Ad Hoc Networks

Mark Wang

Intelligent Robotics and Manufacturing Systems Laboratory

Simon Fraser University

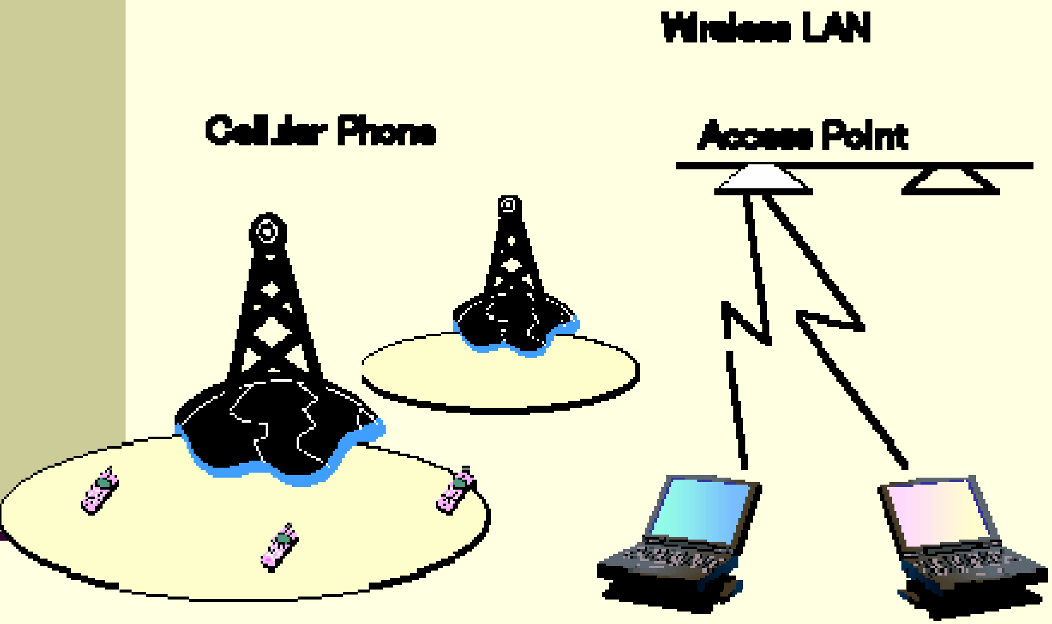
June 3, 2004

Roadmap

- Introduction to Ad Hoc Networks
- Ad hoc Networks characteristics and challenges
- Routing algorithms in Ad Hoc Networks
- Problems and my goals
- Summary and Comparison
- Schedules

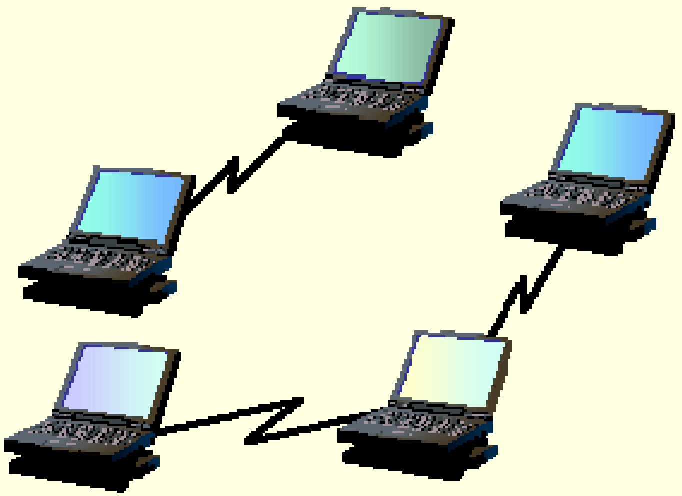
Wireless Ad Hoc Networks

Present Mobile Communication



Base station or access point recognizes terminal location and decides communication route.

Wireless Ad Hoc Network



- No infrastructure (base station, access point)

  → Network anywhere

  (disaster stricken area, stadium)

- Key technologies
  - Routing algorithm
  - Adaptation to network topology change
  - Efficiency in frequency and power

Ad Hoc Network

Ad Hoc? from Latin: “for this (only)”

We hope to have:

- wireless, self-configuring, self-optimizing data network
- trillions of nodes, global interconnectivity, quality of service
- all Internet applications, and voice, and video
- seamless operation from laptops, mainframes, to headsets and it shouldn’t cost too much.

Research in Ad Hoc Networks

- **Hardware** :

  Reduced power consumption

  Reduced size and cost

  Improved user interface
- **Software** :

  Communication protocols for routing

  Energy-efficient algorithms

  Bandwidth saving

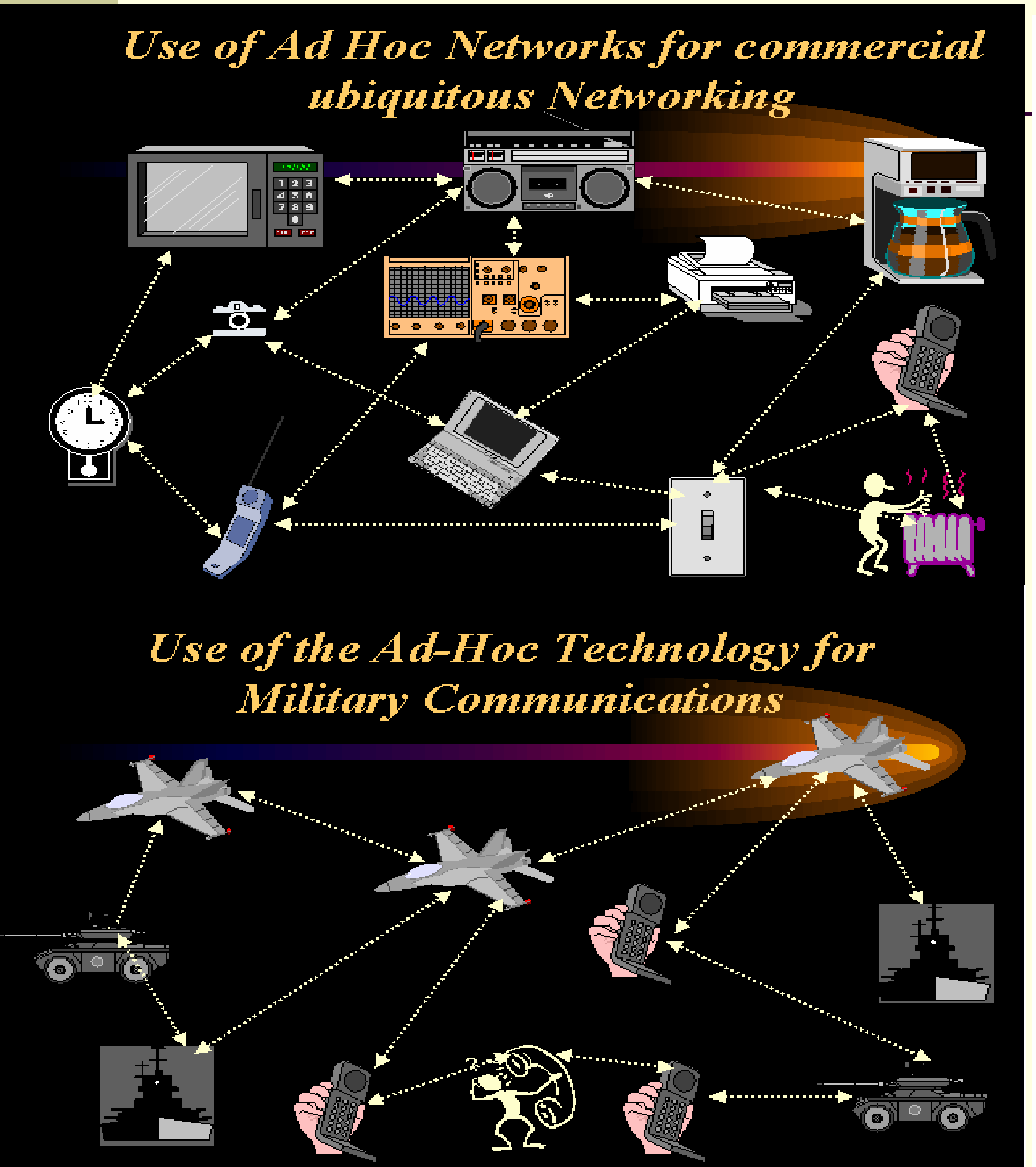
  Multicasting
- **Other Directions** :

  Privacy of mobile users (security)

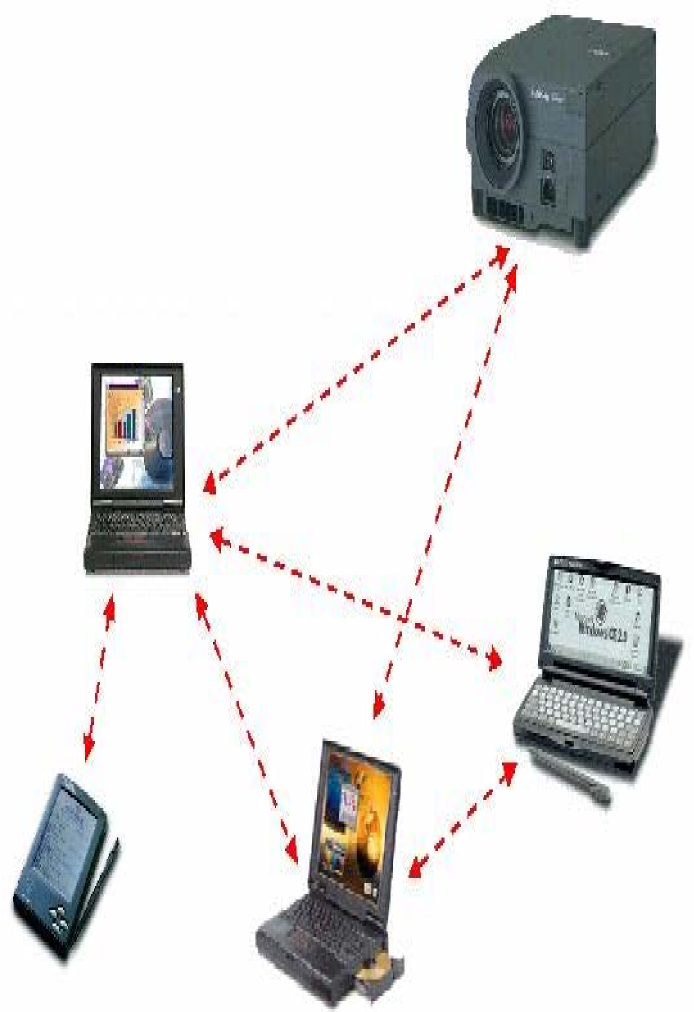
  Multimedia, mobility, multihop

Power-Efficient Ad Hoc Mobile Networking

Application Examples

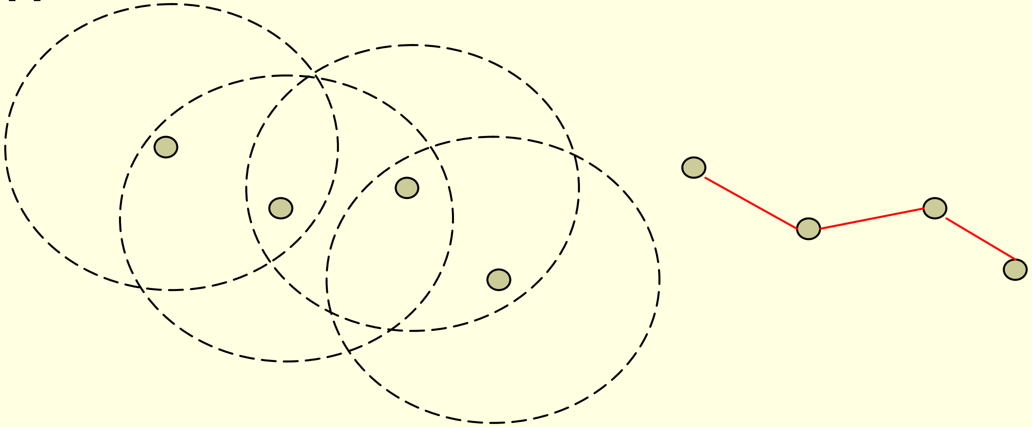


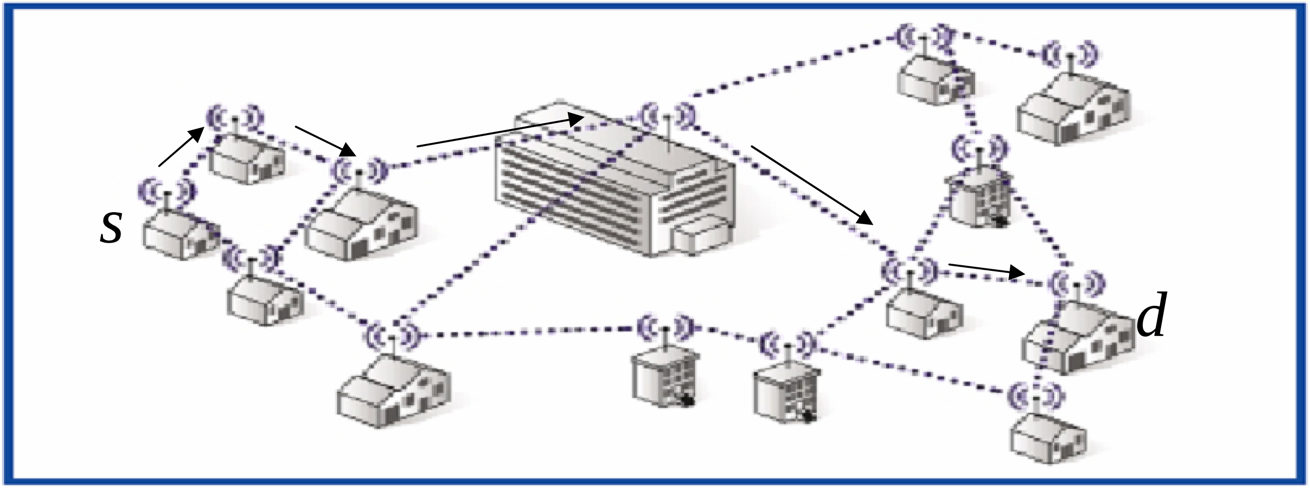
Personal Ad – Hoc Network



Multi-Hop Wireless

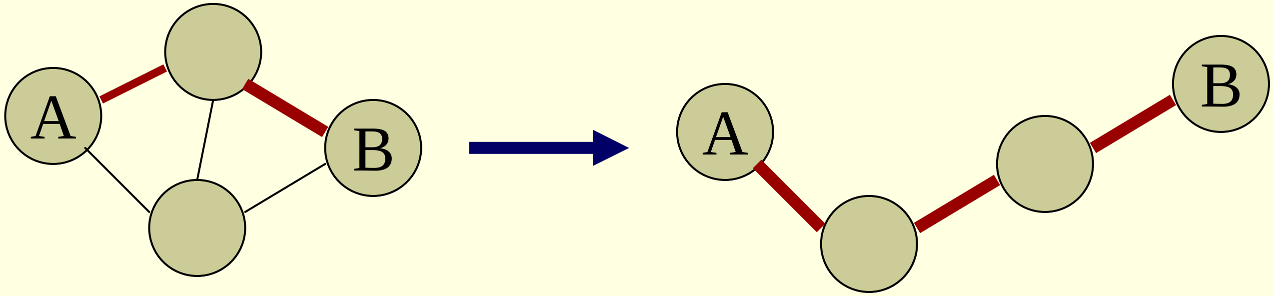
- May need to traverse multiple links to reach destination





Mobile Ad Hoc Networks (MANET)

- Host moves frequently
- Topology changes frequently
- No cellular infrastructure
- Multi-hop wireless links
- Data must be routed via intermediate nodes



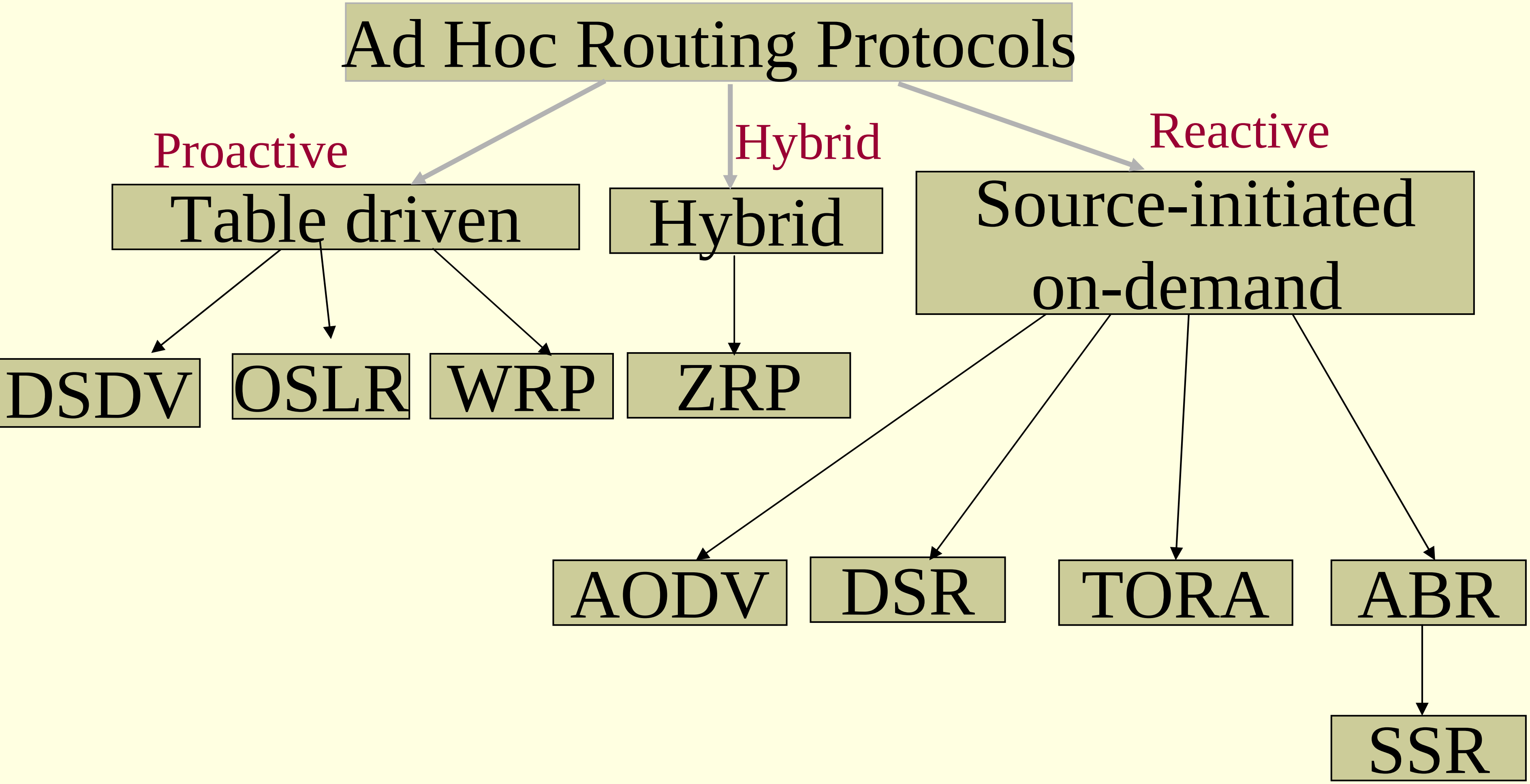
Challenges in Mobile Environments

- Limitations of wireless networks
  - 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 mobile computers
  - Short battery life
  - Limited capacity

Unicast Routing Protocols

- Many protocols have been proposed
- Some specifically invented for MANET
- Others adapted from protocols for wired networks
- No single protocol works well in all environments
  - Some attempts made to develop adaptive/hybrid protocols
- Standardization efforts in IETF
  - MANET, MobileIP working groups
  - http://www.ietf.org

Current Ad Hoc Routing Protocols



Routing Protocols

- Proactive protocols
  - Traditional distributed shortest-path protocols
  - Maintain routes between every host pair at all times
  - Based on periodic updates; high routing overhead
  - Example: DSDV (destination sequenced distance vector)
- Reactive protocols
  - Determine route if and when needed
  - Source initiates route discovery
  - Example: AODV (dynamic source routing)
- Hybrid protocols
  - Adaptive; Combination of proactive and reactive
  - Example : CBRP (Cluster-based Routing Protocol)

Protocol Trade-offs

- Proactive 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
- 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

DSDV

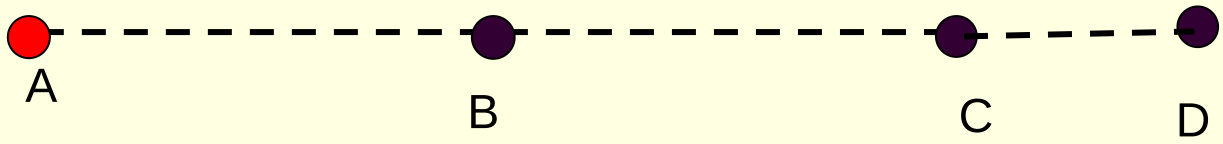
Destination-Sequenced Distance-Vector Routing

DSDV Protocol

- Innovative distance-vector routing approach
- Key idea: Operate each host as a special router
- Routing protocol modification to Bellman-Ford
- Guarantee Loop Freeness
  - New Table Entry for Destination Sequence Number
- Allow fast reaction to topology changes
  - Make immediate route advertisement on significant changes in routing table
  - but wait with advertising of unstable routes (damping fluctuations)

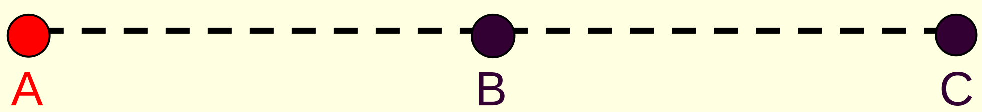
DSDV (Table Entries)

Destination	Next	Metric	Seq. Nr	Install Time	Stable Data
A	A	0	A-550	001000	Ptr_A
B	B	1	B-102	001200	Ptr_B
C	B	2	C-588	001200	Ptr_C
D	B	3	D-312	001200	Ptr_D



- **Sequence number** originated from destination. Ensures loop freeness.
- **Install Time** when entry was made (used to delete stale entries from table)
- **Stable Data** Pointer to a table holding information on how stable a route is. Used to damp fluctuations in network.

DSDV (Tables)



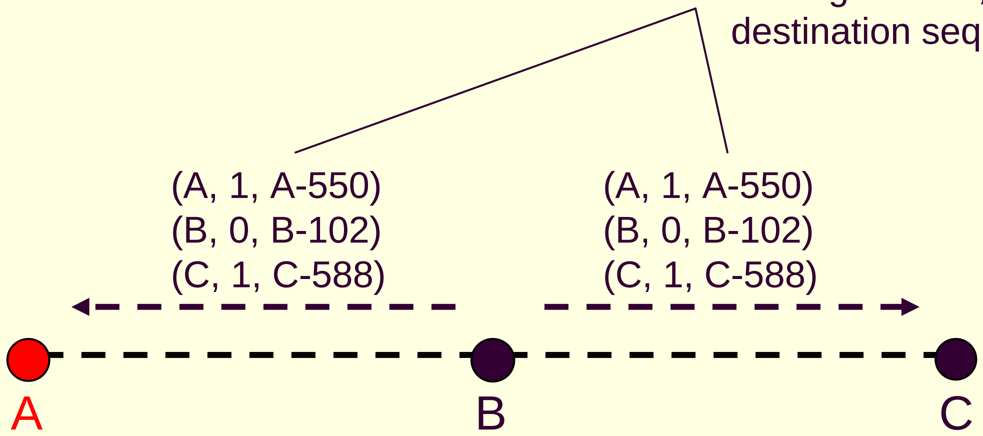
Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-100
C	B	2	C-586

Dest.	Next	Metric	Seq
A	A	1	A-550
B	B	0	B-100
C	C	2	C-588

Dest.	Next	Metric	Seq.
A	B	1	A-550
B	B	2	B-100
C	C	0	C-588

DSDV (Route Advertisement)

B increases Seq.Nr from 100 -> 102
B broadcasts routing information
to Neighbors A, C including
destination sequence numbers



Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-102
C	B	2	C-588

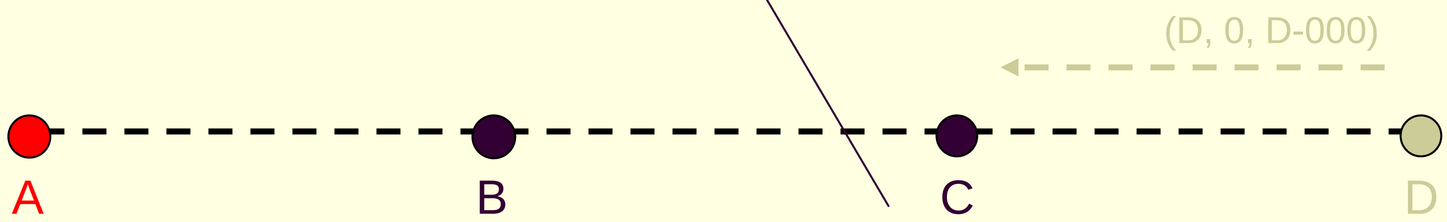
Dest.	Next	Metric	Seq
A	A	1	A-550
B	B	0	B-102
C	C	1	C-588

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-102
C	C	0	C-588

DSDV (New Node)

2. Insert entry for D with
sequence number D-000
Then immediately broadcast own
table

1. D broadcast for first time
Send Sequence number D-000



Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-102
C	B	2	C-590

Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-102
C	C	1	C-590

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-102
C	C	0	C-590
D	D	1	D-000

DSDV (New Node)

3. C increases its sequence number to C-592 then

Immediately broadcasts!

its new table.

(A, 2, A-550)
(B, 1, B-102)
(C, 0, C-592)
(D, 1, D-000)

(A, 2, A-550)
(B, 1, B-102)
(C, 0, C-592)
(D, 1, D-000)

Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

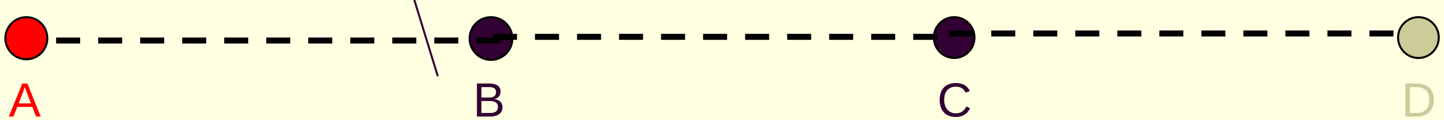
Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-102
C	C	1	C-590

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-102
C	C	0	C-592
D	D	1	D-000

DSDV (New Node)

4. B gets this new information and updates its table…….

D gets routing table from C and create its own table.



Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-102
C	C	1	C-592
D	C	2	D-000

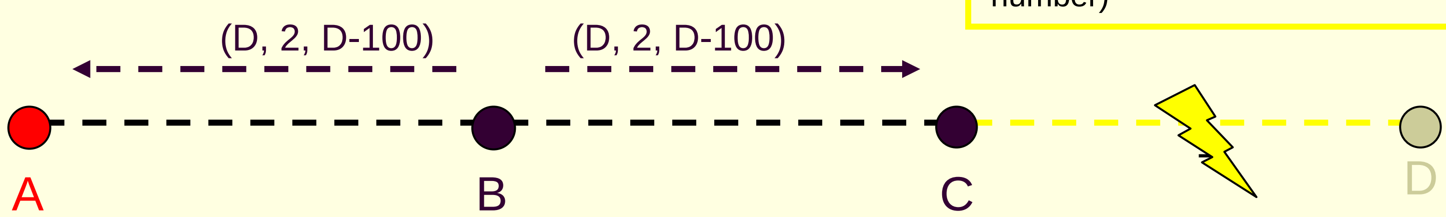
Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-102
C	C	0	C-592
D	D	1	D-000

Dest.	Next	Metric	Seq.
A	C	3	A-550
B	C	2	B-102
C	C	1	C-592
D	D	0	D-000

DSDV (no loops, no count to infinity)

2. B does its broadcast
-> no affect on C (C knows that B has stale information because C has higher seq. number for destination D)
-> no loop -> no count to infinity

1. Node C detects broken Link:
-> Increase Seq. Nr. by 1
(only case where not the destination sets the sequence number -> odd number)



Dest.	Next	Metric	Seq.
…	…	…	
D	B	3	D-100

Dest.c	Next	Metric	Seq.
…	…	…	
D	C	2	D-100

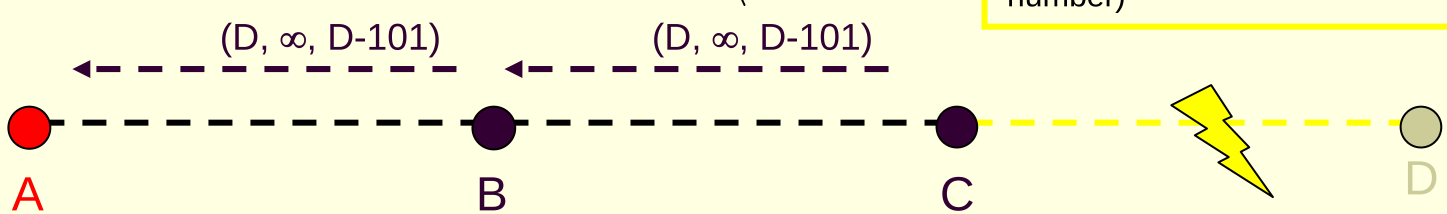
Dest.	Next	Metric	Seq.
…	…	…	
D	D	∞	D-101

DSDV (Immediate Advertisement)

3. Immediate propagation B to A:
(update information has higher Seq. Nr. -> replace table entry)

2. Immediate propagation C to B:
(update information has higher Seq. Nr. -> replace table entry)

1. Node C detects broken Link:
-> Increase Seq. Nr. by 1
(only case where not the destination sets the sequence number -> odd number)



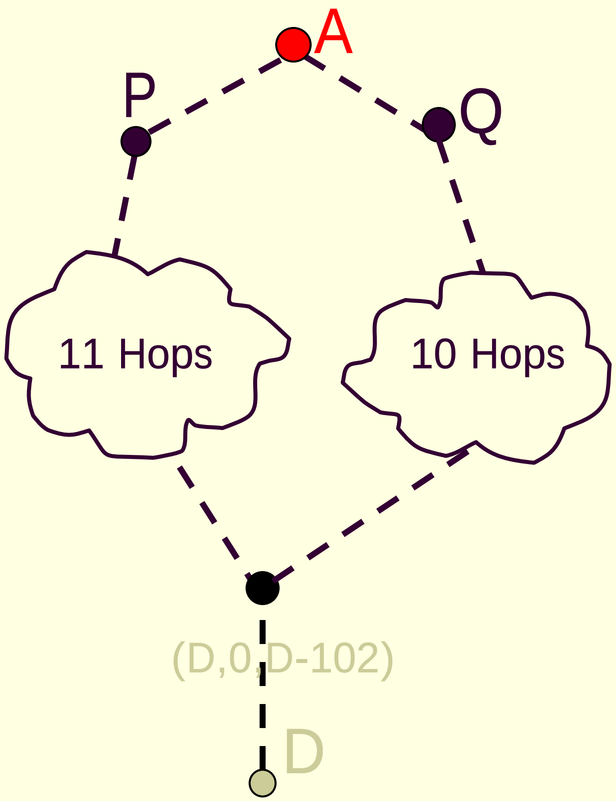
Dest.	Next	Metric	Seq.
…	…	…	...
~~D~~	~~B~~	~~3~~	~~D-100~~
D	B	∞	D-101

Dest.c	Next	Metric	Seq.
…	…	…	...
~~D~~	~~C~~	~~2~~	~~D-100~~
D	C	∞	D-101

Dest.	Next	Metric	Seq.
…	…	…	
~~D~~	~~D~~	~~1~~	~~D-100~~
D	D	∞	D-101

DSDV (Problem of Fluctuations)

What are Fluctuations?

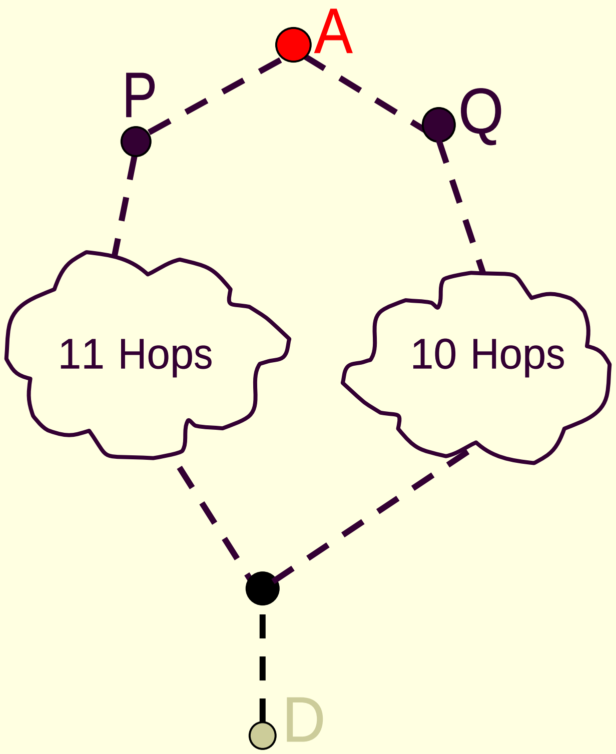


- Entry for D in A: [D, Q, 14, D-100]
- D makes Broadcast with Seq. Nr. D-102
- A receives from P Update (D, 15, D-102)
  -> Entry for D in A: [D, P, 15, D-102]
  A must propagate this route immediately.
- A receives from Q Update (D, 14, D-102)
  -> Entry for D in A: [D, Q, 14, D-102]
  A must propagate this route immediately.

This can happen every time D or any other node does its broadcast and lead to unnecessary route advertisements in the network, i.e., fluctuations.

DSDV (Damping Fluctuations)

How to damp fluctuations



- Record last and average Settling Time of every Route in a separate table. (Stable Data) Settling Time = Time between arrival of first route and the best route with a given sequence number.
- A user must update his routing table on the first arrival of a route with a newer sequence number but he can wait to advertise it. Time to wait is 2*(avg. Settling Time).
- By this means, fluctuations in larger networks can be damped to avoid unnecessary advertisement, thus saving bandwith.

DSDV Summary

- Advantages
  - Simple (similar to Distance Vector)
  - Loop free through destination sequence numbers
  - No latency caused by route discovery

- Disadvantages
  - No sleeping nodes
  - Overhead: most routing information never used
  - Poor Scalability

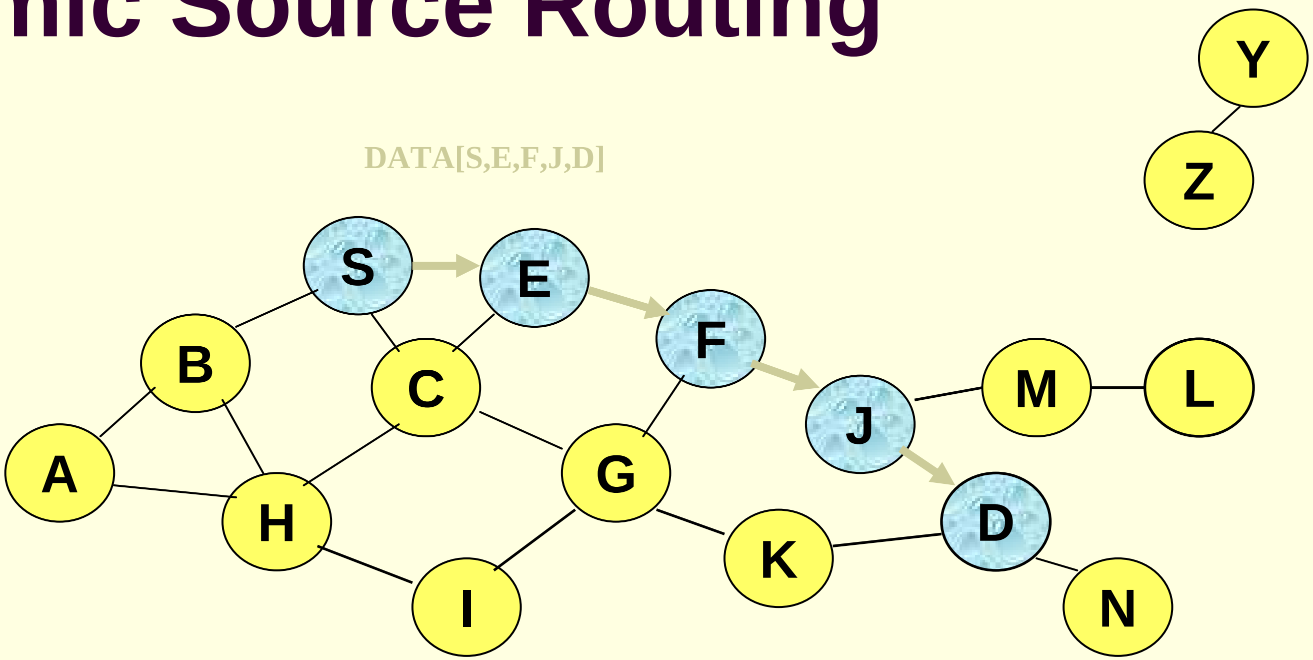
DSR

Dynamic Source Routing

Basic Assumptions in DSR

- All nodes are willing to forward packets for other nodes in the network
- The diameter of an ad-hoc network will not be too large
  - Packet header will be larger than the payload if route is very longer
- The node’s speed is moderate
  - Local route cache will become stale if node’s speed is high
- All nodes are overhearing (promiscuous)
  - No energy saving

Dynamic Source Routing



- When S sends a data packet to D, the entire route is included in the packet header
- Intermediate nodes use the source route embedded in the packet's header to determine to whom the packet should be forwarded
- Different packets may have different routes, even they have the same source and destination

Hence called dynamic source routing

Basics of DSR

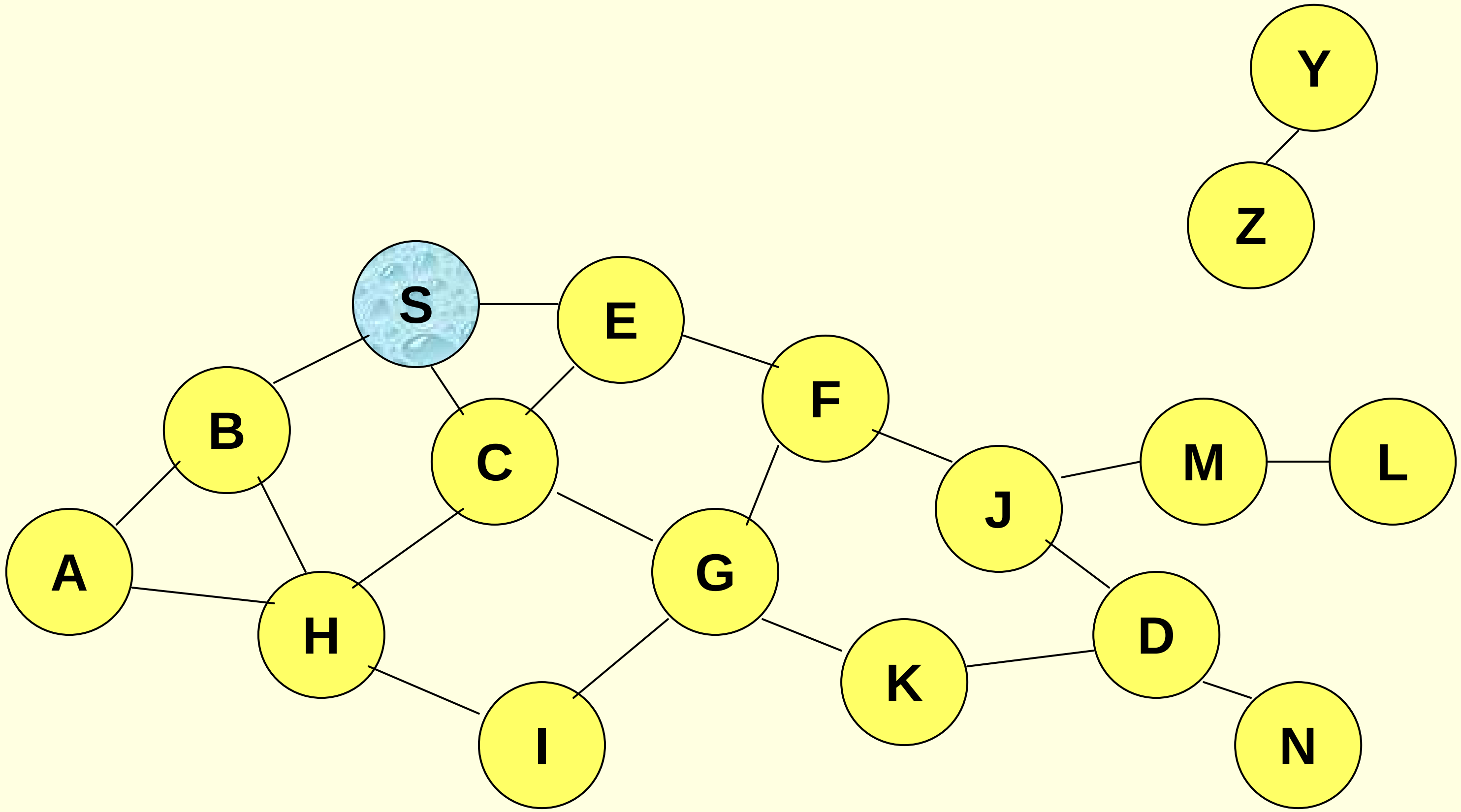
- Basic mechanisms
  - Route Discovery
    - Route Request (RREQ)
    - Route Reply (RREP)
  - Route Maintenance
  - Route Error (RERR)
- Key optimization
  - Each node maintains a route cache
    - Overhears data, RREQ, RREP, and RERR packets
    - Passively collects new routes as many as possible
    - Reduces the cost of Route Discovery and Route Maintenance

Route Discovery

- When to perform a Route Discovery ?
- Every route request packet (RREQ) contains

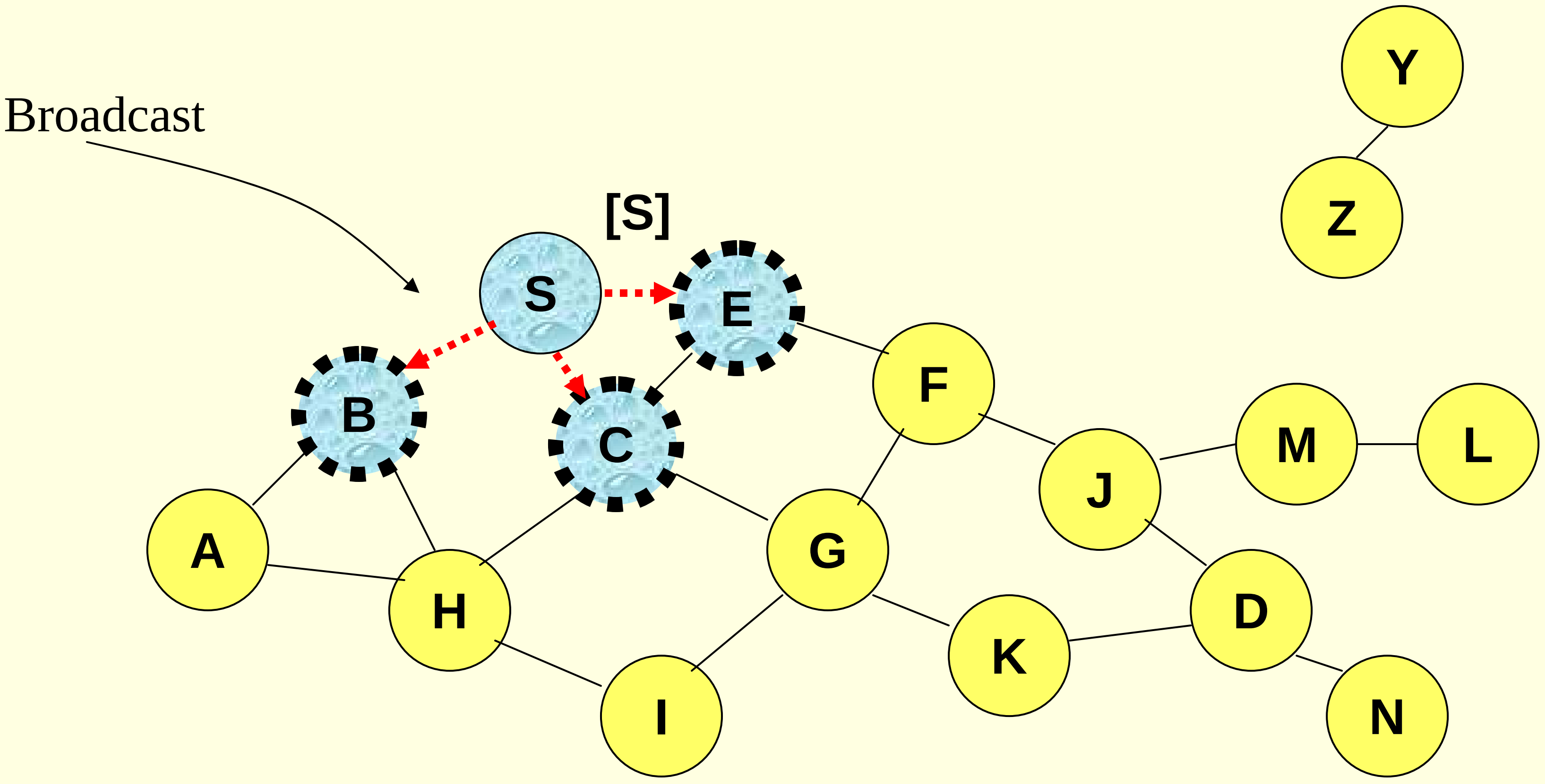
  <target address, initiator address, route record, request ID>
- Each node maintains a list of the < initiator address, request ID>
- When a node Y receives a RREQ
  - Discards the route request packet
    - if < initiator address, request ID> is in its list
  - Return a route reply packet which contains a route from initiator to target
    - If Y is target
    - If Y has an entry in its route cache for a route to target
  - Append itself address to the route record in RREQ and re-broadcast RREQ

Route Discovery in DSR



Represents a node that has received RREQ for D from S

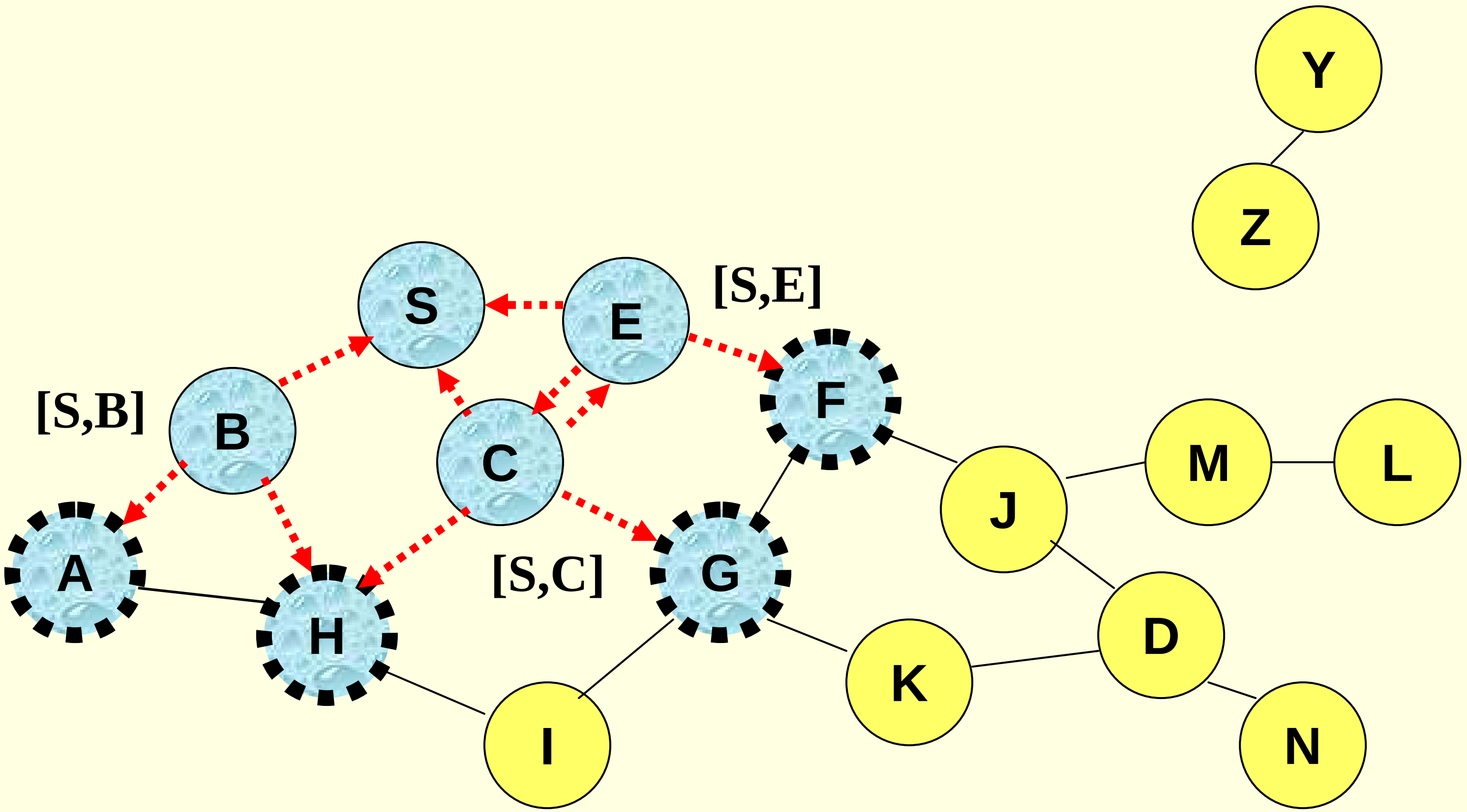
Route Discovery in DSR



Represents transmission of RREQ

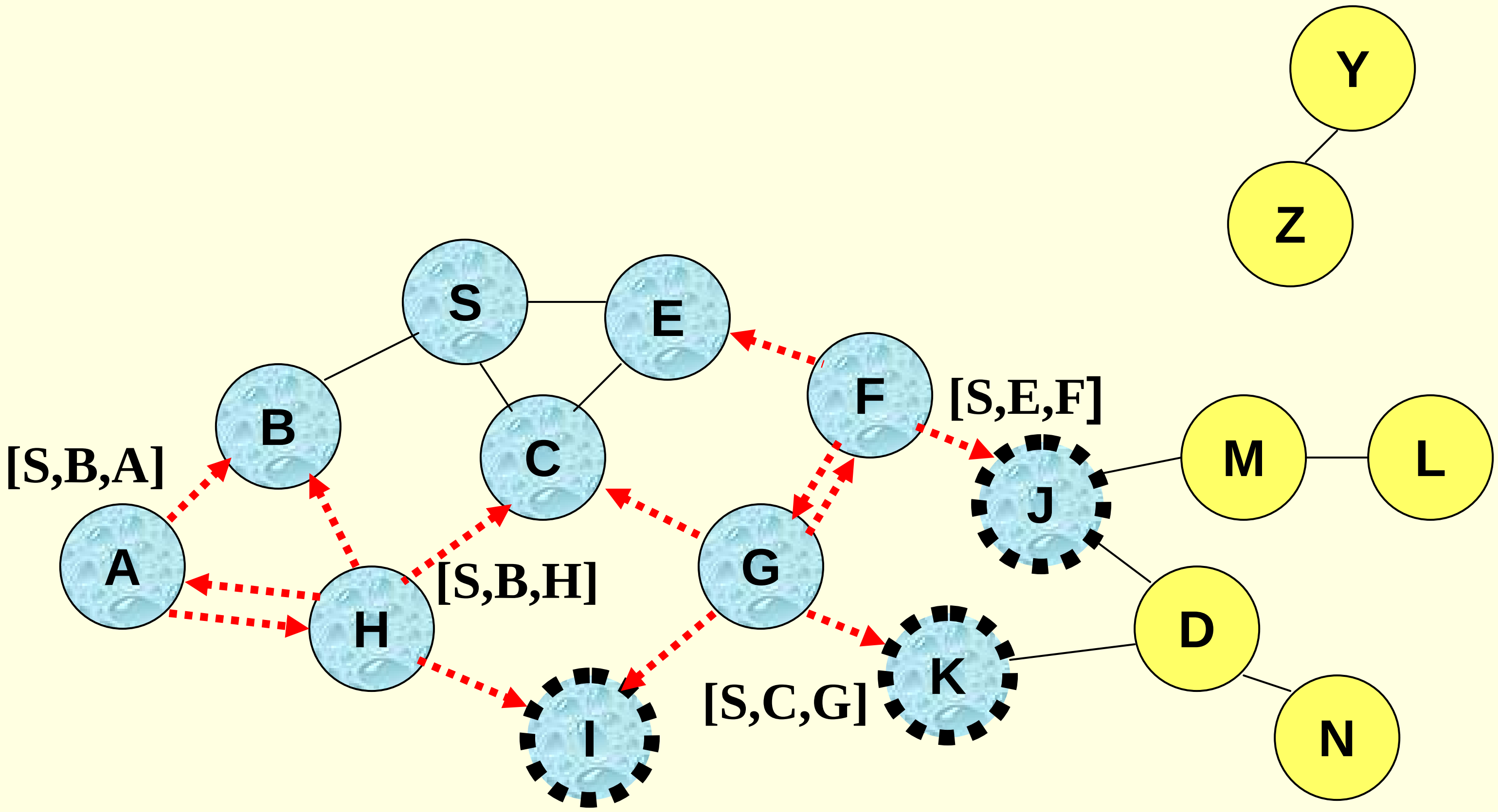
[X,Y] Represents route record stored in RREQ

Route Discovery in DSR



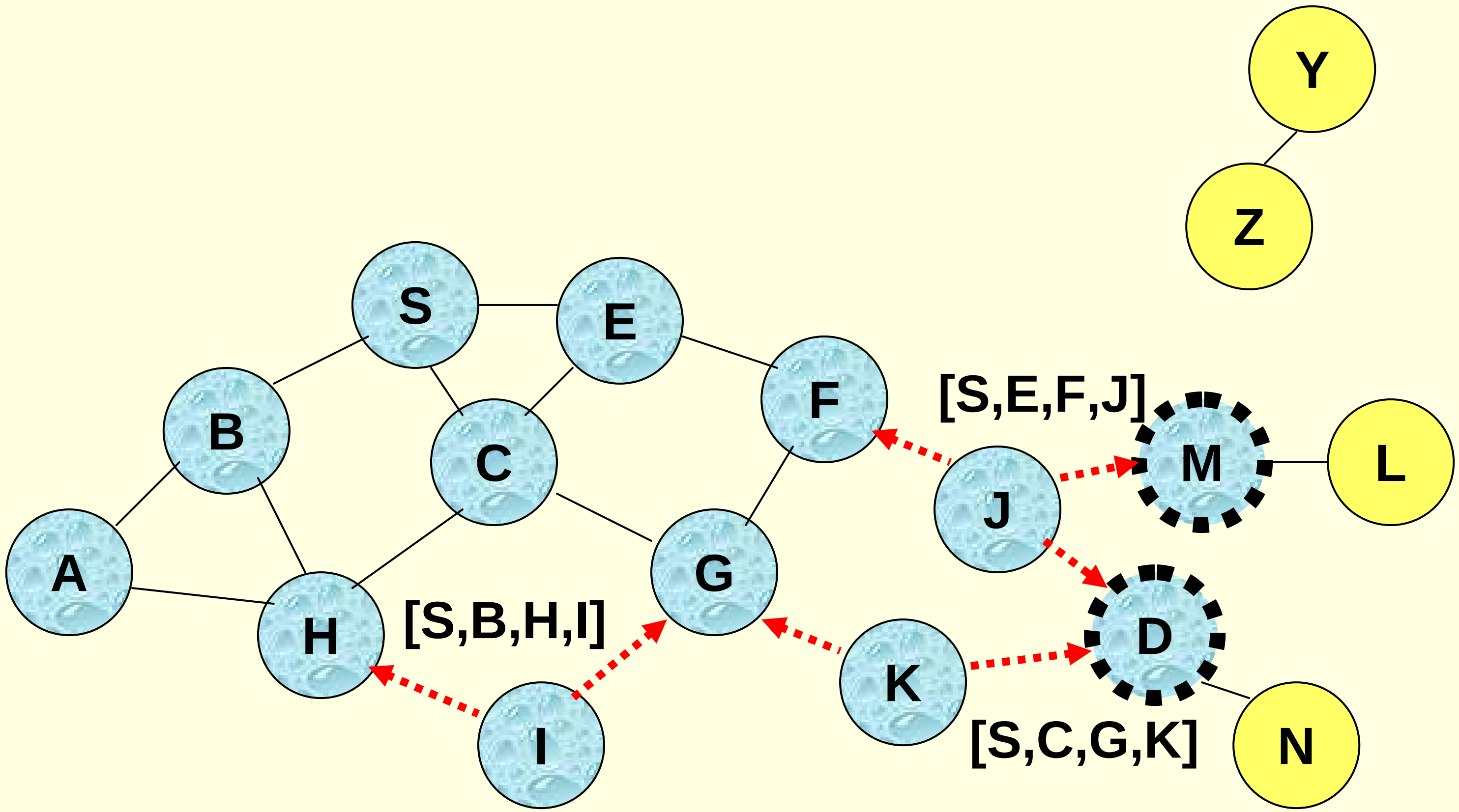
- **Node H receives packet RREQ from two neighbors: potential for collision**

Route Discovery in DSR



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

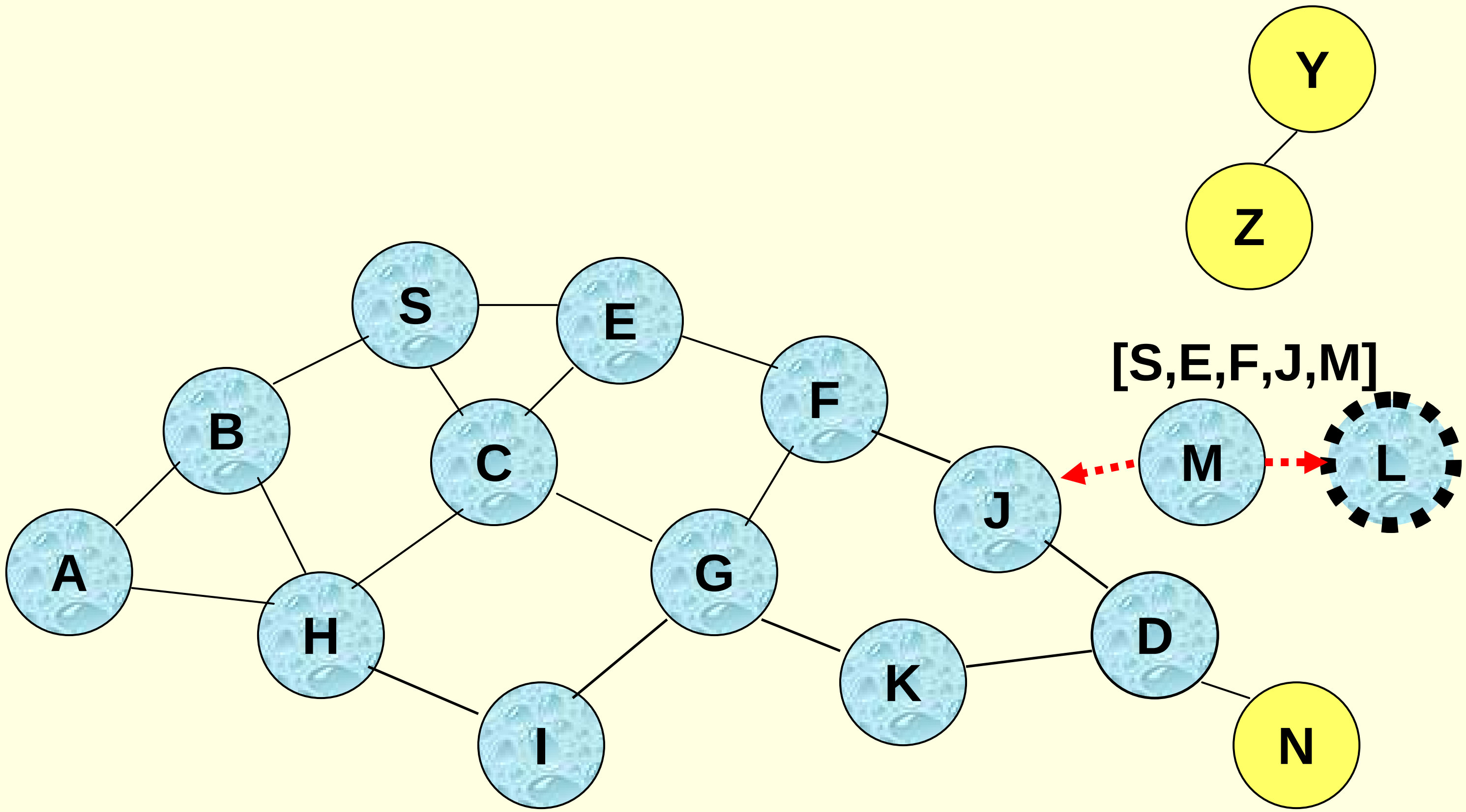
Route Discovery in DSR



J and **K** both broadcast RREQ to **D**

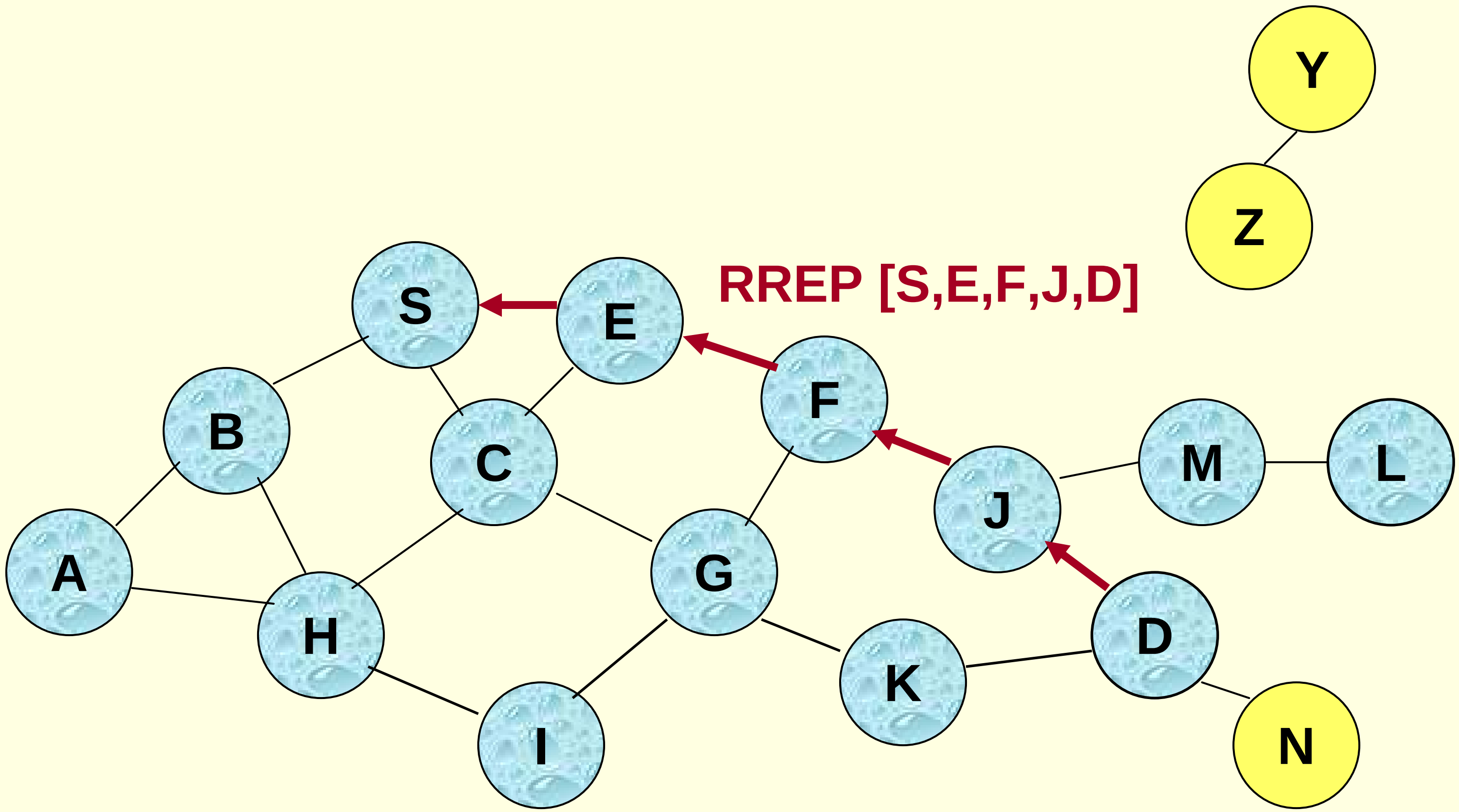
Their transmissions may collide at D

Route Discovery in DSR



D does not forward RREQ, because D is the intended target

Route Reply in DSR



Represents RREP control message

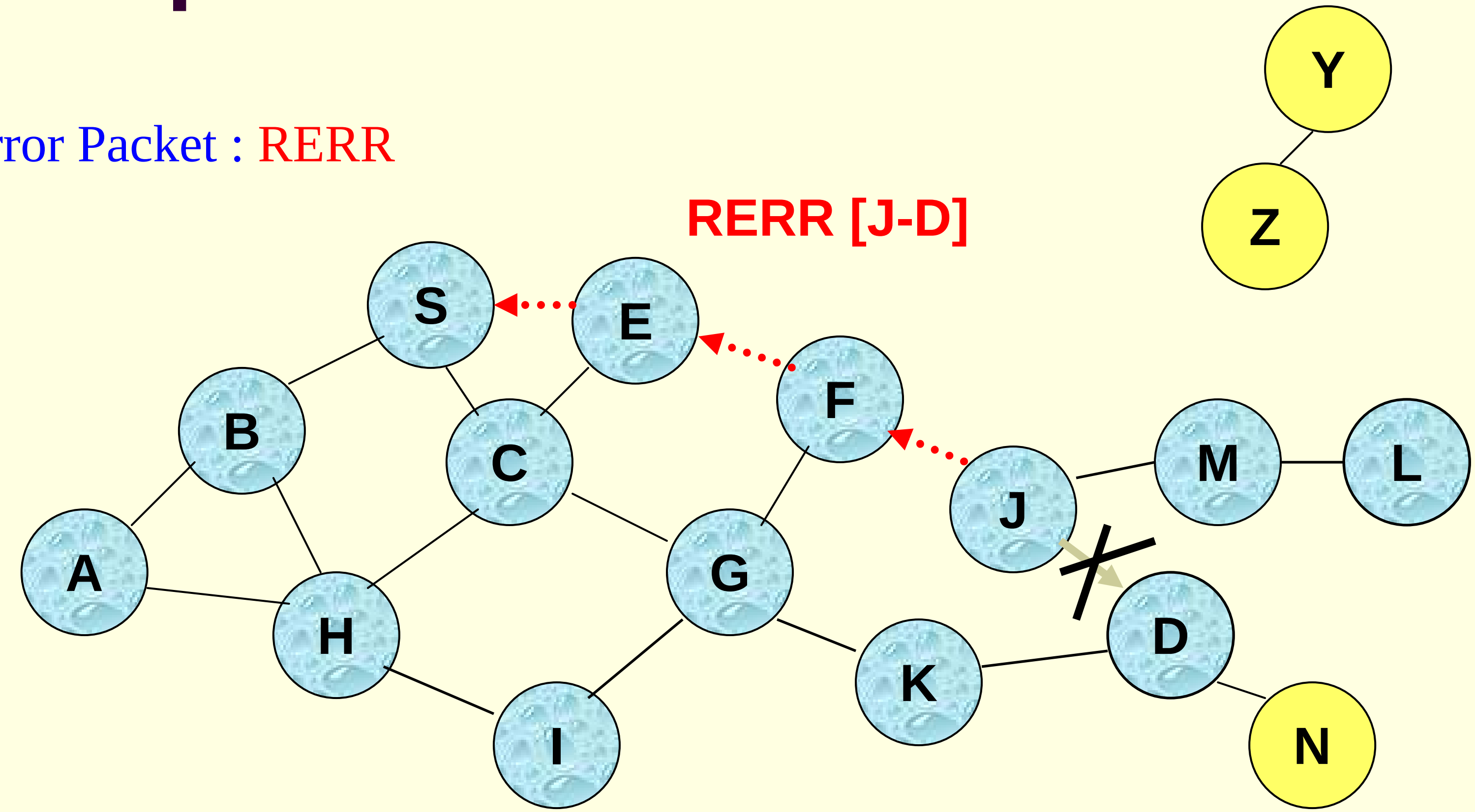
Details of Route Reply in DSR

- Destination D on receiving the first RREQ, sends a Route Reply (RREP)
- RREP includes the route from S to D
- How Route Reply packet is sent to S?
  - Route Reply can be sent by reversing the route in Route Request (RREQ)
    - If links are bi-directional
  - If unidirectional (asymmetric) links are allowed, then a route to S is needed
    - Local route cache has a route to S
    - Piggybacking Route Reply in Route Request packet for S

NOTE: If IEEE 802.11 MAC is used, then links have to be bi-directional

Example of Route Maintenance

Route Error Packet : RERR



J sends a route error to S along route J-F-E-S when it finds link [J-D] broken

Nodes hearing RERR update their route cache to remove all invalid routes related with link J-D

More Details on Route Maintenance

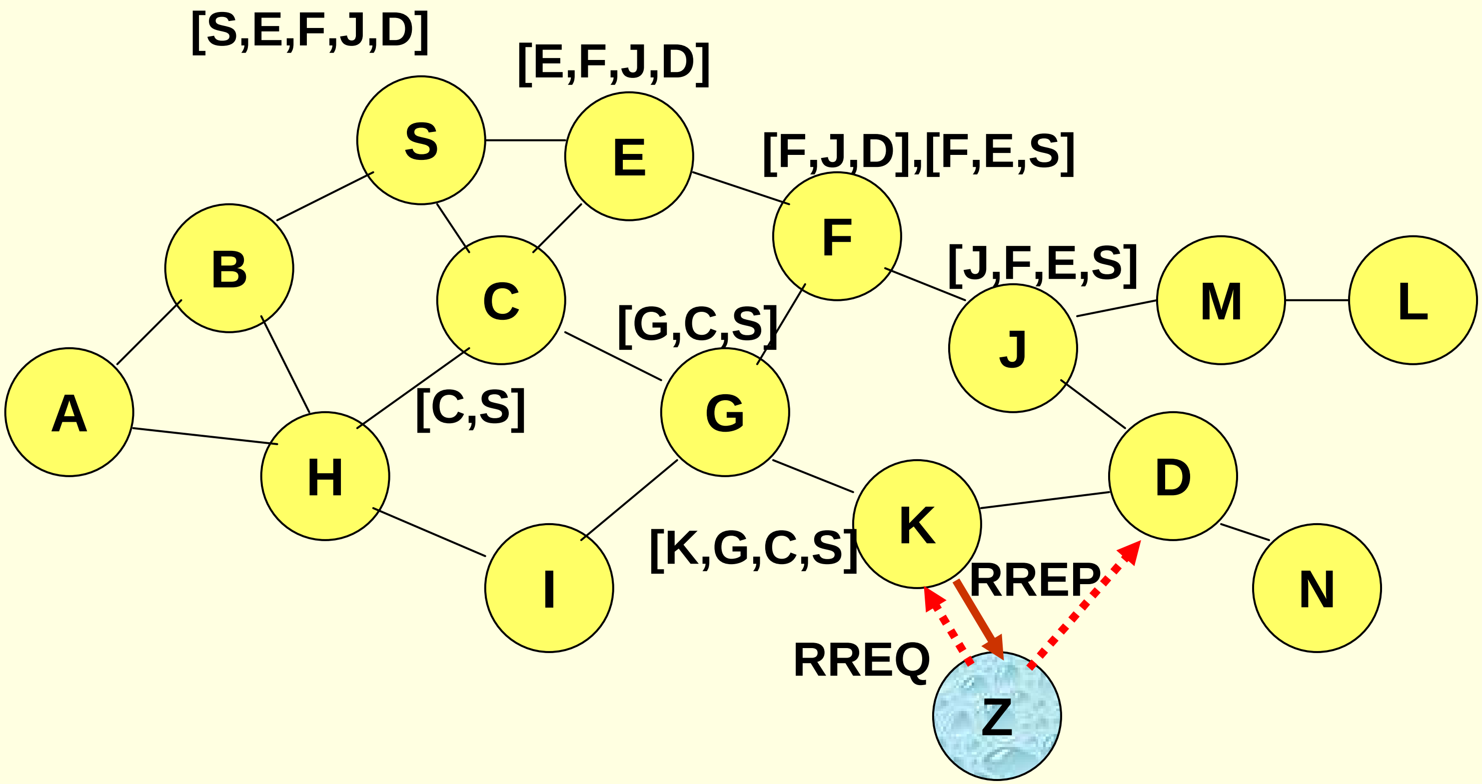
Route [S, node-1,node-2,……,node-k, D]

- Hop-by-hop maintenance (MAC or network layer)
  - How to find link [node-i,node(i+1)] is down ?
    - Utilize MAC level acknowledgement
    - Passive acknowledge (overhearing node(i+1) re-transmission)
    - Insert a bit in packet header to ask an explicit acknowledgement from node(i+1)
  - How to send route error packet to S?
    - Use the reverse route [node-i,node(i-1), ……,node-1, S]
    - Use node-i route cache to get a route to S
    - Piggybacking route error packet in route discovery packet S
- End-to-end maintenance (transport or application layer)
  - D sends ACK to S to indicate the route status
    - But S does not know which link is broken

DSR Optimization: Route Caching

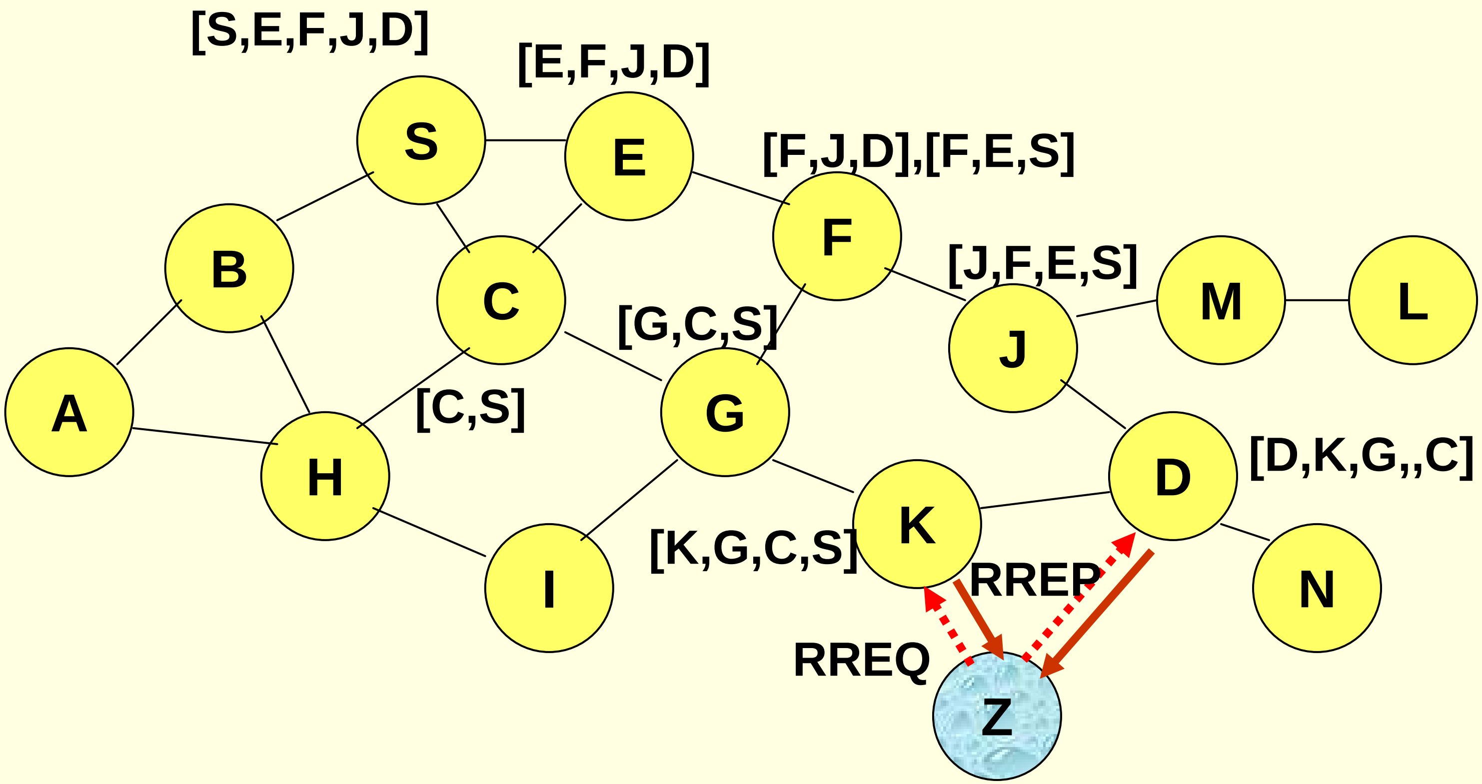
- Each node caches a new route it learns by *any means*
- When node S finds route [S,E,F,J,D] to node D, node S also learns route [S,E,F] to node F
- When node K receives Route Request [S,C,G] destined for node, node K learns route [K,G,C,S] to node S
- When node F forwards Route Reply RREP [S,E,F,J,D],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

Route Caching can accelerate 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

Use of Route Caching can Reduce Propagation of Route Requests



Route Replies (RREP) from node K and D limit flooding of RREQ.

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
- , due to intermediate nodes replying from local caches

Dynamic Source Routing: Disadvantages

- Packet header size grows with route length due to source routing: Inefficiency
- Flood of route requests may potentially reach all nodes in the network: RREQ flooding
- 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: Route Reply *Storm*
- Stale caches will lead to increased overhead

AODV

Ad Hoc On-Demand Distance Vector Routing

Ad Hoc On-Demand Distance Vector Routing

- 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 nodes, so that data packets do not have to contain routes
- AODV retains the desirable feature of DSR that routes are maintained only between nodes which need to communicate

AODV

- Route Requests (RREQ) are forwarded in a manner similar to DSR

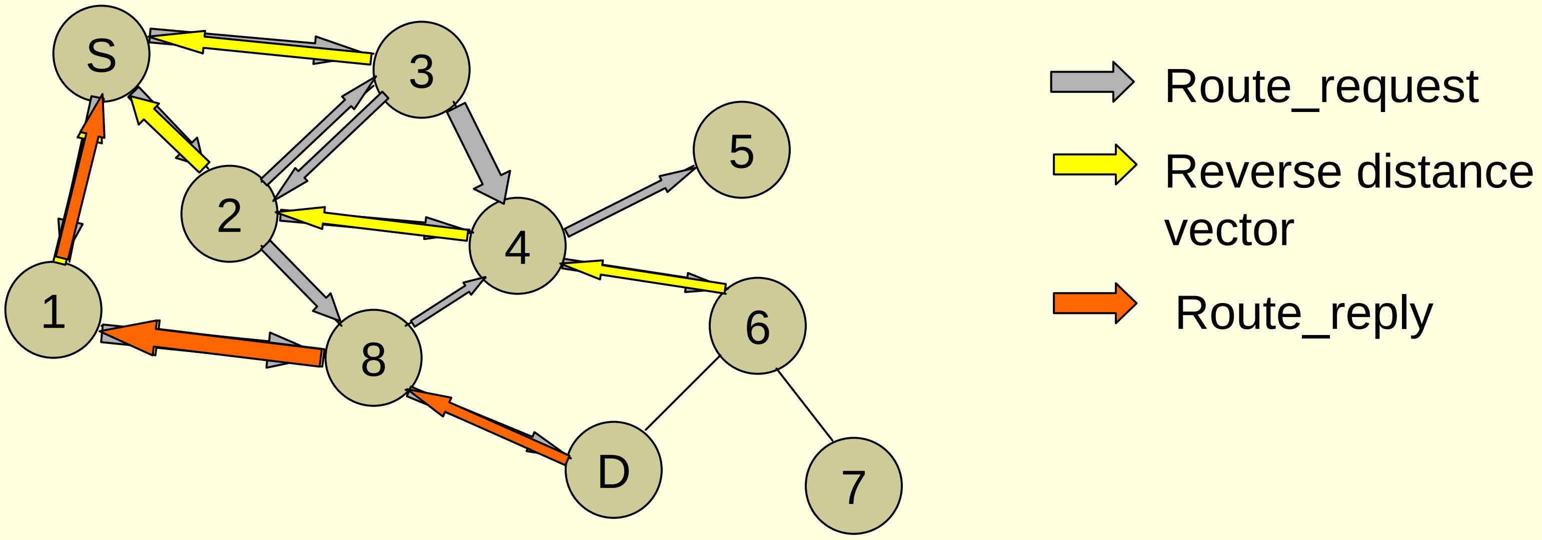
- When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source
  - AODV assumes symmetric (bi-directional) links

- When the intended destination receives a Route Request, it replies by sending a Route Reply (RREP)

- Route Reply travels along the reverse path set-up when Route Request is forwarded

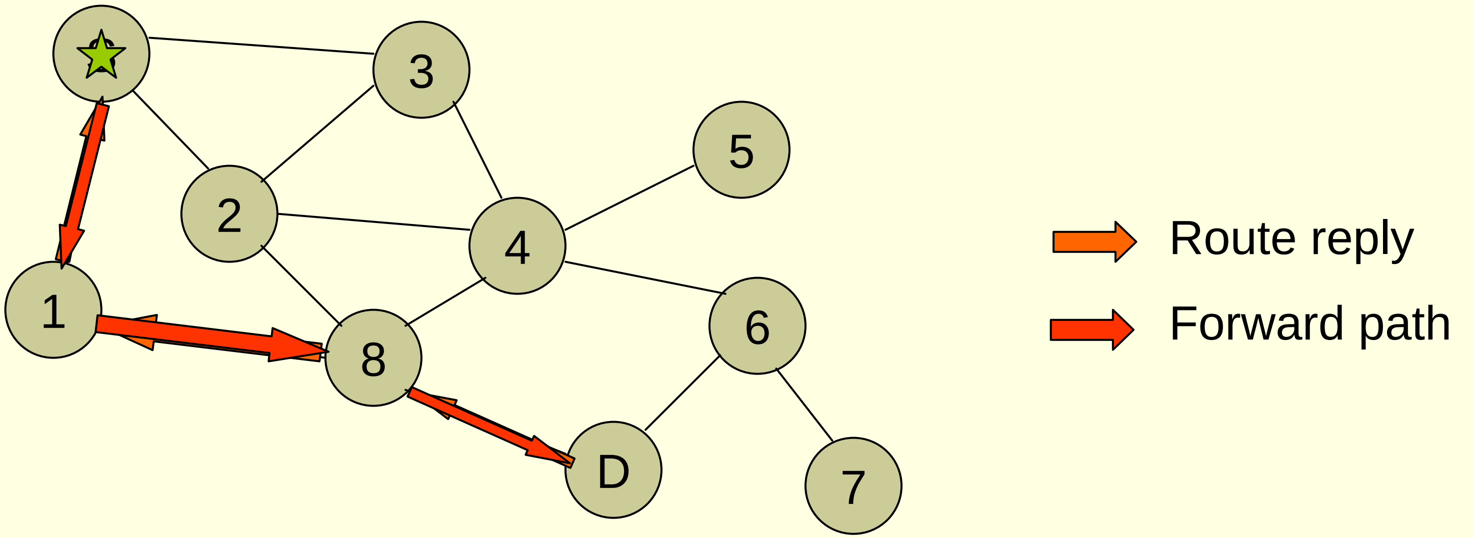
AODV (Route Discovery)

- Route Request



AODV (Route Discovery)

- “Forward” path



- An intermediate node can reply with a route reply on behalf of the destination node if it has an up to date route to the destination

Route Request and Route Reply

- Route Request (RREQ) includes the last known sequence number for the destination
- An intermediate node may also send a Route Reply (RREP) provided that it knows a more recent path than the one previously known to sender
- Intermediate nodes that forward the RREP, also record the next hop to destination
- 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

Link Failure

- A neighbor of node X is considered active for a routing table entry if the neighbor sent a packet within *active_route_timeout* interval which was forwarded using that entry
- Neighboring nodes periodically exchange hello message
- 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

Route Error

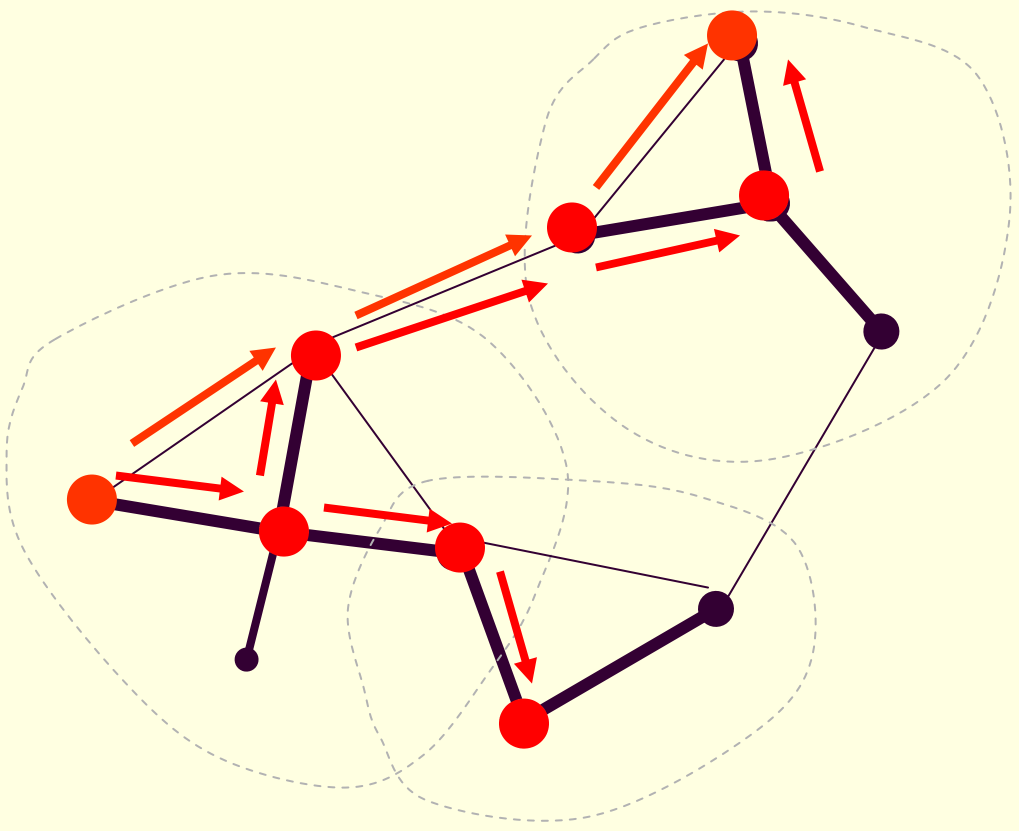
- When node X is unable to forward packet P (from node S to node D) on link (X,Y), it generates a RERR message
- Node X increments the destination sequence number for D cached at node X
- The incremented sequence number *N* is included in the RERR
- When node S receives the RERR, it initiates a new route discovery for D using destination sequence number at least as large as *N*
- When node D receives the route request with destination sequence number N, node D will set its sequence number to N, unless it is already larger than N

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
  - DSR may maintain several routes for a single destination
- Sequence numbers are used to avoid old/broken routes
- Sequence numbers prevent formation of routing loops
- Unused routes expire even if topology does not change

CBRP
Cluster-based Routing Protocol

CBRP: Protocol Overview

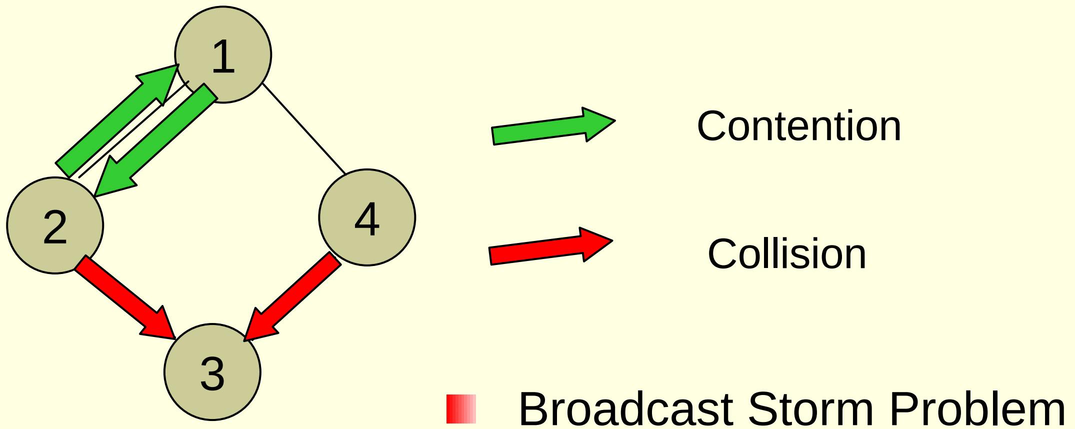


My Goals for the Research

- Solve the flooding problem
- Find mutipaths to improve load balance
- Combine different routing protocols

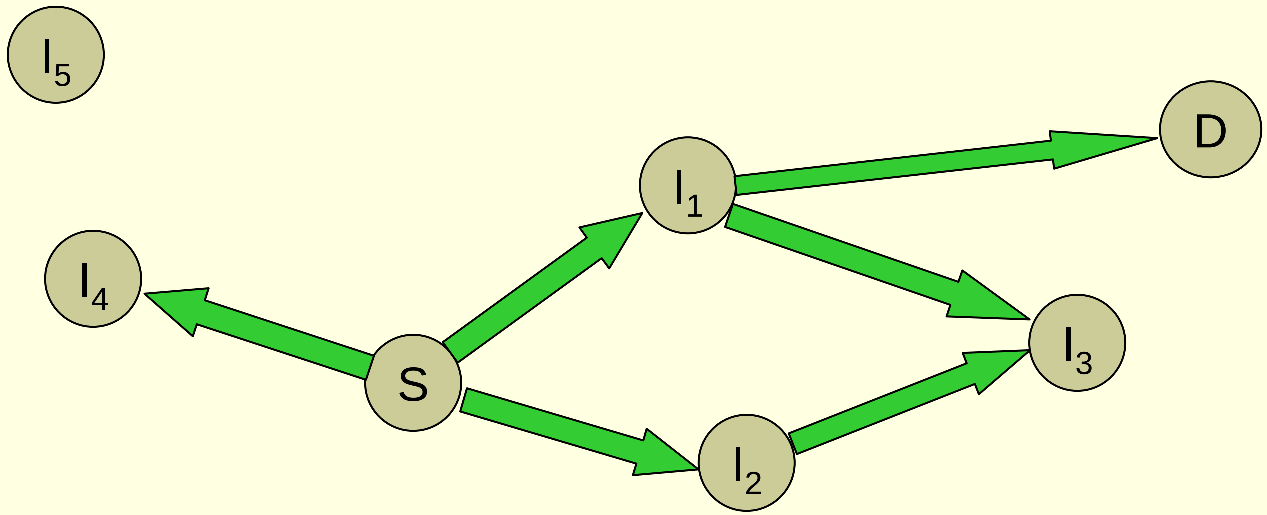
Areas for Improvement of an On-Demand Algorithm

- In on-demand protocols, route discoveries are performed by **flooding** the network with route request packets.
- Problems with the technique:
  - Flooding is highly redundant, causes collisions and contentions
  - Flooding causes route request packets to go beyond the destination and onto unnecessary regions of the network



Related Work: Optimizing Flooding

- Exploits location information to limit the scope of the route request flood
  - Location information being obtained from a GPS unit

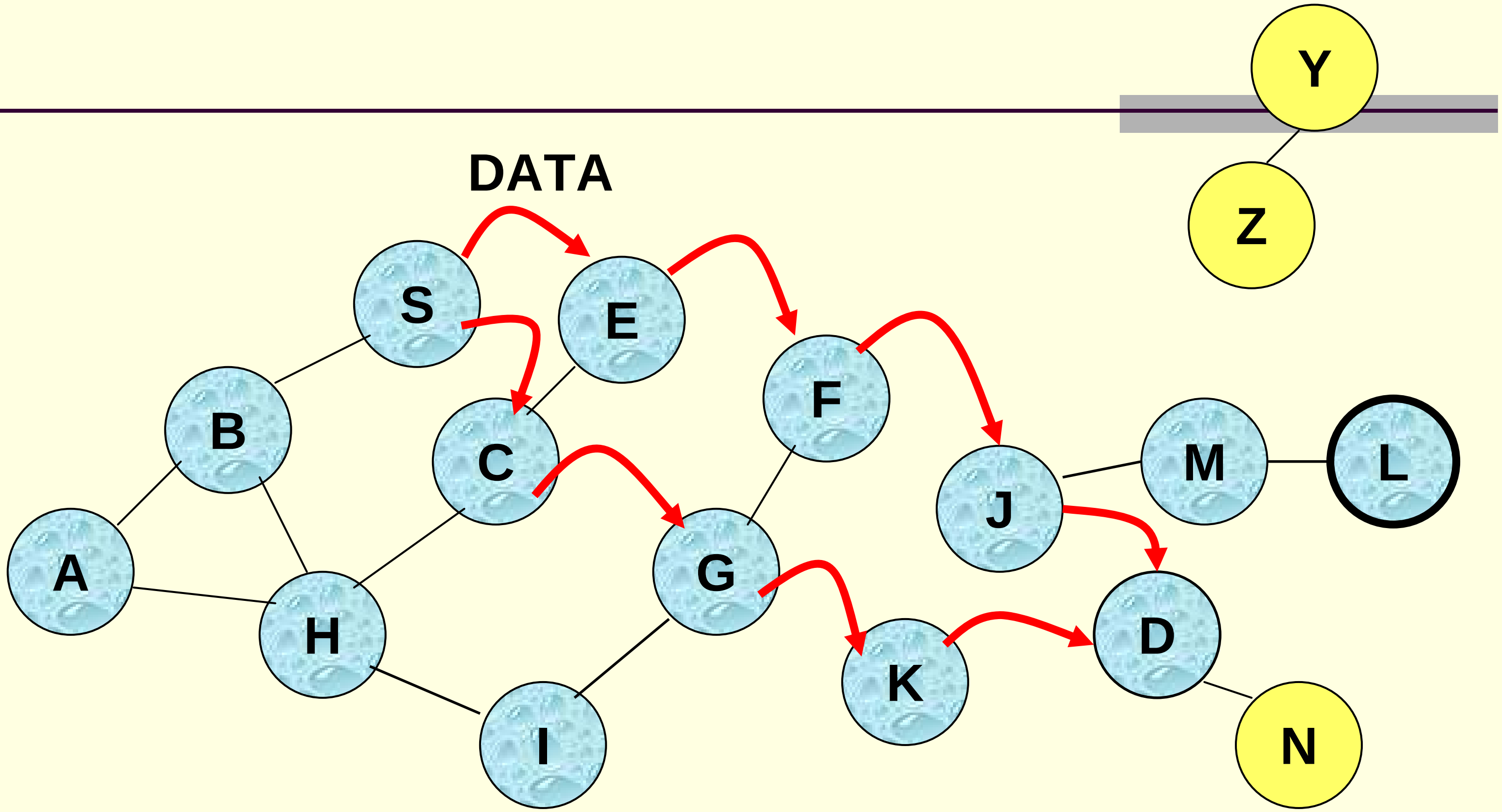


  - Neighbor-designating

    Self-Pruning, MPR (MultiPoint Relay), TBRPF

Drawback of above schemes: Background traffic O/H to exchange information between neighbors

Find Multi-paths

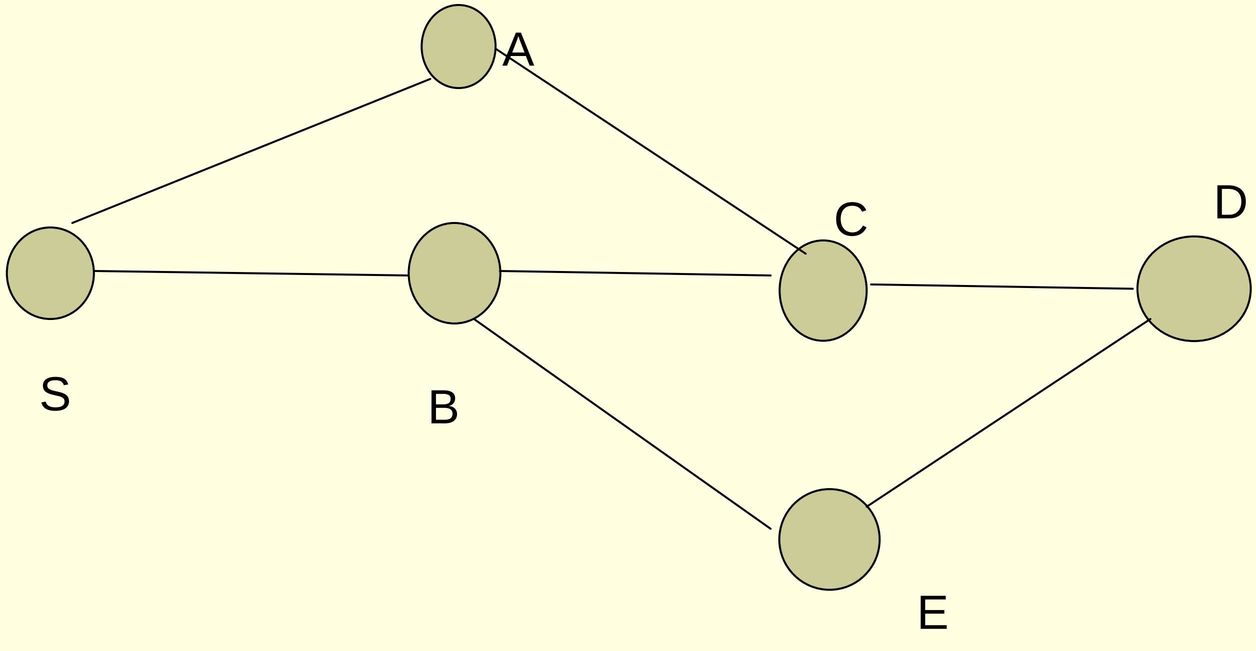


Benefits of multiple node-disjoint paths:

- improving the reliability of the transmitted information
- providing load balance capability

Difficulty with Current Approaches

- Using the current method, we may only find one route {S->B->C->D}, however two routes are possible: {S->A->C->D} and {S->B->E->D}.
- We need a better way to find all possible paths.



Comparison of Protocols

	DSDV	AODV	DSR
Reliability	▪ Link and Network Layer Detection ▪ Routes may be chosen based on stale information	▪ Able to detect topology changes within a few seconds ▪ Link Layer Detection	▪ Takes slightly longer due to non passive acknowledgement but change is propagated very fast ▪ Link and Network Layer Detection
Effectives – Resource Usage	▪ Computationally more efficient ▪ High waste of bandwidth ▪ ineffective for rapid topological changes	▪ Route Table ▪ Less computation intensive ▪ Less wastage of bandwidth by only one hop periodic broadcast	▪ Route Cache ▪ Computation intensive ▪ Flooding only during Route Discovery
Scalability	Poor Scalability	▪ More scalable	▪ Less scalable – Suitable for small and medium sized networks due to packet header
Latency	No	Yes	Yes
Overhead	Yes	Less	Less

Thank you