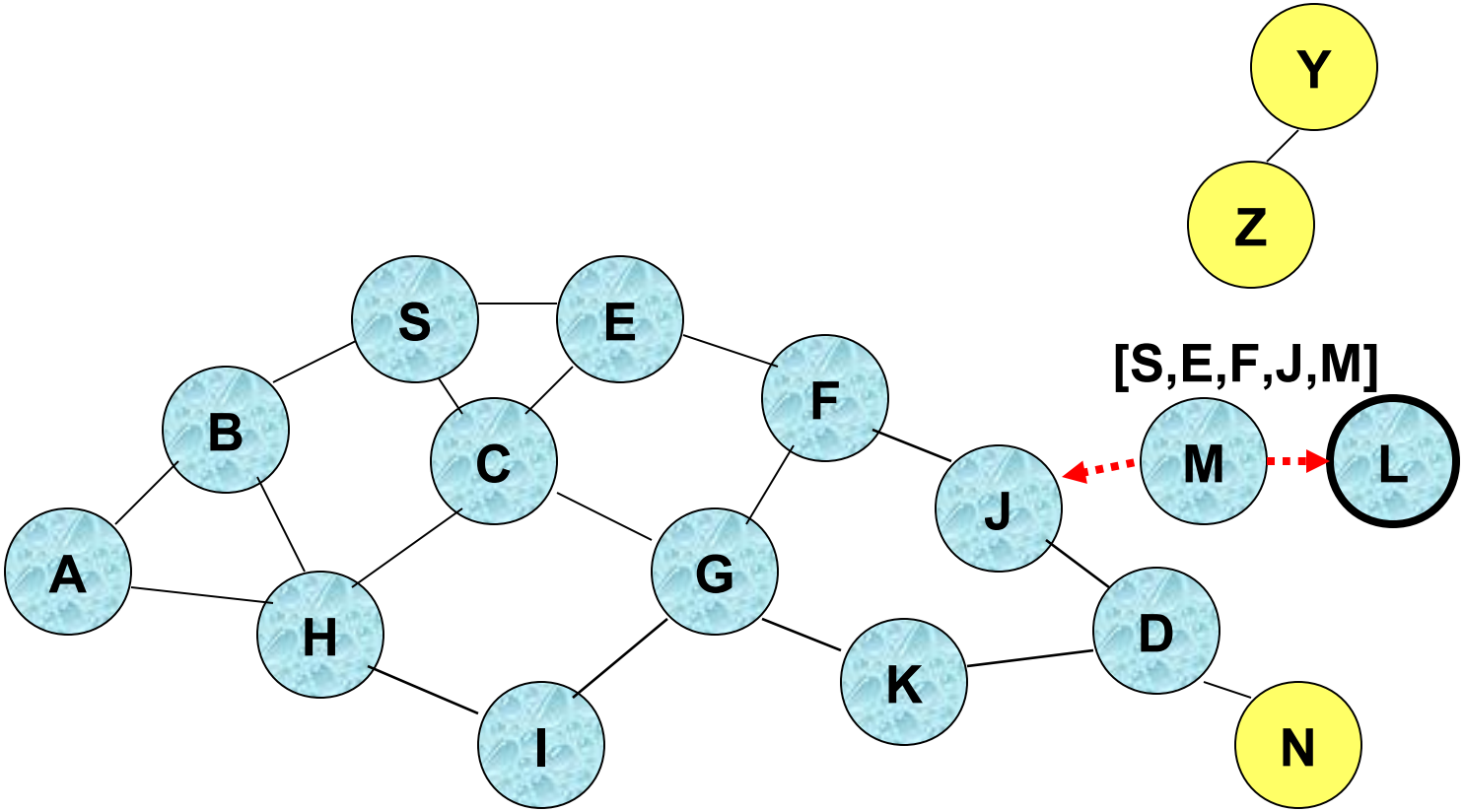
- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

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

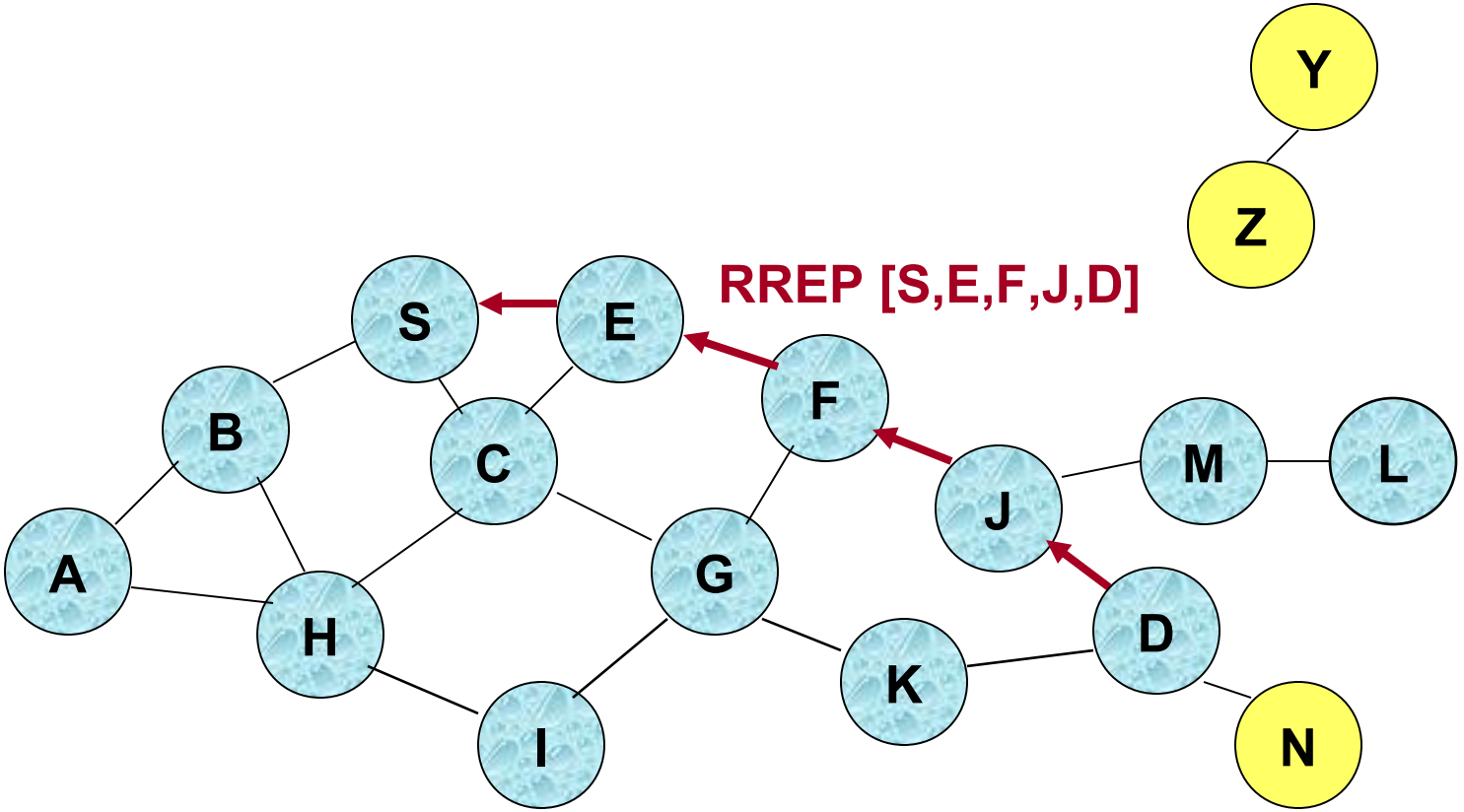


- Node D **does not forward** RREQ, because node D is the **intended target** of the route discovery

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

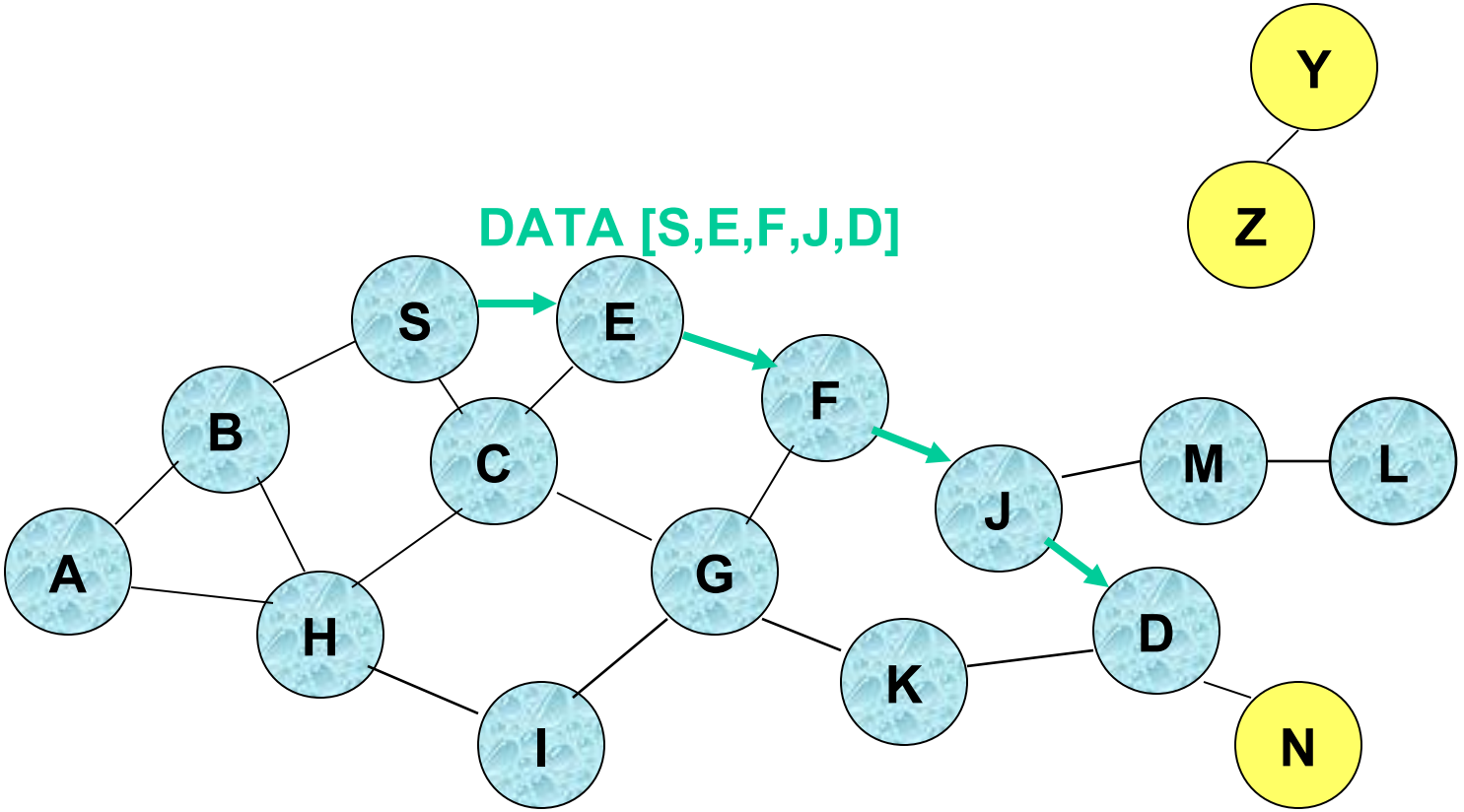


Represents RREP control message

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

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
- Problem: Stale caches may increase overheads

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
- Potential 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
- Stale caches will lead to increased overhead