Light Infrastructure Networks

UTC

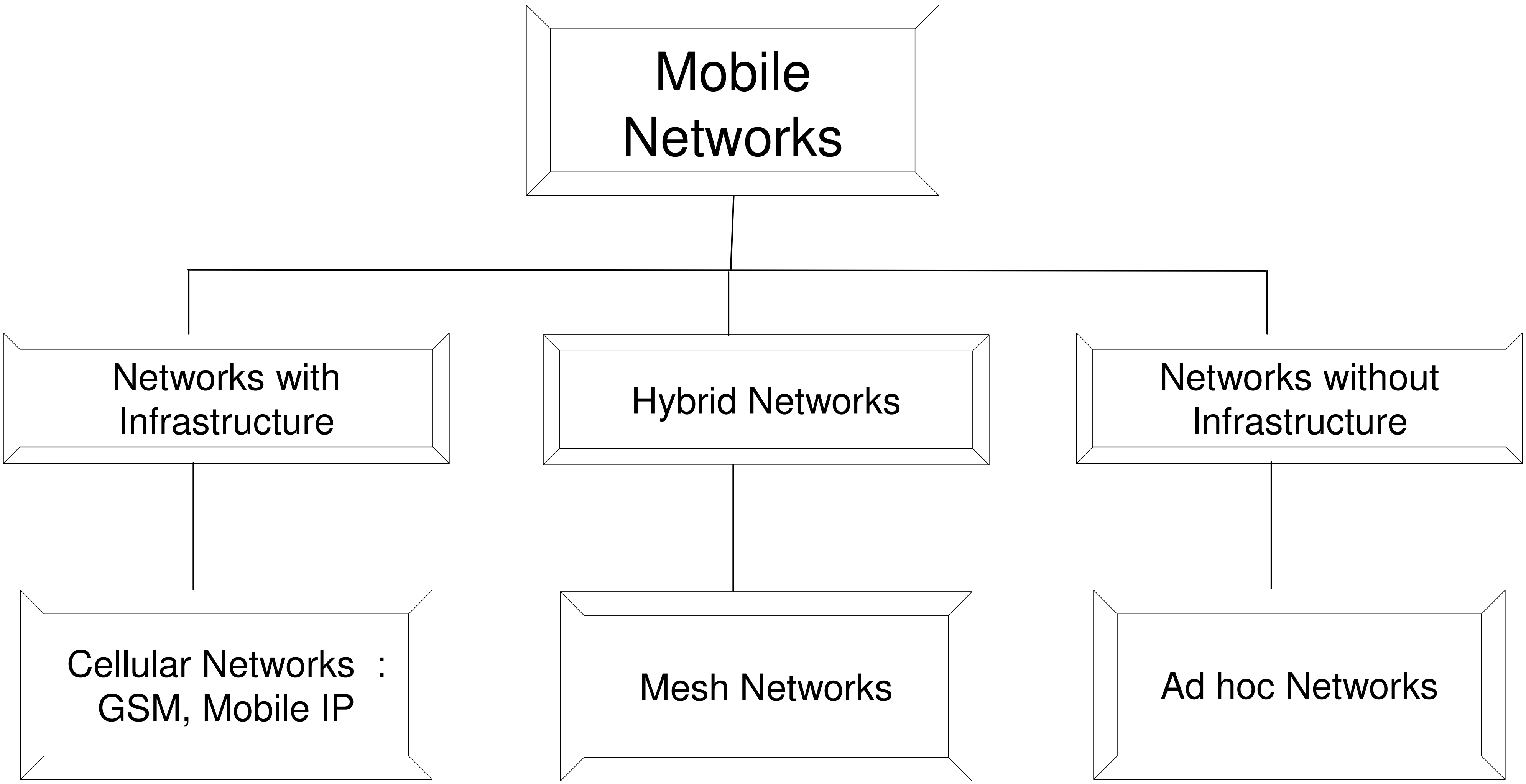
24/11/2008

Sidi-Mohammed Senouci
France Telecom R&D

Course Outlinse

- ➔ **Introduction**
- ➔ **Wireless Ad hoc Networks**
- ➔ **Wireless Mess Networks and IEEE 802.11s**
- ➔ **WIMAX and IEEE 802.16**
- ➔ **Vehicular Communications**

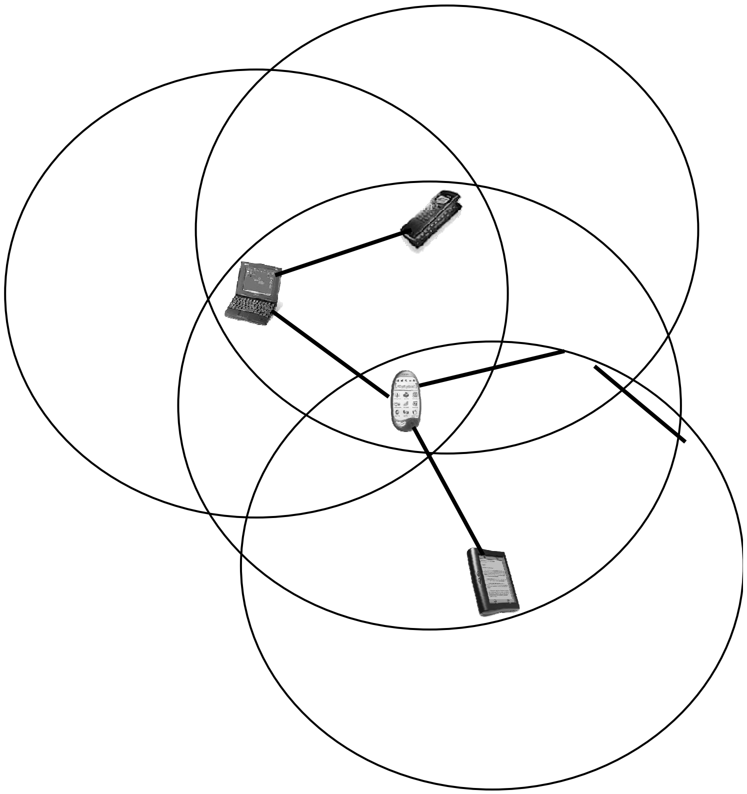
Introduction



Wireless Ad hoc Networks

Ad Hoc Networks - Definitions

- ➔ **An ad hoc wireless network is a collection of two or more devices equipped with wireless communications capability**
- ➔ **Such devices can communicate with another node that is immediately within their radio range or one that is outside their radio range using intermediate nodes**
- ➔ **Dynamic network topology**
  - Mobility causes route changes



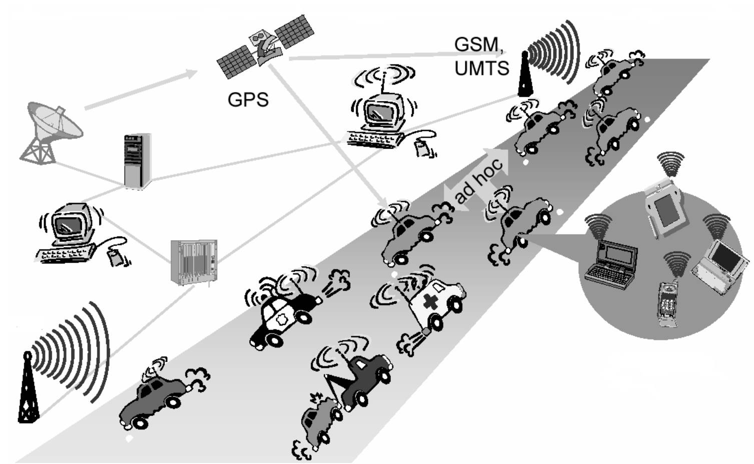
Why Ad Hoc Networks ?

➔ **Some advantages**

- Ease and speed of deployment
- Low cost: infrastructureless
- Self-organizing and adaptive

Ad hoc Networks – Applications

- **Military environments**
  - soldiers, tanks, planes
- **Personal area networking**
  - cell phone, laptop, ear phone, wrist watch
- **Civilian environments**
  - IVC (cooperative driving, safety driving, and comfort services)
  - Meeting rooms, sport stadiums, airports, subway..
  - Sensor networks
- **Emergency operations**
  - search-and-rescue, earthquake, fire fighting



Many Variations

➔ **Fully Symmetric Environment**
- all nodes have identical capabilities and responsibilities

➔ **Asymmetric Capabilities**
- transmission ranges and radios may differ
- battery life at different nodes may differ
- processing capacity may be different at different nodes
- speed of movement

➔ **Asymmetric Responsibilities**
- only some nodes may route packets
- some nodes may act as leaders of nearby nodes (e.g., cluster head)

Many Variations

- ➔ **Mobility may be different (application dependent)**
  - speed
  - predictability
    - direction of movement
    - pattern of movement
      - *cars movements (highway, city, …)*
      - *kids playing*
      - *military movements*
      - *personal area network*
      - *people sitting at an airport lounge*
- ➔ **May co-exist (and co-operate) with an infrastructure-based network -> Hybrid**

Challenges

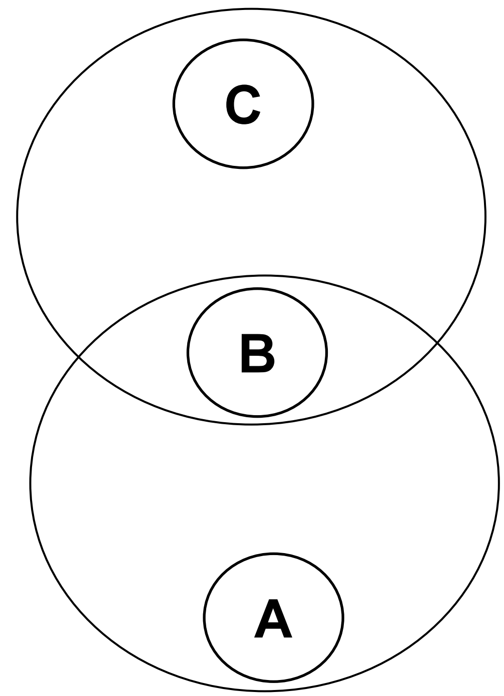
- ➔ **Limited resources**
  - shared bandwidth
    - Each packet is received by all nodes -> bandwidth ↓
  - Battery constraints
- ➔ **Mobility-induced**
  - route changes
  - packet losses
  - frequent network partitions
- ➔ **Broadcast nature of the wireless medium**
  - Hidden terminal problem (see next slide) and interferences (more errors)
  - Packet losses due to shared medium (interference, collision, …)
  - Ease of snooping on wireless transmissions (security hazard)

Significant research activity

Hidden Terminal Problem

➔ Problem

- A and C cannot hear each other.
- A sends to B, C cannot receive A.
- C wants to send to B, C senses a “free” medium (carrier sense fails)
- Collision occurs at B.
- A is “hidden” for C.



Routing
in
Mobile Ad Hoc Networks

Why is Routing in MANET different ?

- **Host mobility**
  - Rate of link failure/repair may be high when nodes move fast
- **New performance criteria may be used**
  - route stability despite mobility
  - energy consumption
  - quality of the links
- **Many protocols have been proposed**
  - Some have been invented specifically for MANET
  - Others are adapted from previously proposed protocols for wired networks
  - No single protocol works well in all environments
    - Some attempts made to develop adaptive protocols

Routing Protocols

➔ **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**

Trade-Off

➔ **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**

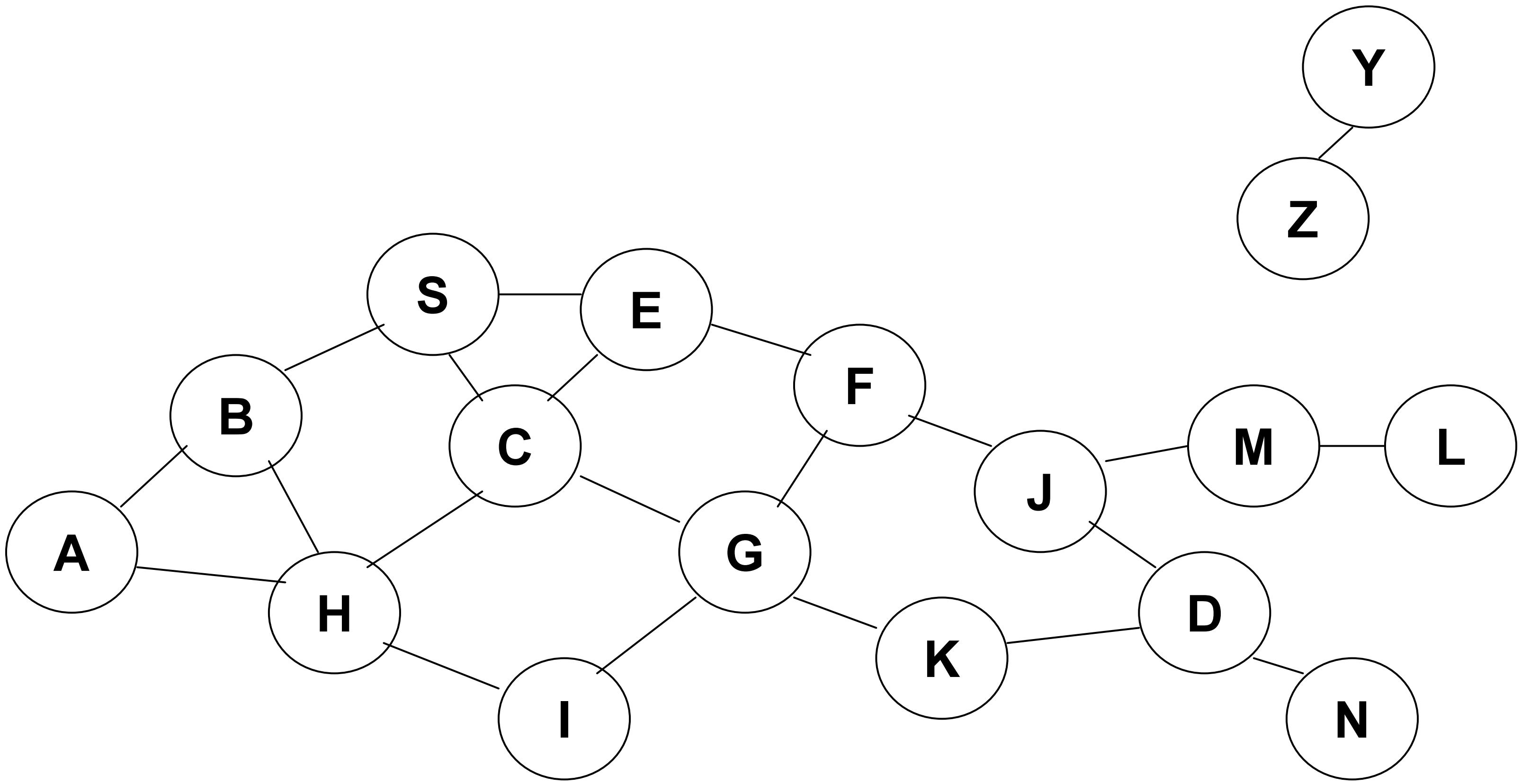
- Reactive protocols may have lower overhead since routes are determined only if needed
- Proactive protocols can (but not necessarily) result in higher overhead due to continuous route updating

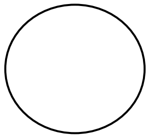
➔ **Which approach achieves a better trade-off depends on the traffic and mobility patterns**

Dynamic Source Routing (DSR) [Johnson96]

- **Reactive protocol**
- **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**

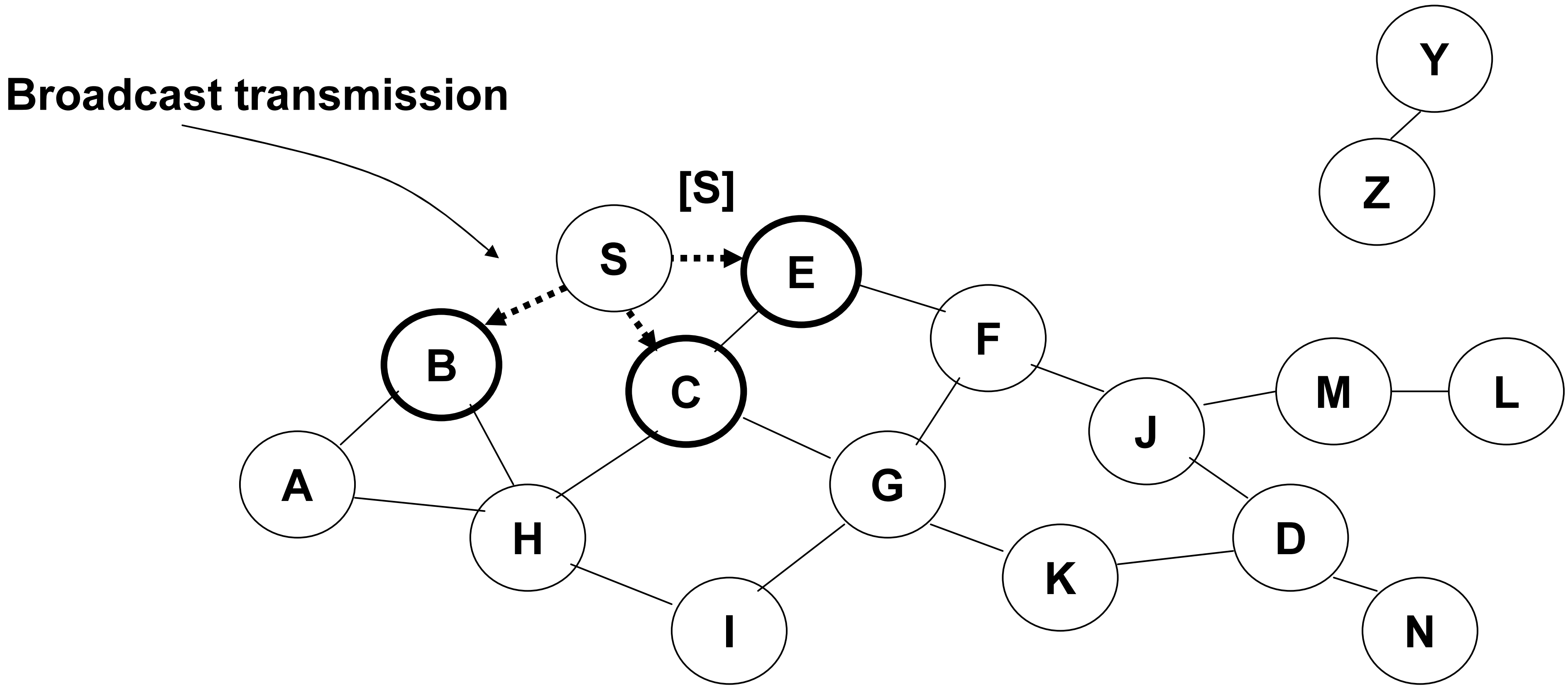
Route Discovery in DSR





Represents a node that has received RREQ for D from S

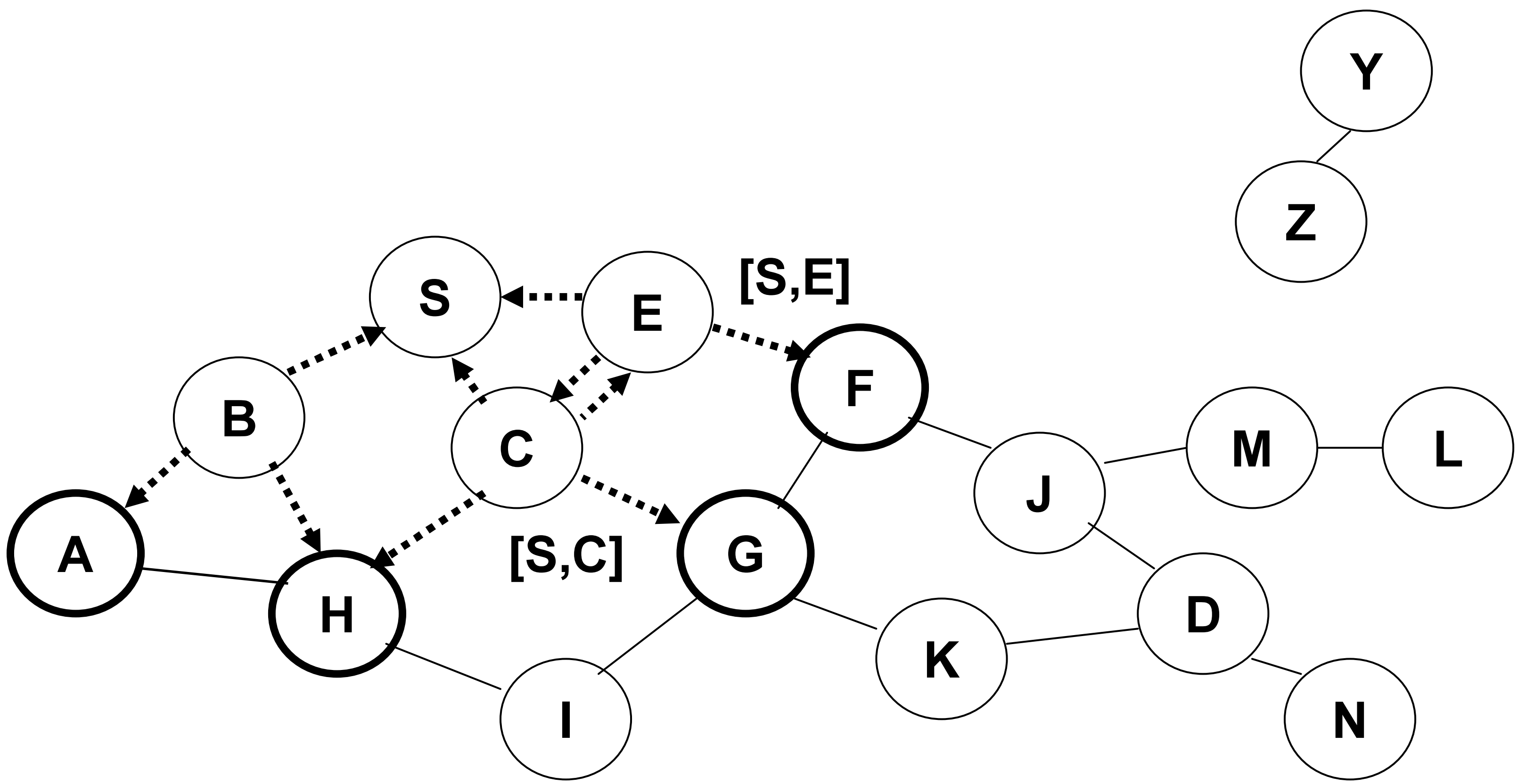
Route Discovery in DSR



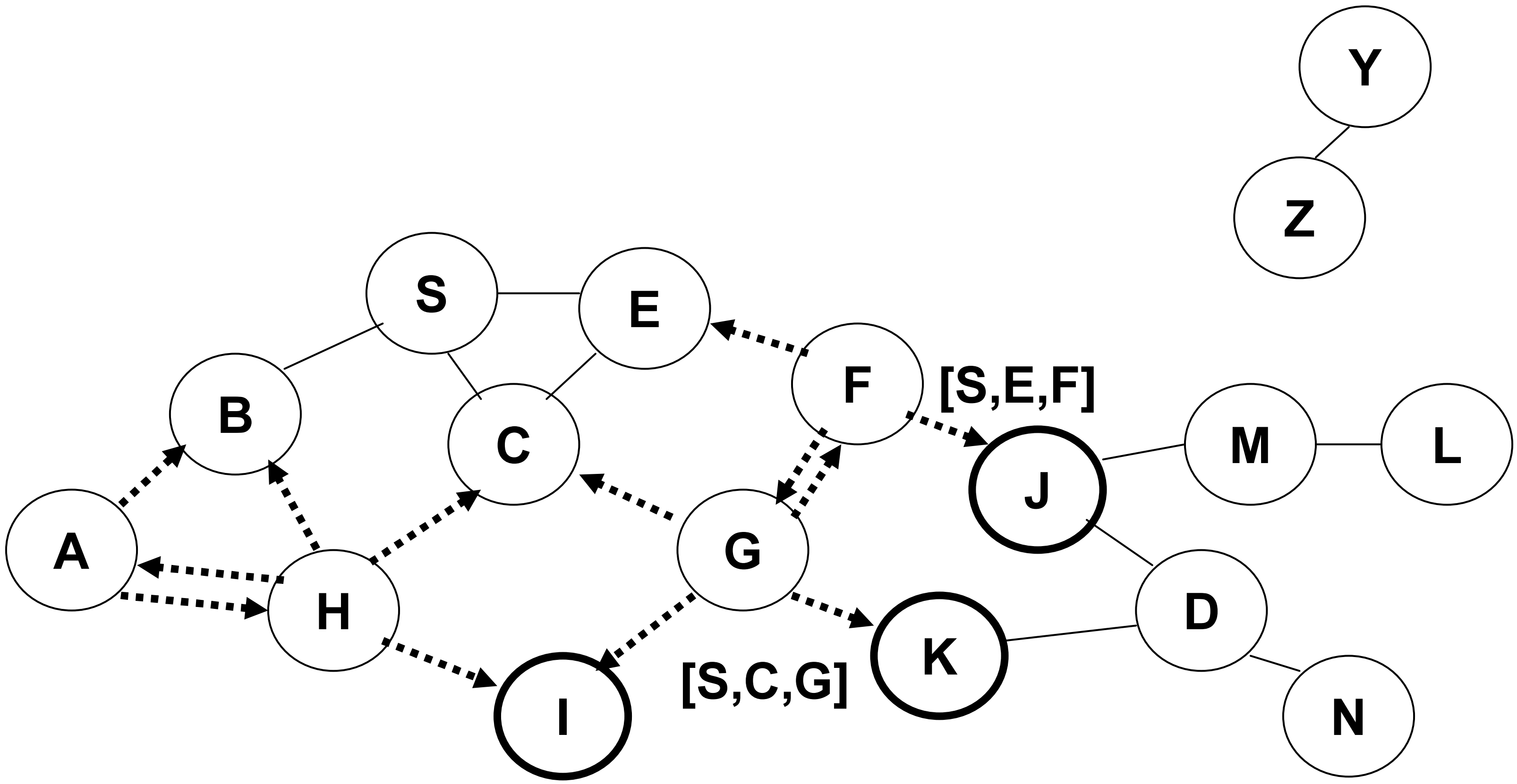
Represents transmission of RREQ

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

Route Discovery in DSR

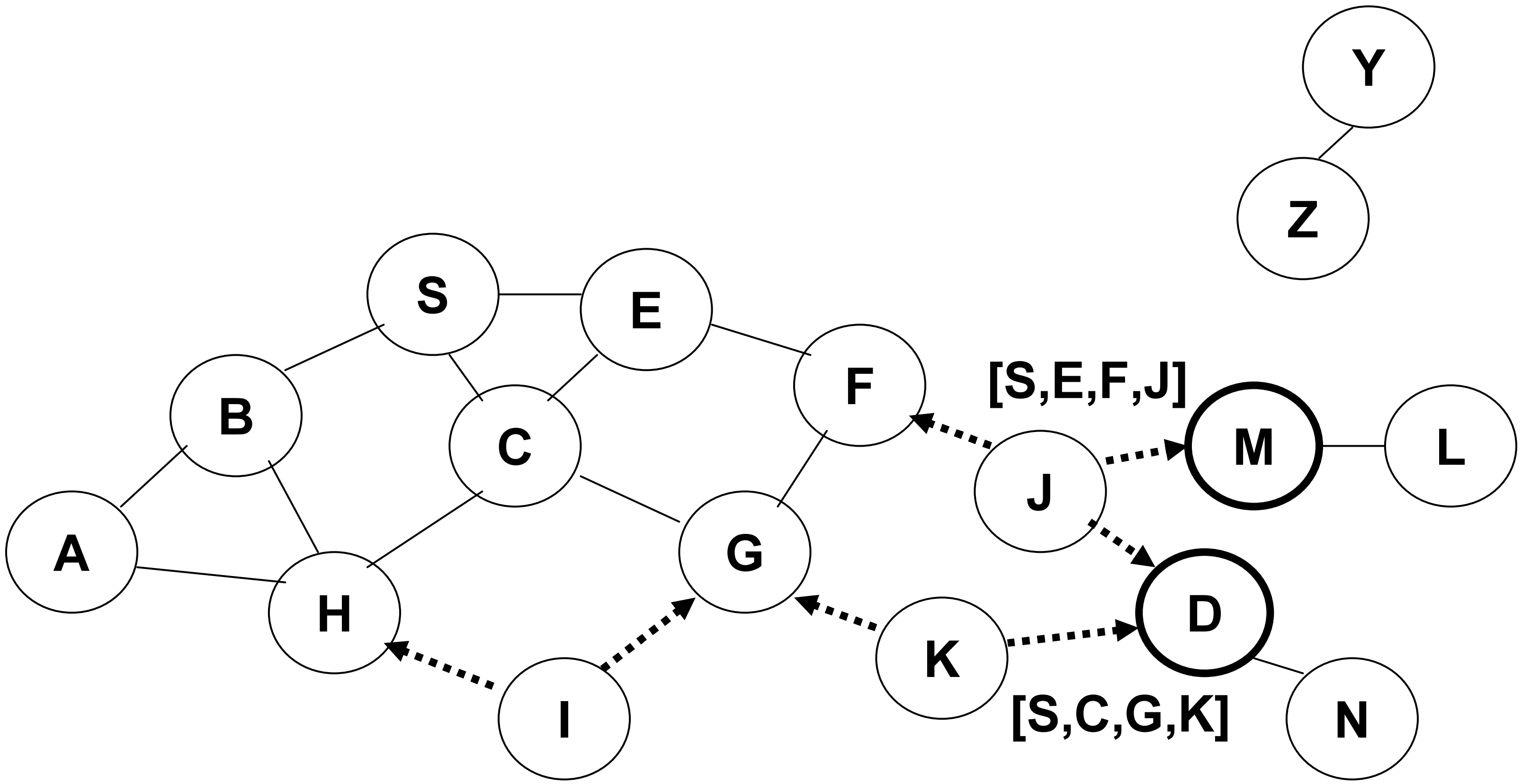


Route Discovery in DSR



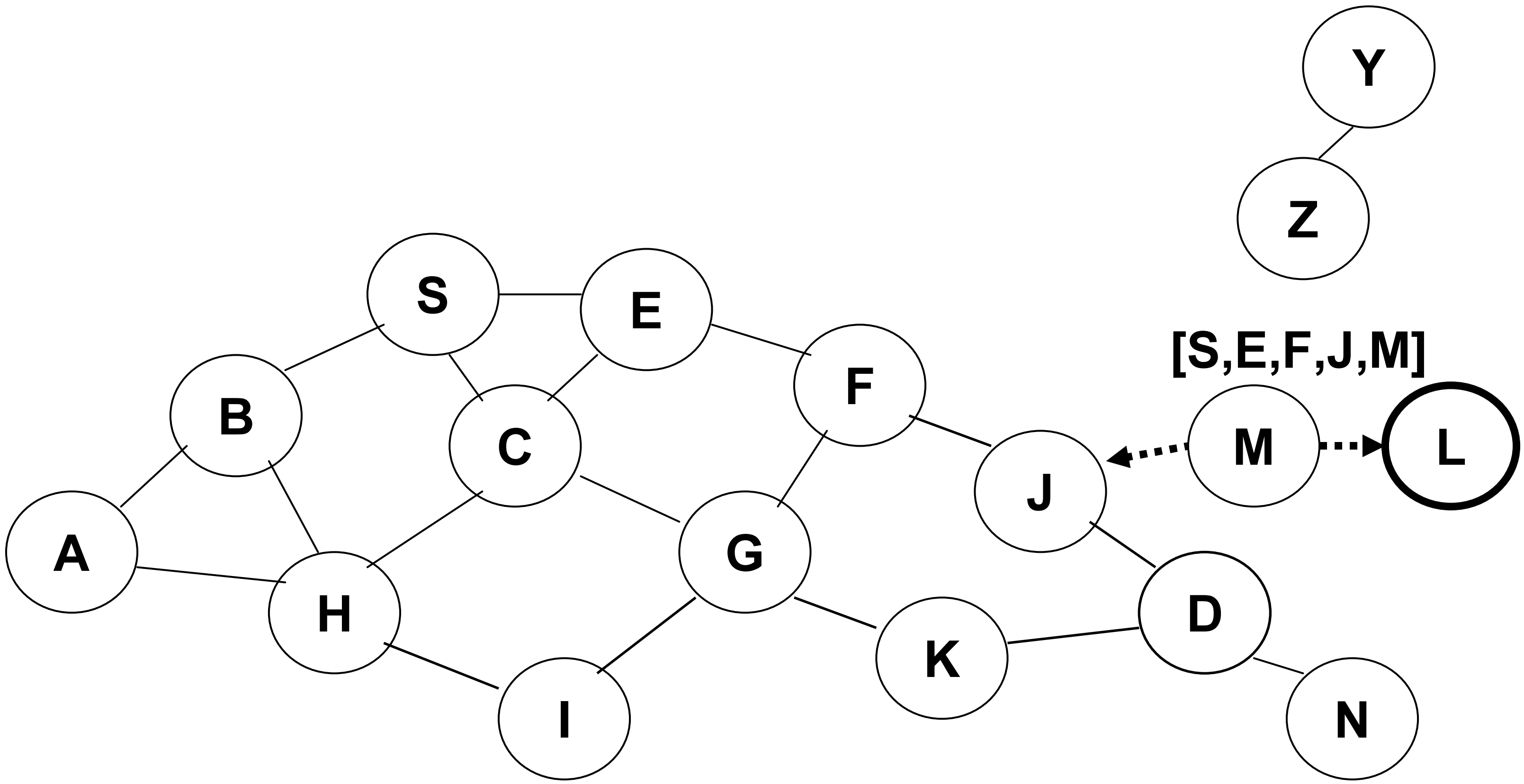
- **Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once**

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

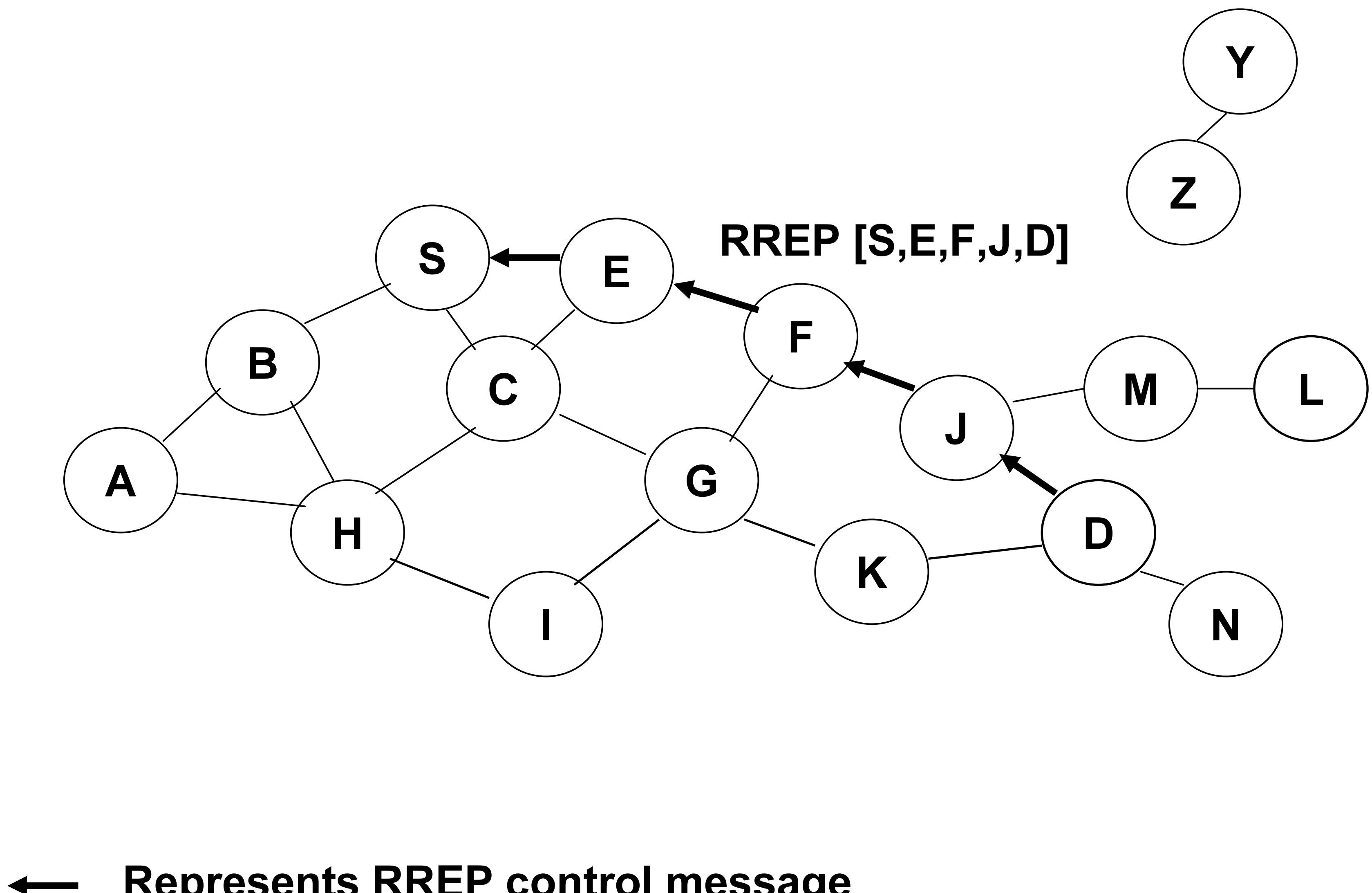


- **Node D does not forward RREQ, because node D is the intended target of the route discovery**

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**

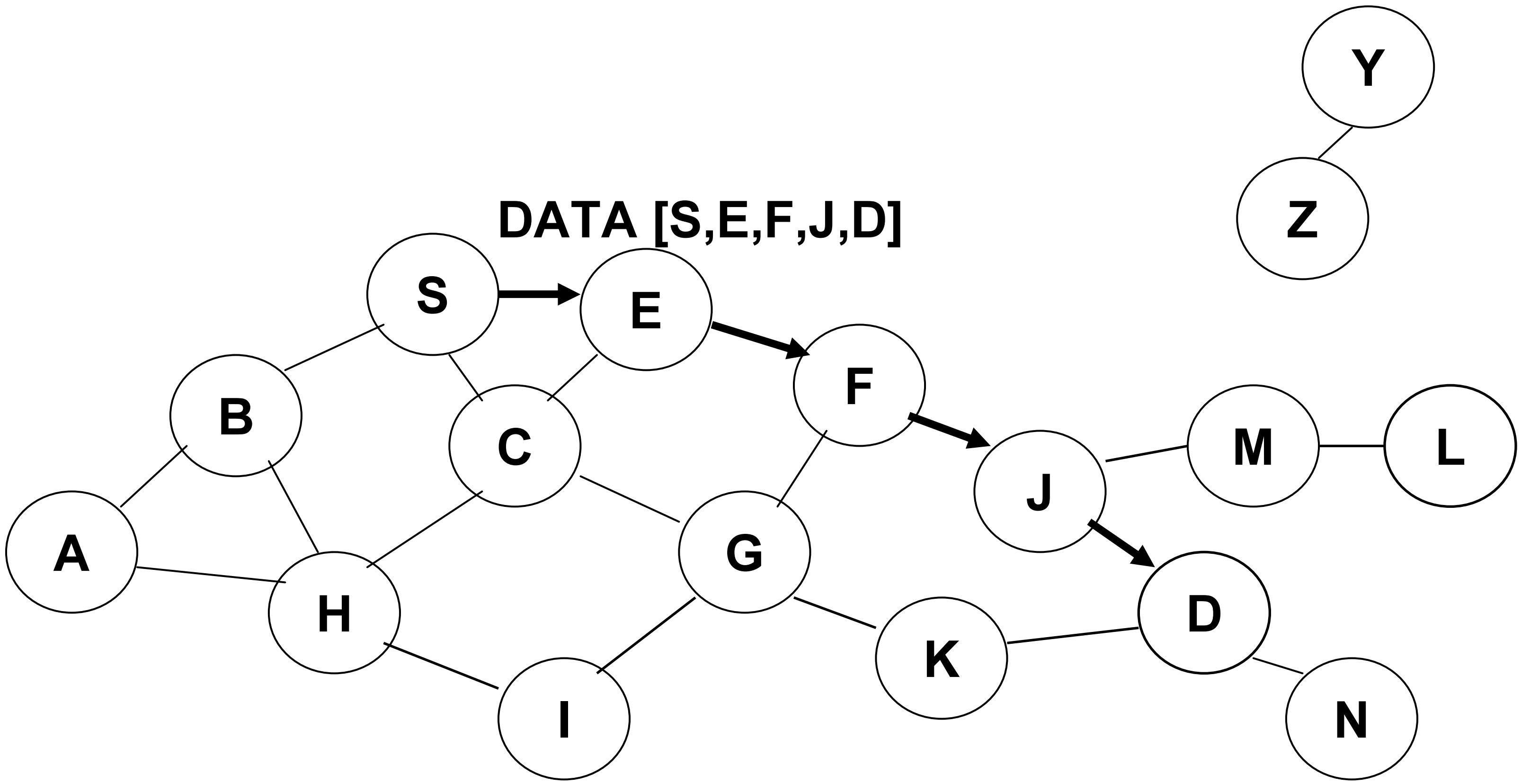
- Unless node D already knows a route to node S
- If a route discovery is initiated by D for a route to S, then the Route Reply is piggybacked (added) on the Route Request from D.

➔ **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

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

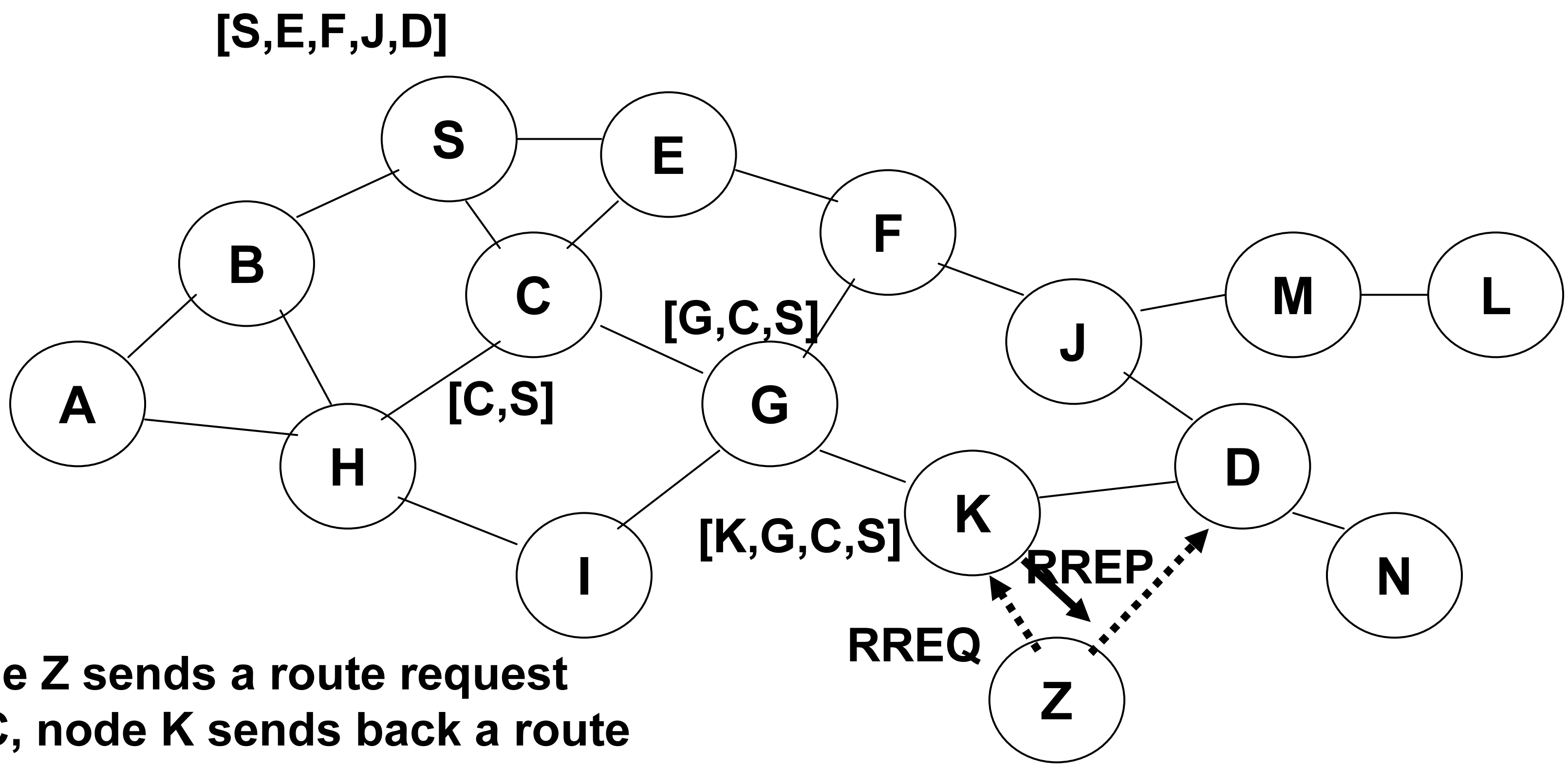
Use of Route Caching

- **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**

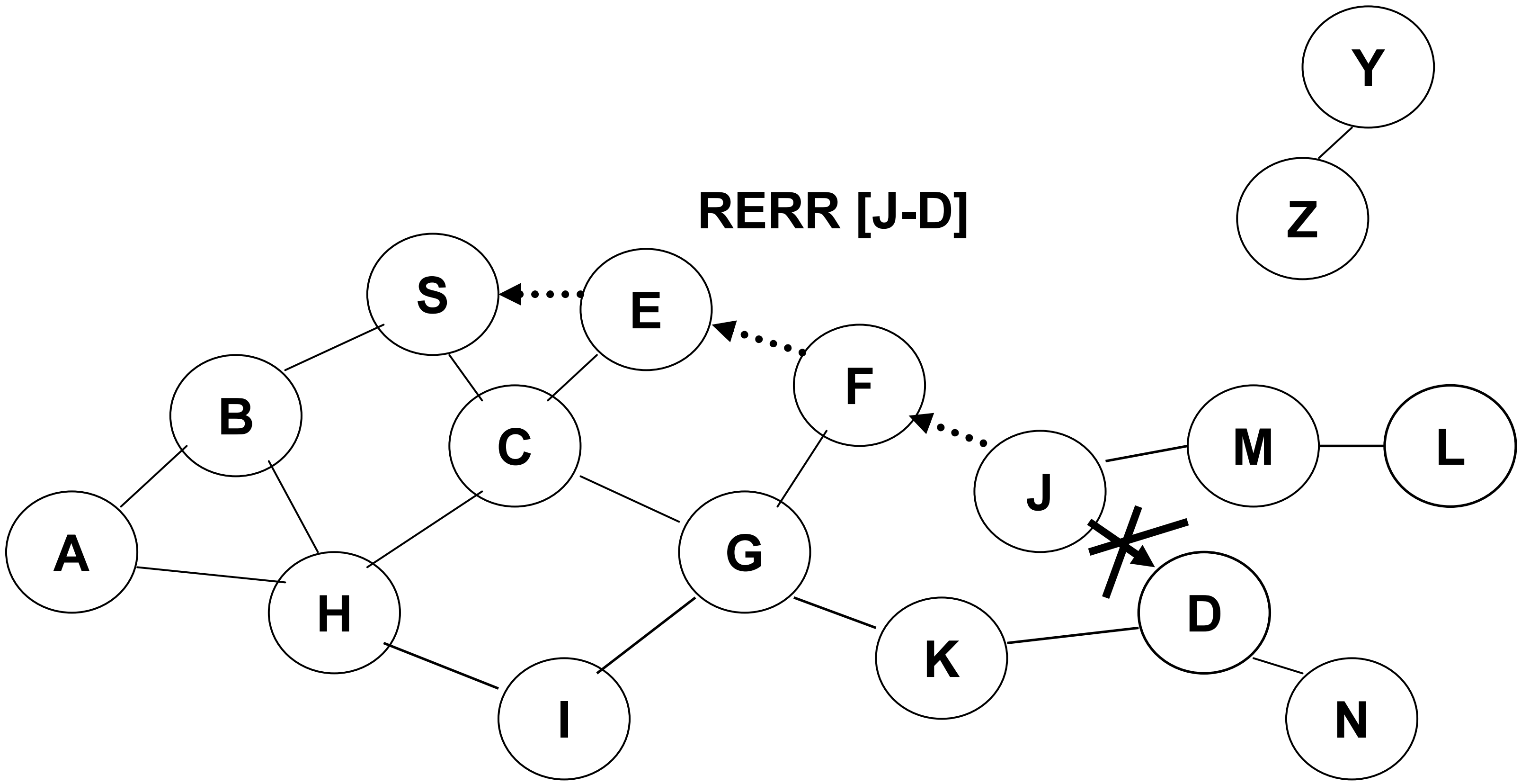
- **Use of route cache**
  - can speed up route discovery
  - can reduce propagation of route requests

Use of Route Caching



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 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

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 produce many routes to the destination, due to intermediate nodes replying from local caches**

Dynamic Source Routing: Disadvantages

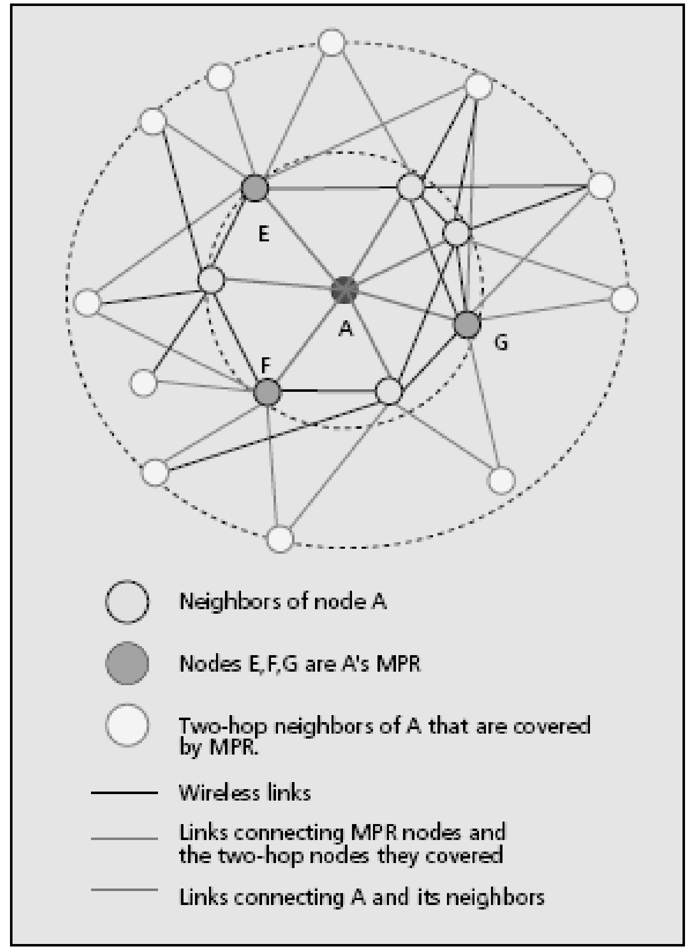
- ➔ **Packet header size grows with route length due to source routing**
- ➔ **Flood of route requests may potentially reach all nodes in the network**
- ➔ **An intermediate node may send Route Reply using a stale (old) cached route, thus polluting other caches**
  - This problem can be eased if some mechanism to purge (potentially) invalid cached routes is incorporated

Link State Routing (LSR) [Huitema95]

- **Proactive protocol**
- **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) [Jacquet00ietf,Jacquet99Inria]

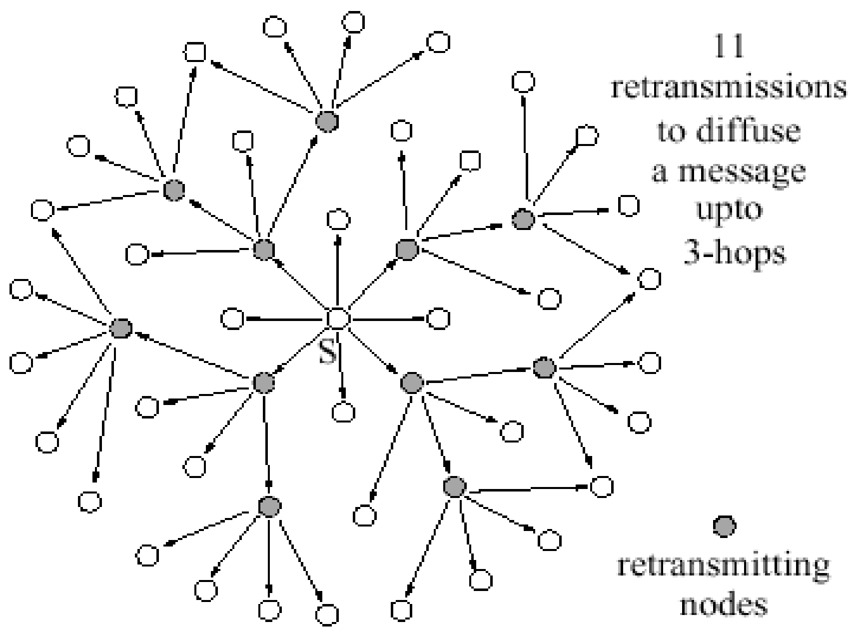
- ➔ **The overhead of flooding link state information is reduced by requiring fewer nodes to forward the information**
  - ●a broadcast from node A is only forwarded by its *multipoint relays (MPR)*
- ➔ **Multipoint relays of node A are its neighbors such that each two-hop neighbor of A is a one-hop neighbor of at least one multipoint relay of A**
  - ●Each node transmits its neighbor list in periodic beacons (HELLO messages), so that all nodes can know their 2-hop neighbors, in order to choose the multipoint relays



OLSR

- ➔ **OLSR floods information through the multipoint relays**

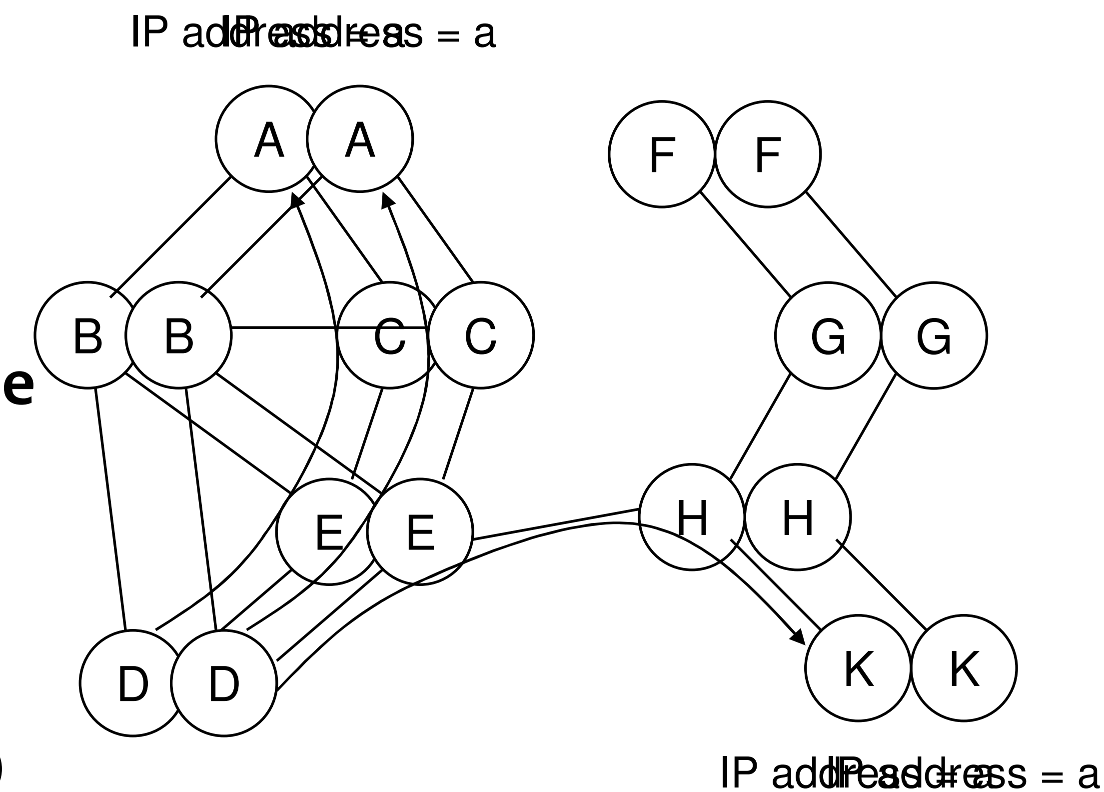
- ➔ **Routes used by OLSR only include multipoint relays as intermediate nodes**



Other schemes: Auto-configuration, security, MAC Layer Misbehavior

1. Address Auto-configuration

- ➔ **IP address is a finite and conflict resource**
- ➔ **IP auto-configuration is desirable**
- ➔ **How to auto-assign the address without conflicts?**
  - DHCP is not suitable
  - Solution : Duplicate Address Detection (DAD)
    - Strong DAD
    - Weak DAD



1. Duplicate Address Detection (DAD) in Ad Hoc Networks

➔ **Strong DAD [Perkins]:**

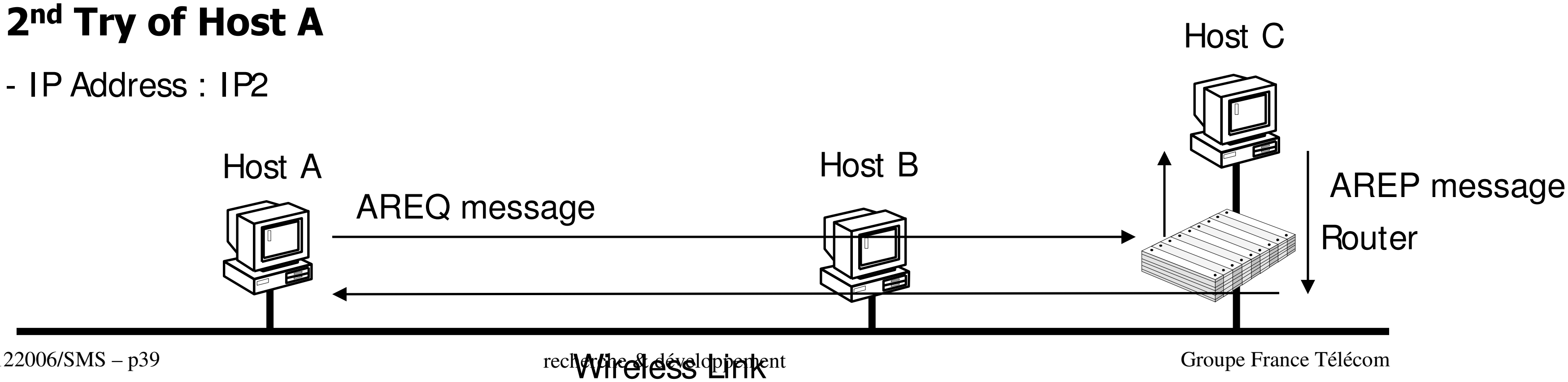
- Host picks an address randomly
- Host performs route discovery (AREQ) for the chosen address
- If a route reply (AREP) is received, address duplication is detected

1st Try of Host A

- IP Address : IP1

2nd Try of Host A

- IP Address : IP2



1. Strong DAD

- ➔ **Strong DAD is performed during the initiation of node's network interface for detecting IP address duplication in a connected MANET partition within a finite bounded time interval**
- ➔ **Not possible to guarantee strong DAD**
  - Host unreachable problem
    - Partitioning/Merging
  - Concurrent address requesting problem
    - Two nodes A and B simultaneously performs DAD process

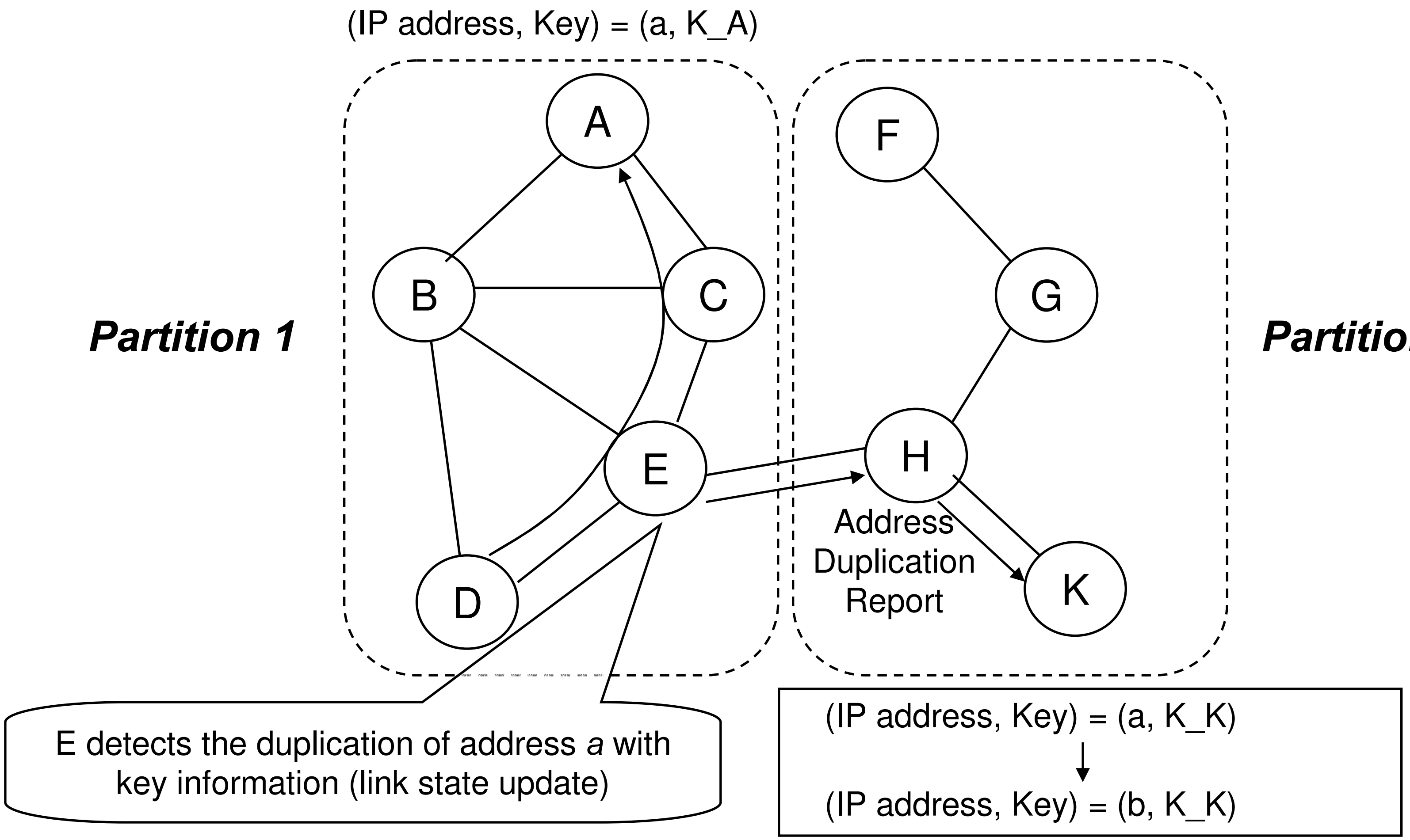
1. Weak DAD [Vaidya02MobiHoc]

➔ Weak DAD

- For detecting IP address duplication during ad hoc routing
- It can handle the address duplication by MANET partition and mergence
- Key is used for the purpose of detecting duplicate IP addresses
  - Virtual IP Address = IP Address + Key
  - Each host has a unique (with high probability) key
    - *May include MAC address, serial number, …*
  - In all routing-related packets (link state updates) IP addresses tagged by keys

1. Weak DAD

➔ Resolution of Address Conflict by Weak DAD



2. Security Issues in Mobile Ad Hoc Networks

- **Not much work in this area as yet**
  - Many of the security issues are same as those in traditional wired networks and cellular wireless

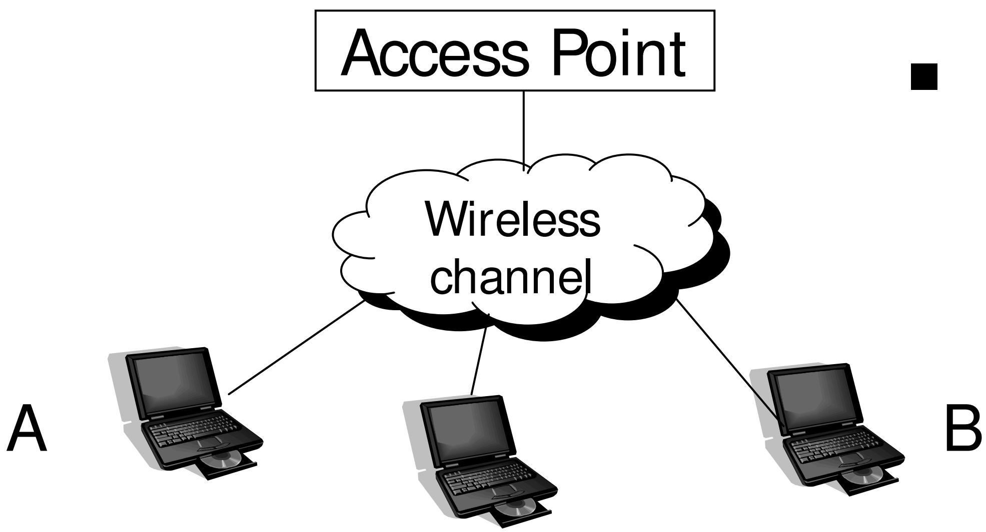
- **What's new ?**
  - Wireless medium is easy to snoop on
  - Due to ad hoc connectivity and mobility, it is hard to guarantee access to any particular node (for instance, to obtain a secret key – cryptography)
  - Easier for trouble-makers to insert themselves into a mobile ad hoc network (as compared to a wired network)

2. Secure Routing [Zhou99]

- ➔ **Attackers may inject erroneous routing information (creating routing loops)**
- ➔ **The attacker may interact with a mobile node often with the goal of draining the mobile node's battery**
  - [Zhou] suggests use of digital signatures to protect routing information and data both
    - Such schemes need a Certification Authority to manage the private-public keys
    - Establishing a Certification Authority (CA) difficult in a mobile ad hoc network, since the authority may not be reachable from all nodes at all times
    - [Zhou] suggests distributing the CA function over multiple nodes

3. MAC Layer Misbehavior

➔ **Selfish Misbehavior to Improve Performance**



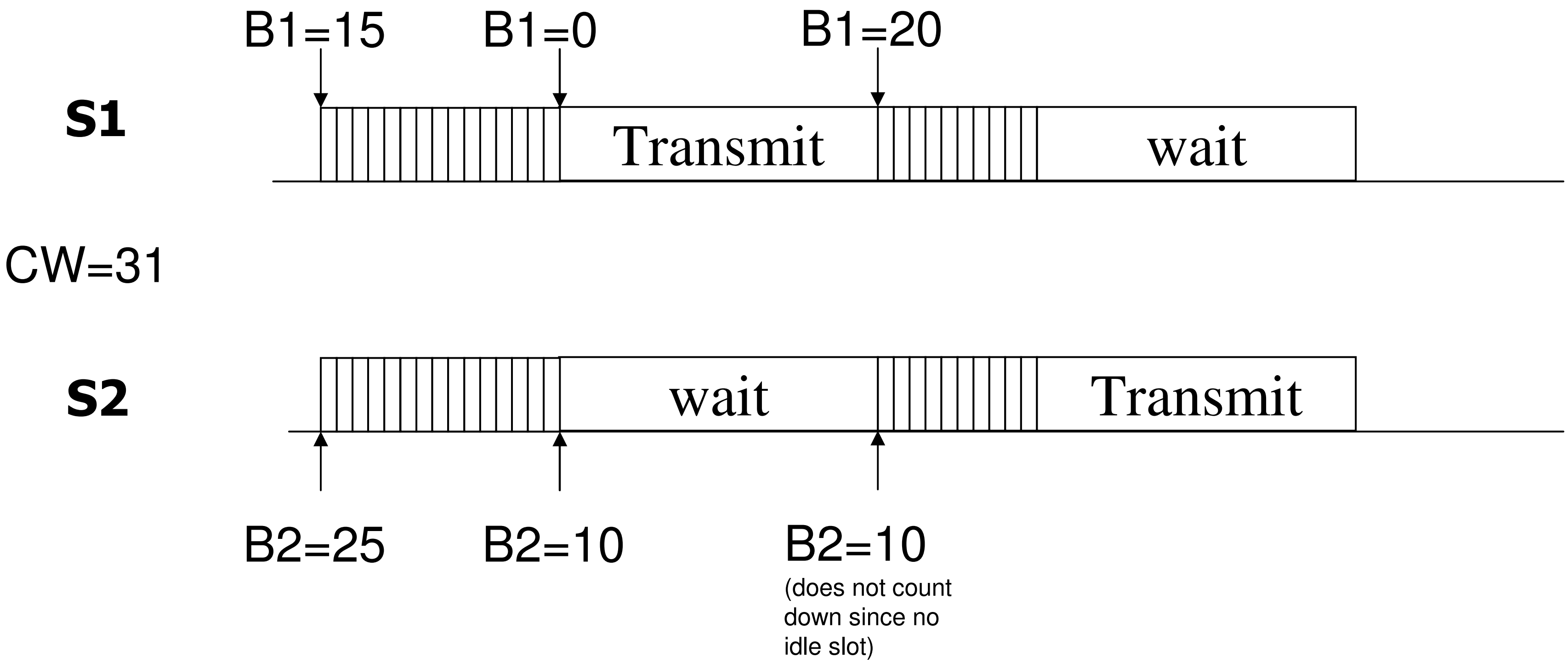
- Nodes are required to follow Medium Access Control (MAC) rules

Misbehaving nodes may violate MAC rules

3. MAC Layer Misbehavior

➔ Backoff Example

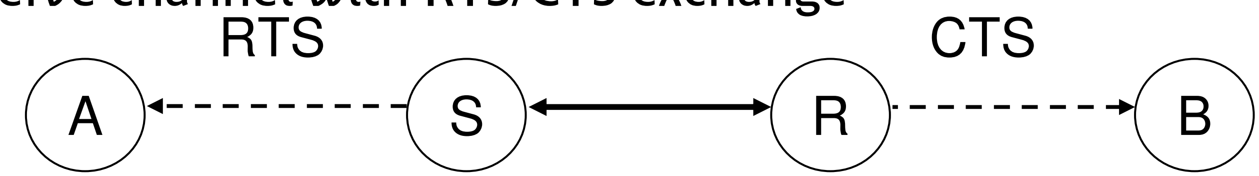
- Choose backoff value B in range [0,CW]
  - CW is the Contention Window
- Count down backoff by 1 every **idle slot**

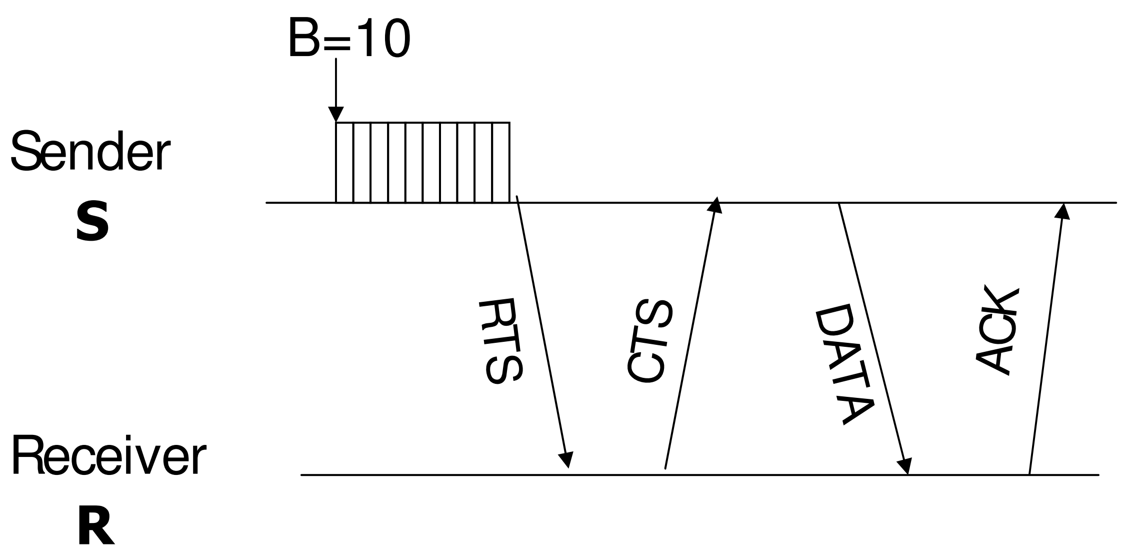


3. MAC Layer Misbehavior

➔ Data Transmission

- Reserve channel with RTS/CTS exchange

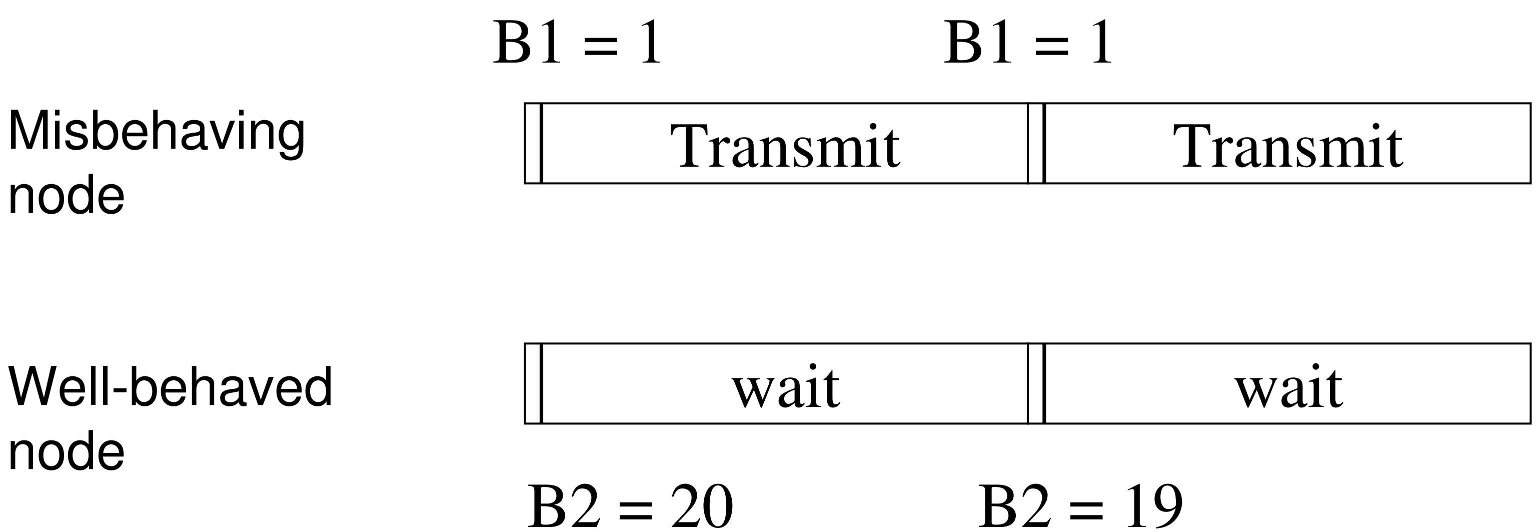




3. MAC Layer Misbehavior

➔ Possible Misbehavior

- Backoff from biased distribution
  - *Example*: Always select a small backoff value



3. MAC Layer Misbehavior

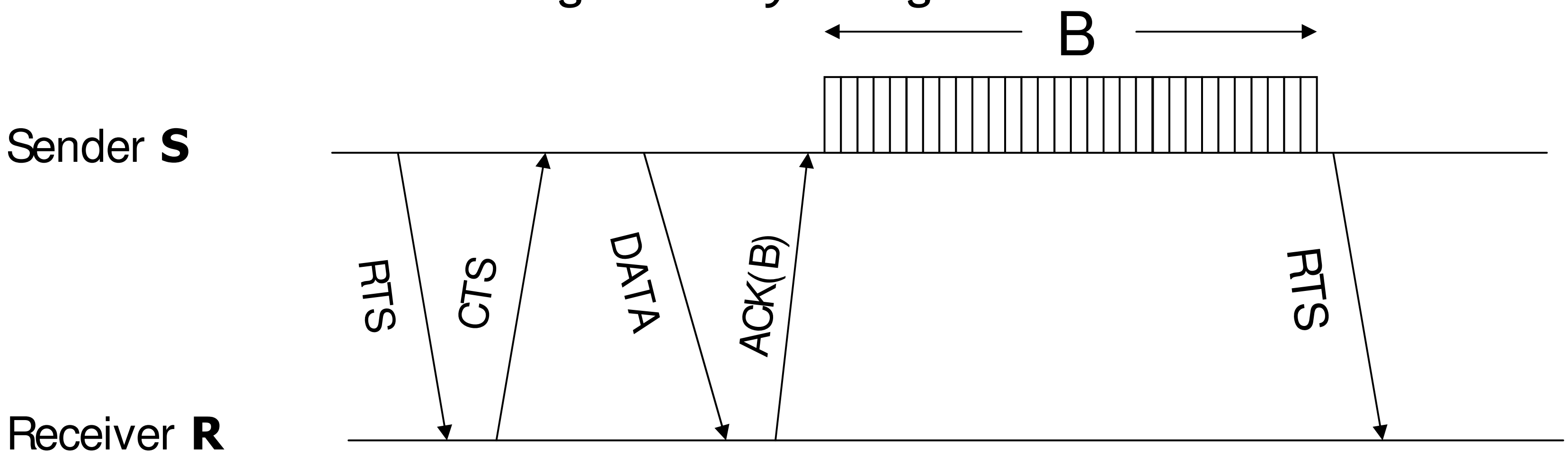
➔ **Potential Solution : Use long-term statistics**

- Observe backoffs chosen by sender over multiple packets
- Backoff values not from expected distribution ➔ Misbehavior

3. MAC Layer Misbehavior

➔ An Other Simpler Approach

- Receiver provides backoff values to sender
  - Receiver specified backoff for next packet in ACK for current packet
- Modification does not significantly change 802.11 behavior



- R provides backoff B to S in ACK

  B selected from [0,CW_{min}]
- S uses B for backoff

MANET Actors

- ➔ **Standards**
  - MANET IETF group (http://www.ietf.org/html.charters/manet-charter.html)
  - IETF AUTOCONF
- ➔ **Industrials**
  - HP, Hitachi, Nokia, MobileRoute
  - Deployment:
    - Métricom network, roofTop
    - France Telecom (Musée des Télécommunications de Pleumeur)
- ➔ **Conferences :**
  - Mobihoc, Mobicom, etc.