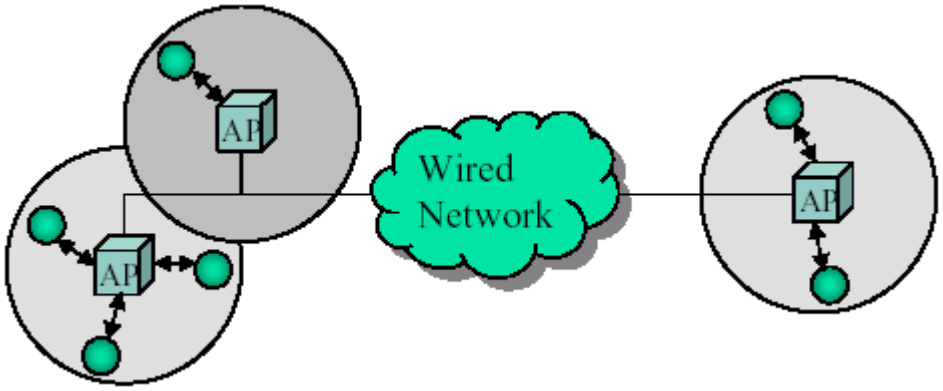
Mobile Ad-Hoc Networks

Carleton
UNIVERSITY
Canada's Capital University

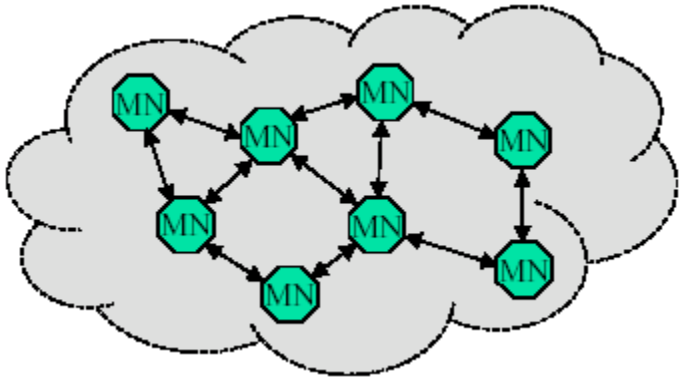
One Type of Wireless Networks: "Infrastructure-based"

- Infrastructured wireless networks
  - Cellular Networks and Wireless LAN
  - Fixed, wired backbone and centralized control
  - Mobiles communicate directly with access points (AP)
  - Suitable for locations where APs can be deployed

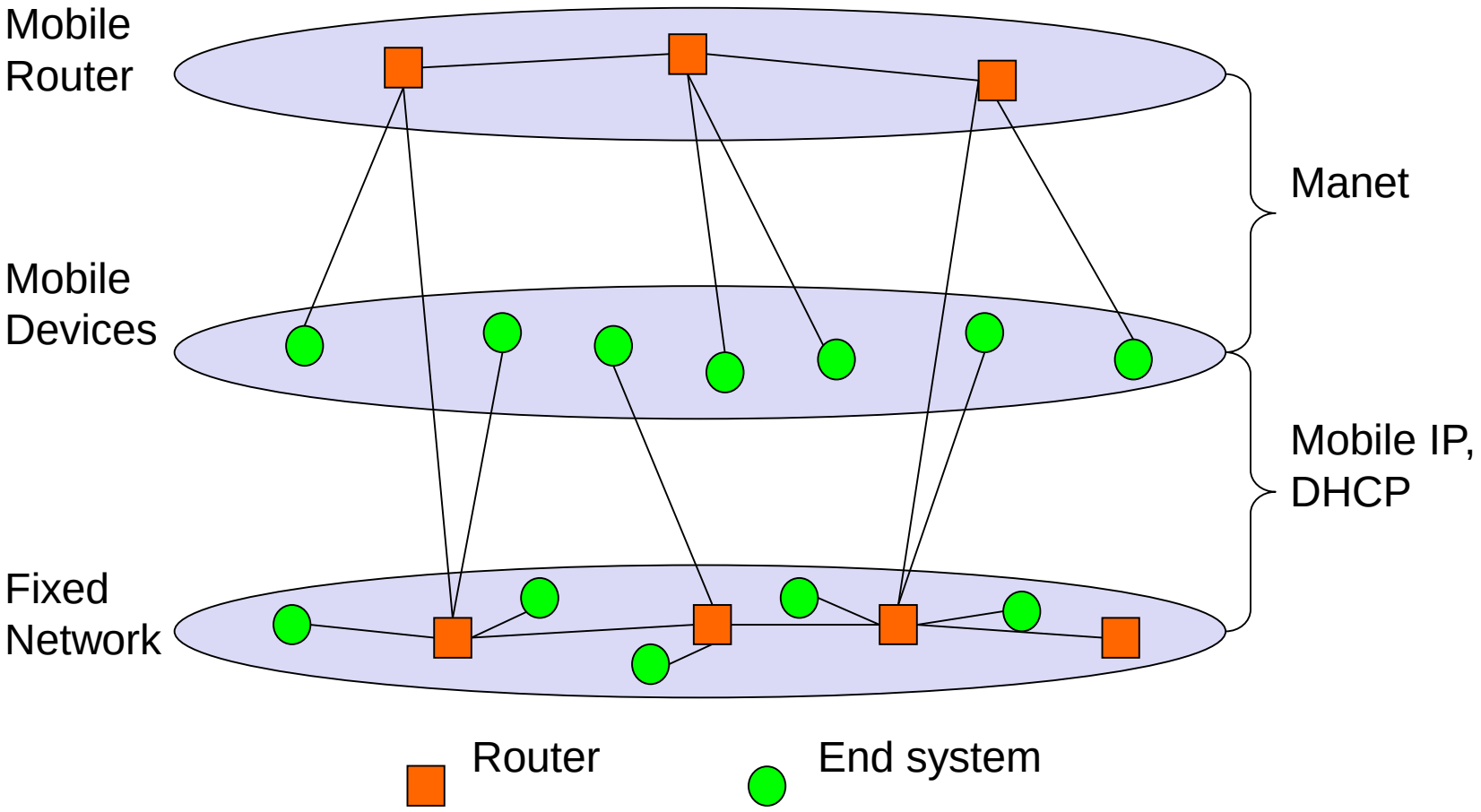


Another Type of Wireless Networks: "Infrastructure-less"

- (Mobile) Ad-Hoc Networks
  - Neither pre-existing, wired backbone nor centralized administration
  - Peer-to-Peer and self-organizing networks
  - Each mobile serves as routers, not just an end point.
- Mesh: has wireless infrastructure (multihop wireless)
  - Maintains separation between (mobile) routers and end hosts
- Wireless Sensor Networks: mostly static topology, no separation between routes and sensors, multihop wireless



Manet: Mobile Ad-hoc Networking

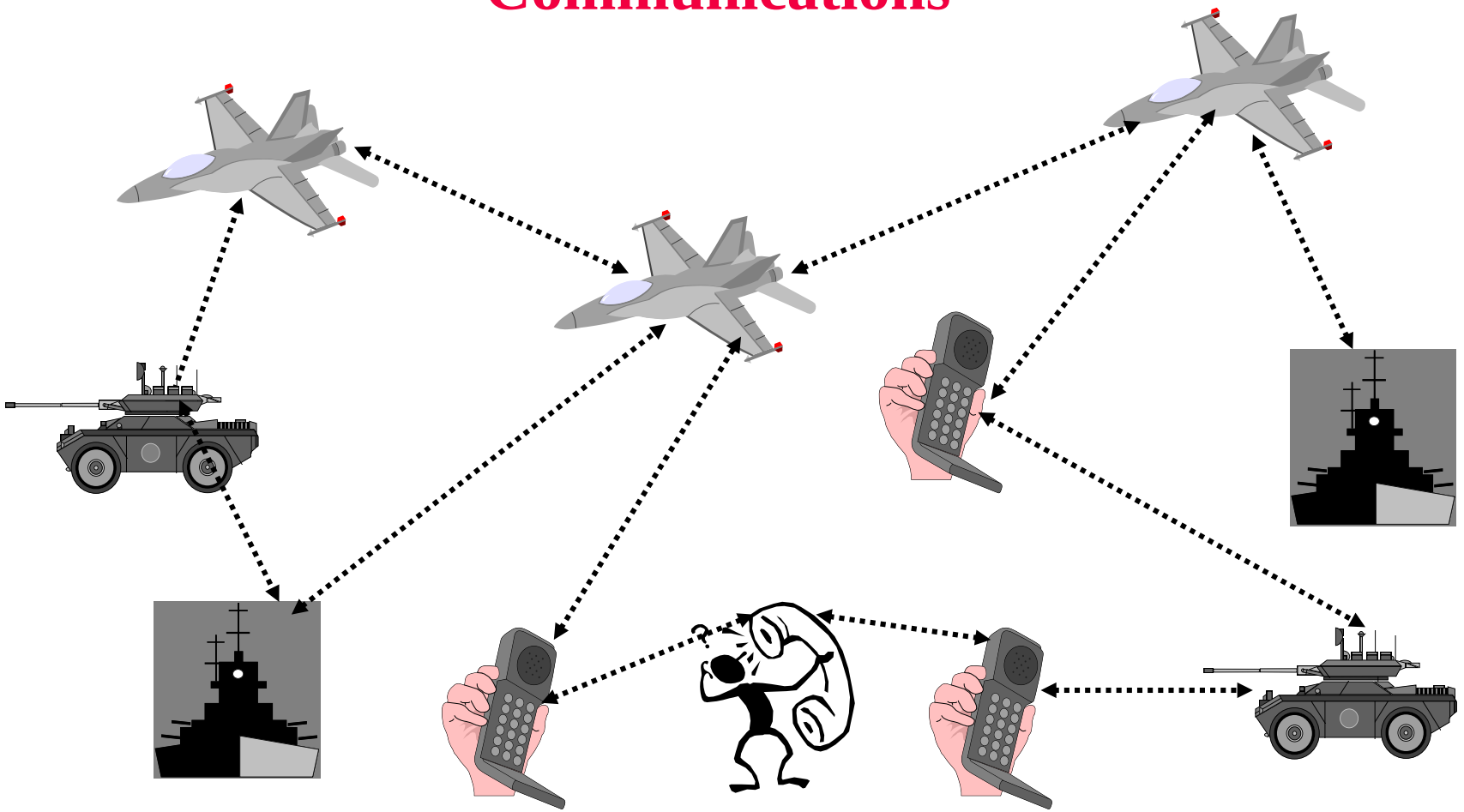


Ad hoc Networks

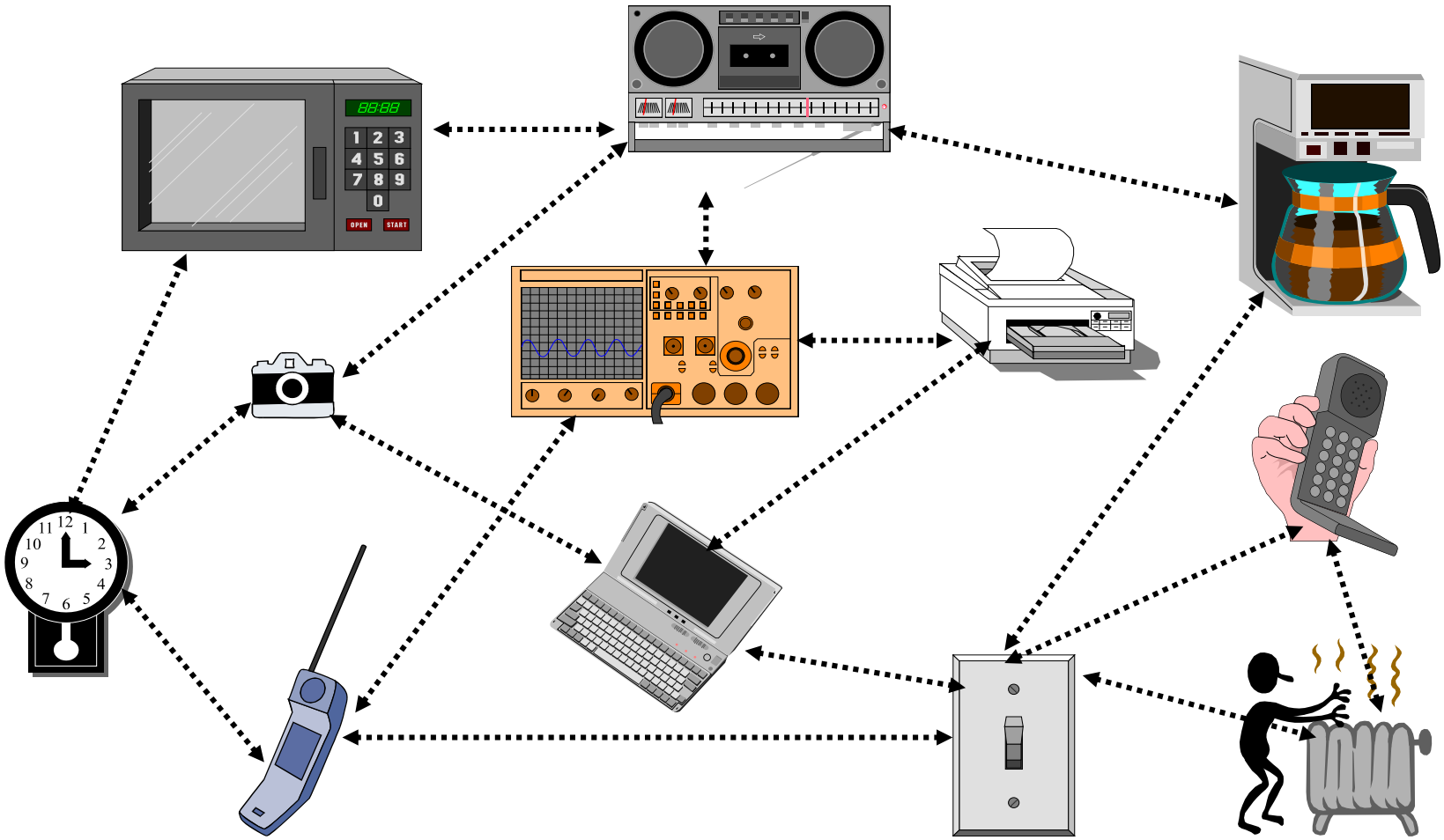
- In Latin, “ad hoc” literally means "for this purpose only”
- It can be regarded as a “spontaneous network”
- A Mobile Ad-hoc NETwork (MANET) is a collection of mobile nodes which communicate over radio and do not need any pre installed communication infrastructure.
- Mobile, multihop wireless network capable of autonomous operation
- Communication can be performed if two nodes are close enough to exchange packets.

Carleton UNIVERSITY
Canada's Capital University

Use of the Ad-Hoc Technology for Military Communications



Ubiquitous Networking

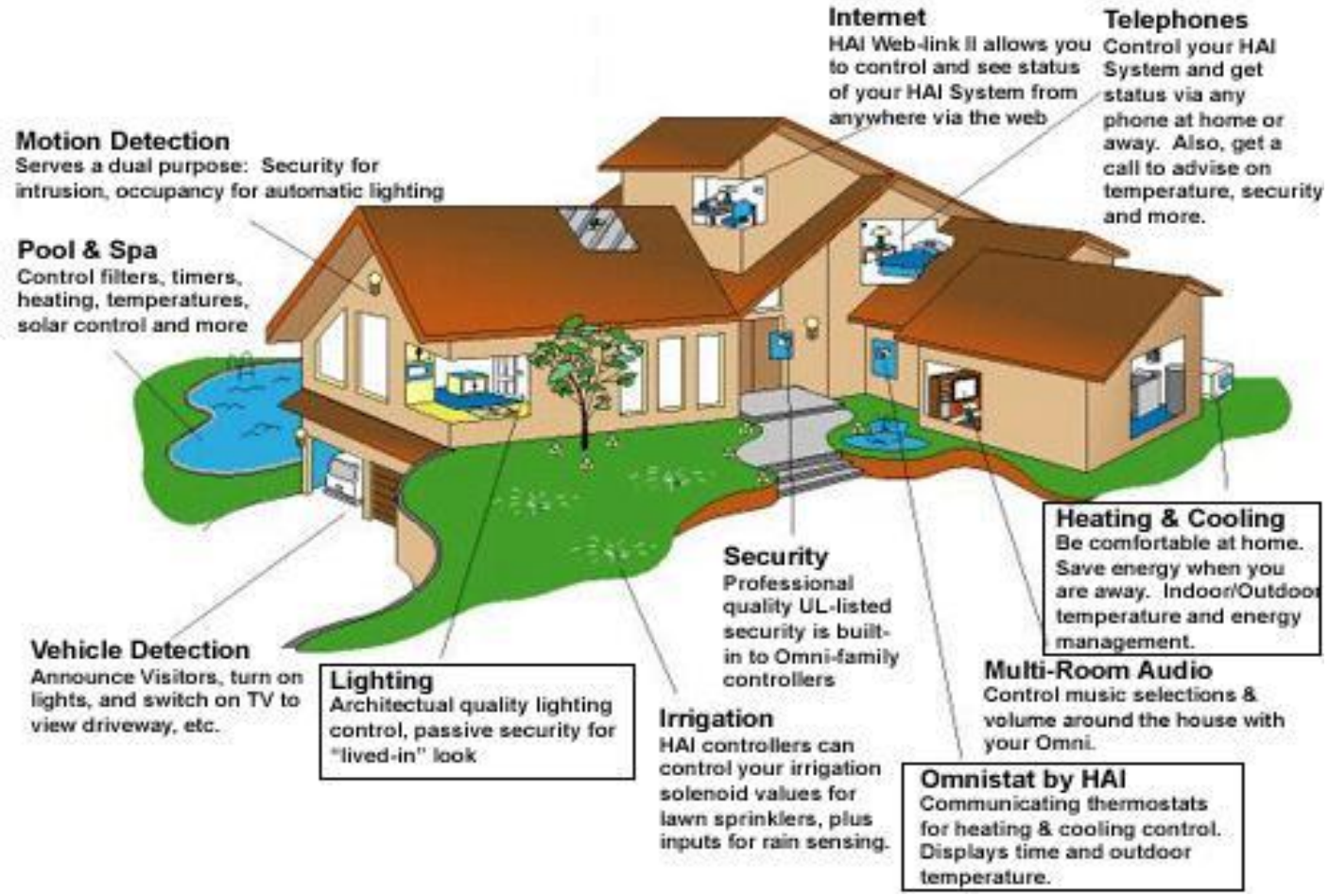


Applications – "Aging in Place"

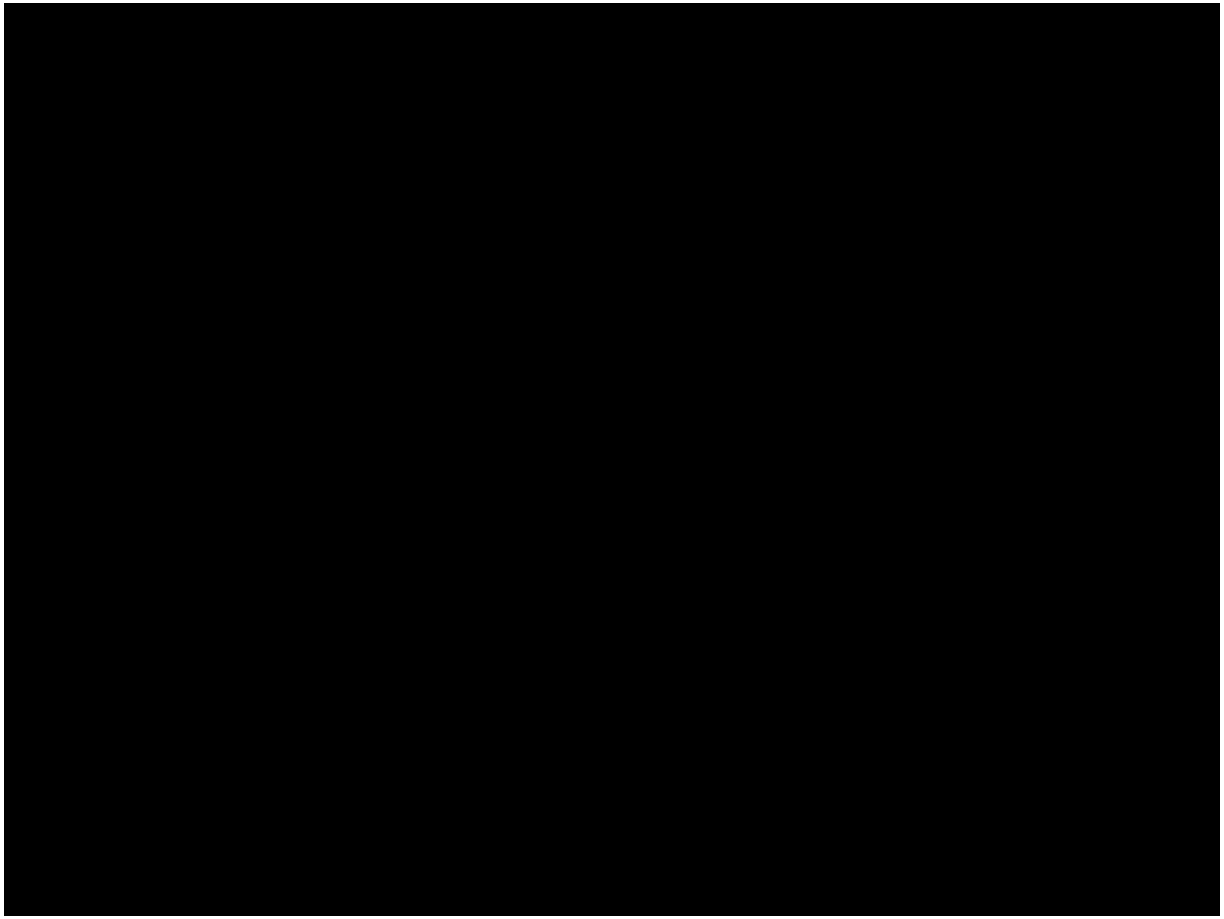
- World's population is aging fast
  - fertility rates are decreasing across the 'Developed World'
  - In 1995, 6.5% of the world's population was over 65*
  - In 2025, 10.7% of the world's population will be over 65*
- Elderly people can be monitored by trusted third parties (e.g. these could be their own children or professional health care providers) in their own homes
  - new WSN technology provides a convenient and practical health-related monitoring service
  - Monitored subjects are the on-site 'users' and are not computer experts
  - Sensed data could include: room temperatures; sleeping patterns; food consumption; medication consumption; electricity/gas/water usage, occupant movement or position, door/window state, occupant heart rate/blood pressure/body temperature/breathing rate/weight ….

* (U.S. Census Bureau, International Data Base) http://www.census.gov/ipc/www/world.html 2006

Application: Smart Homes



Application: Rural Connectivity



Loon – Internet for Rural/Underserviced Areas (Google Project)

https://www.youtube.com/watch?v=cMS2TKVeQVU
http://www.google.com/loon/where/

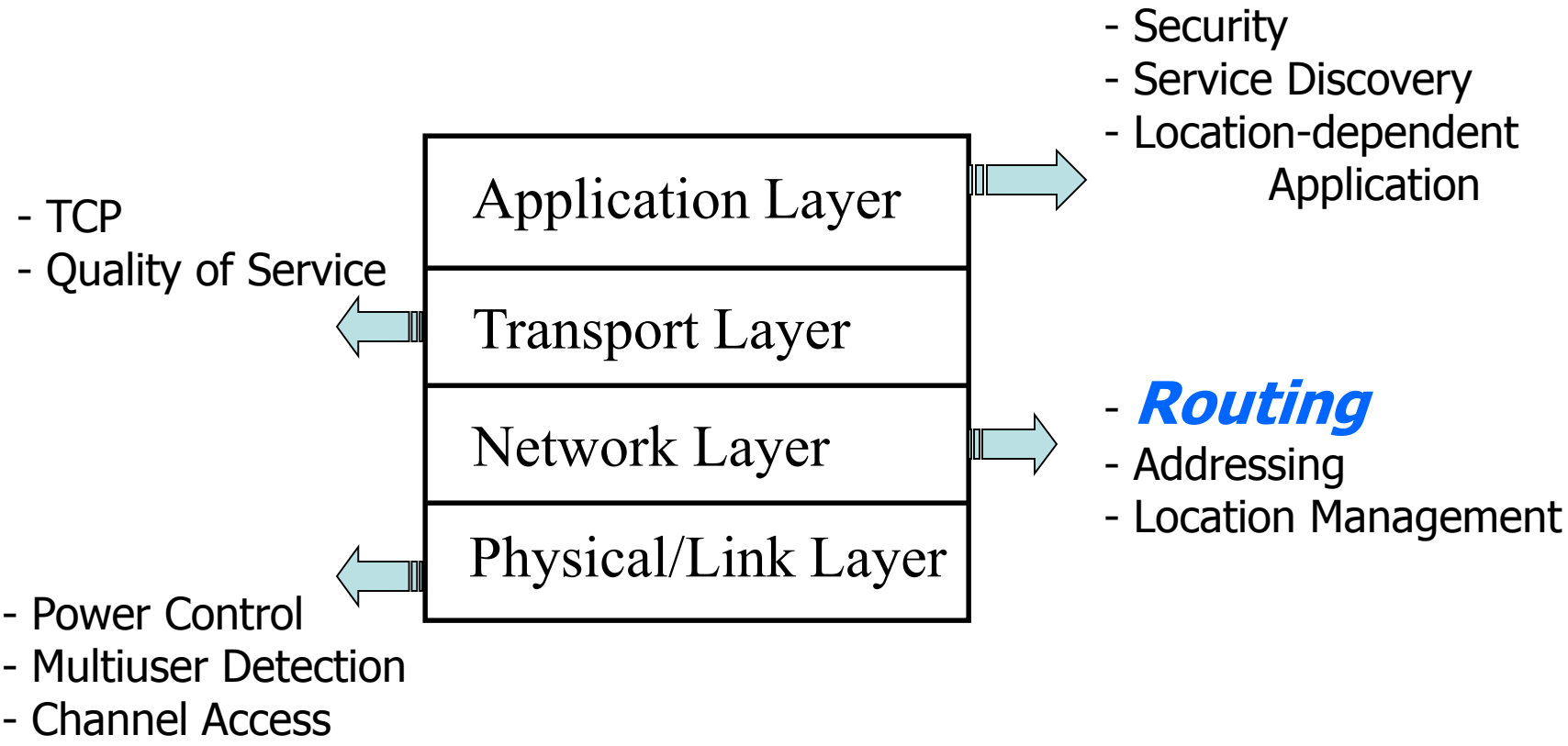
MESH: Why MOBILE Ad-Hoc Networks?

- Mesh, at first sight, as a rather static, albeit multi-hop wireless network
- Mobility of hosts/routers => Dynamic Topology
- Dynamic Topology however does not imply Mobile Network:
  - Nodes come and go
  - Uncontrolled Interference
    - Testbeds show that IEEE 802.11 links are highly asymmetric due to different interference environment at receiver and variable over time
- Personal Opinion: Mesh Community Networks will have many of the same challenges and will benefit from same solutions as MANETs
  - Deal with dynamic topology
  - Little to no configuration/peer-to-peer operation

Challenges in Ad-Hoc Networks

- The challenges in the design of Ad-Hoc networks stem from the following facts:
  - the lack of centralized entity ⇒ self-organizing and distributed protocols
  - the possibility of rapid platforms movement (highly versatile topology) ⇒ efficient and robust protocols
  - all communication is carried over the wireless medium ⇒ power and spectrum efficient communications
- Compare this with the fixed (cellular) networks …

"Mobile Ad Hoc Networking is a multi-layer problem !"



Medium Access Control in MANET

Some interesting issues, but skipped here
Most testbeds use IEEE 802.11x, which works in multihop environment, though it was not designed for that scenario.

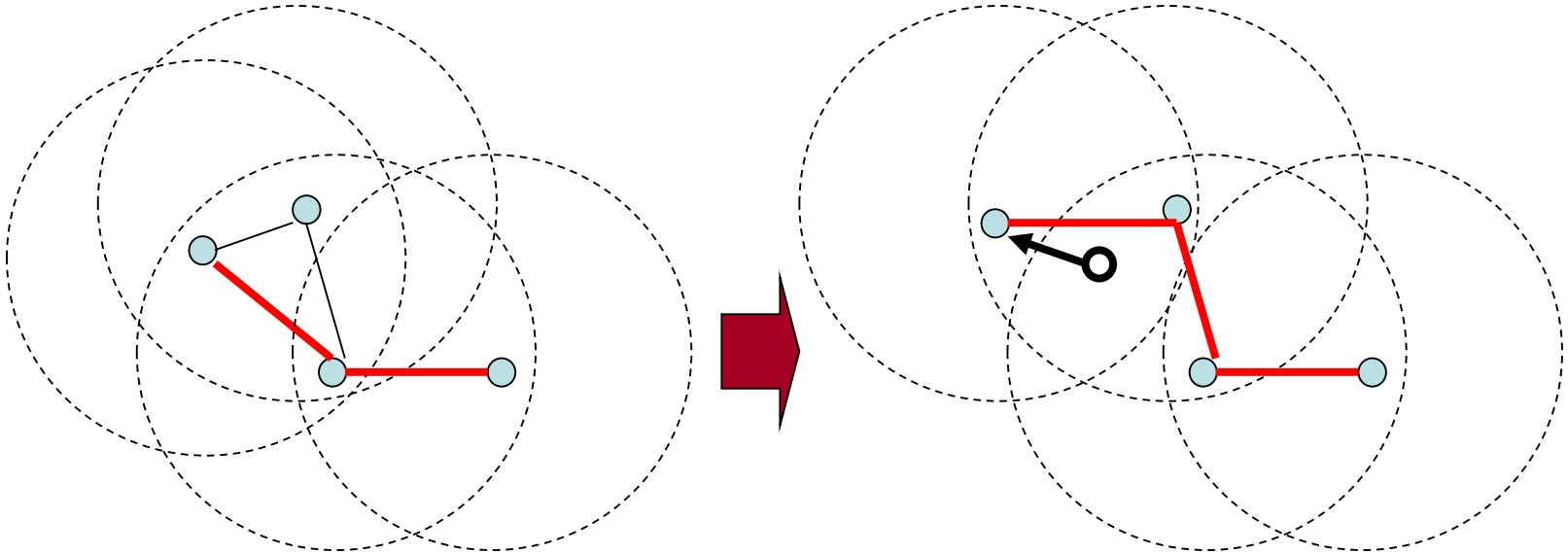
Network Layer in MANET

Has been the focus of past research

Particularly: Routing

Main Issue – "Routing"

- If there is NO direct link between a source and a destination, multi-hop routing is needed to discover their routes.
- Routing is a very challenging task in mobile ad hoc networks.
  - Mobility and link failure/repair may cause frequent route changes.
  - Routing protocol must be distributed, with minimal overhead.



Routing: What Communication Paradigm/Pattern?

- Unicast: one sender, one receiver
- Multicast: one (or multiple) sender, many receivers
- Broadcast: one sender, all nodes receive
- Geocast: one sender, receivers determined by location rather than address
- Anycast: one sender, K out of M receivers need to receive packets
- Reliable vs. unreliable, QoS vs. Best Effort

Approaches to Routing in MANET

- Key challenge: routing requires knowledge of topology, but topology changes, tracking/reacting to changes induces overhead

- Do nothing, flood data to all nodes
- "Mimic Internet routing protocols" -> build routing tables
  - Different ways of doing that, see later
- Fuzzy approaches: random walks
- Geographic routing

Ad hoc Routing Protocols

- Routing problem has received a significant interest in the research community, resulting in several protocols proposed.
  - Some have been invented specifically for MANET.
  - Others are adapted from traditional routing protocols for wired networks (i.e., distance vector or link state algorithms)
    - These traditional protocols do not work efficiently or fail completely.
- The main group of proposals comes from the work of IETF's MANET working group
  - Designed for IP based, homogeneous, mobile ad hoc networks.
  - Focuses on fast route establishment and maintenance with minimal overhead
    - Number of hops is used as the only route selection criteria.
    - Other parameters, such as energy usage or QoS, are not considered.

Ad-Hoc Networking: MANET

- Mobile Ad-hoc Networks (manet) at IETF: http://www.ietf.org/html.charters/manet-charter.html
  - A "mobile ad hoc network" (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links
  - routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably
- The primary focus of the working group is to develop and evolve MANET routing specification(s) and introduce them to the Internet Standards track. The goal is to support networks scaling up to hundreds of routers.
- More recently: standardize routing protocol components/building blocks (jitter, packet formats, neighbor discovery), also develop version 2 of protocols…

Routing Protocols - Design

- Proactive, Table-driven Approach
  - Based on traditional link-state and distance-vector routing protocols.
  - Continuously update the topological view of the network by periodically exchanging appropriate information among the nodes.
  - Determine routes independent of traffic pattern
  - Examples: DSDV, OLSR (Optimized Link State), TBRPF etc.
- Reactive, On-demand Approach
  - Discover and maintain routes only if needed
  - Do not continuously maintain the overall network topology
  - The network is flooded with "route request" control packets when a new route is required.
  - Examples: DSR, AODV, LAR, etc.
- Hybrid Approach
  - Combine the two approaches above: locally proactive, globally reactive !
  - Example: ZRP

Trade-Off

	Proactive Approach	Reactive Approach
Route Latency	**Lower** ■A route is kept at all times	**Higher** ■A route is never kept when not used
Routing Overhead	**Higher** ■A frequent dissemination of topology information is required	**Lower** ■Fewer control packets in general

- Various simulation studies have shown that reactive protocols perform better in mobile ad hoc networks than proactive ones.
  - However, no single protocol works well in all environments.
  - Which approach achieves a better trade-off depends on the traffic and mobility patterns.

MANET Routing Protocols

- Protocols (best-effort unicast routing protocols):
  - On-demand protocols
    - AODV (RFC 3561, currently a draft for version 2)
    - DSR (RFC 4728)
  - Pro-active protocols
    - OLSR (Version 1: RFC 3626, Version 2: RFC 7181)
    - TBRPF: Topology Dissemination Based on Reverse-Path Forwarding (RFC 3684)
  - Mixed modes:
    - Fisheye state routing
    - Zone routing

Leading MANET Contenders

- DSR: Dynamic Source Routing
  - Source routing protocol
  - Complete path in packet header
- AODV: Ad-hoc On-demand Distance Vector Routing
  - "Hop-by-hop" protocol
  - Uses only standard IP packets, intermediate nodes maintain routing table
  - A variant is used in mesh networks (IEEE 802.11s) and Zigbee networks
- Both are "on demand" protocols: route information discovered only as needed
  - Two phases: route discovery and route maintenance
  - Difference: in DSR, source controls complete route, in AODV it only knows the next hop
- Military: OLSR (Optimized Link State Routing)
  - Proactive routing protocol
  - Similar to OSPF, but more efficient link state updates

AODV and DSR Routing

- Will look (briefly) at the operation of both protocols
- Highlight only most common/characteristic features
- Newer drafts/RFCs propose additional details

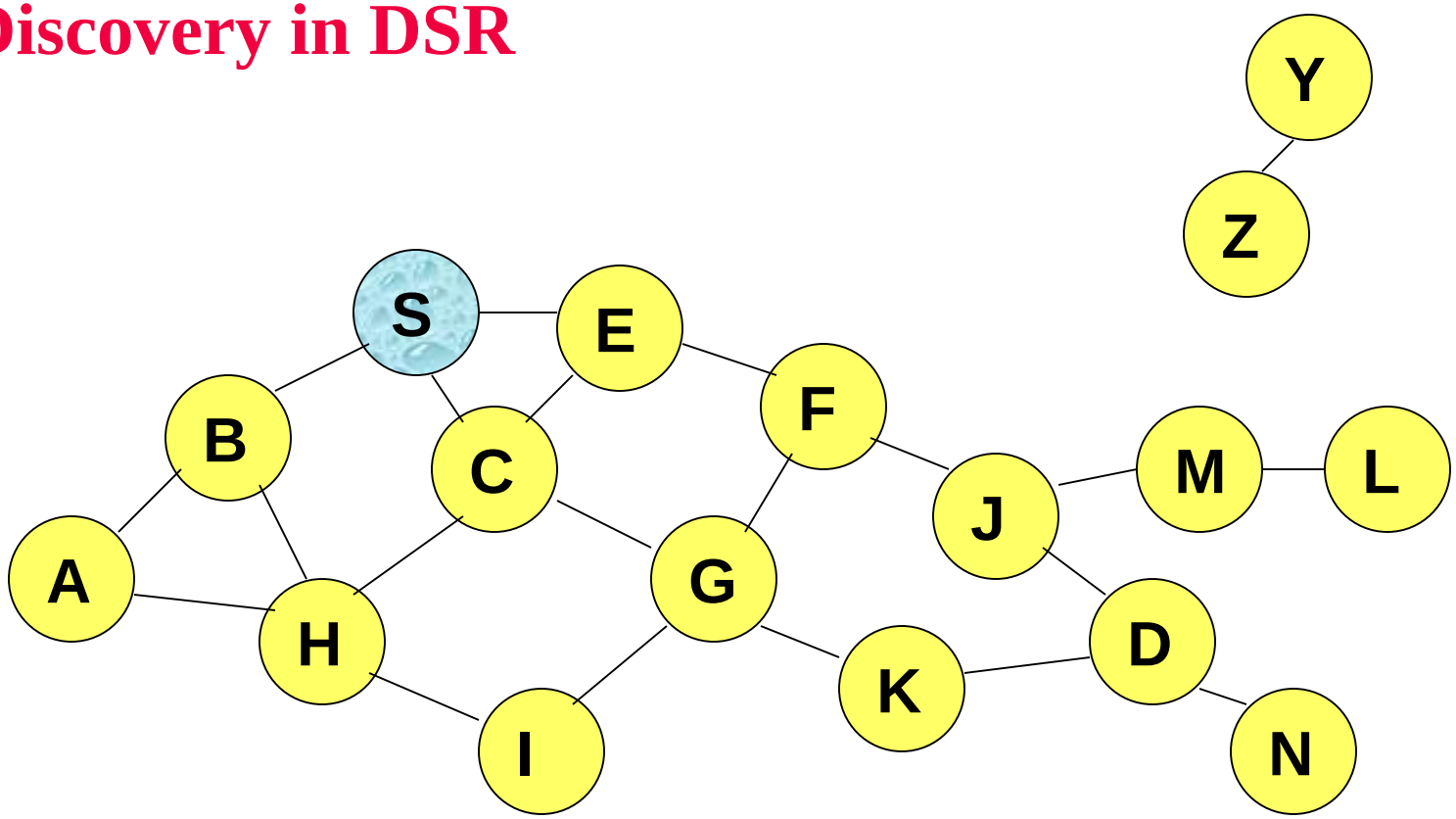
DSR: Dynamic Source Routing

- Source Routing: sender of packet determines complete sequence of nodes along path and lists them in packet header
- use dynamic route discovery to determine path
- advantages:
  - no periodic routing advertisement messages
    - saves bandwidth when there is little change in network
    - saves battery power (no need to send/receive messages)
  - ad-hoc networks have many redundant links, which cause flooding of routing messages
  - no assumption of link symmetry
  - possible to react to changes faster than state-based or distance-vector based protocols
  - better opportunities for route caching and maintenance of alternative routes, compared to AODV

Dynamic Source Routing (DSR)

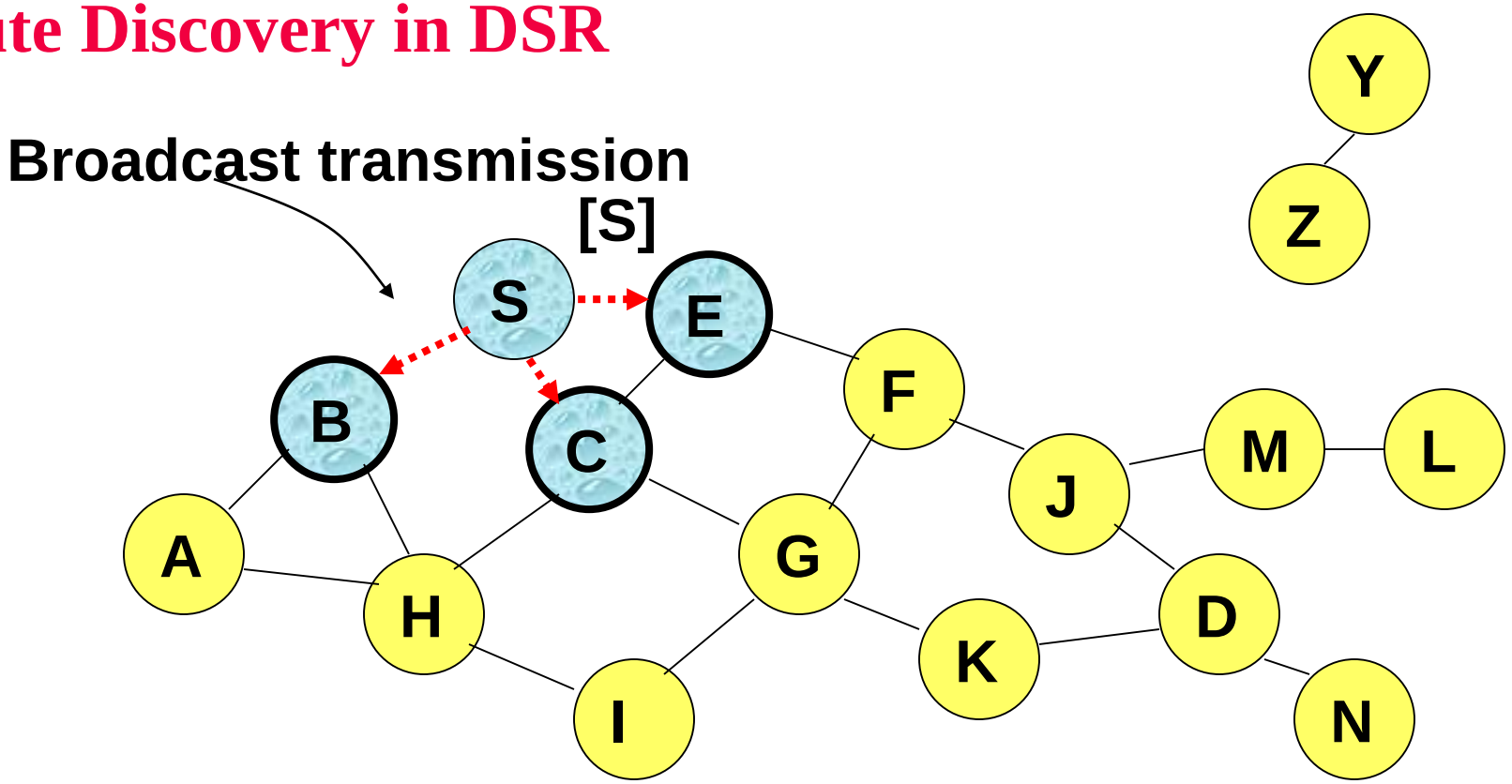
- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a route discovery
- Source node S floods Route Request (RREQ)
- Each node appends own identifier when forwarding RREQ

Route Discovery in DSR



Represents a node that has received RREQ for D from S

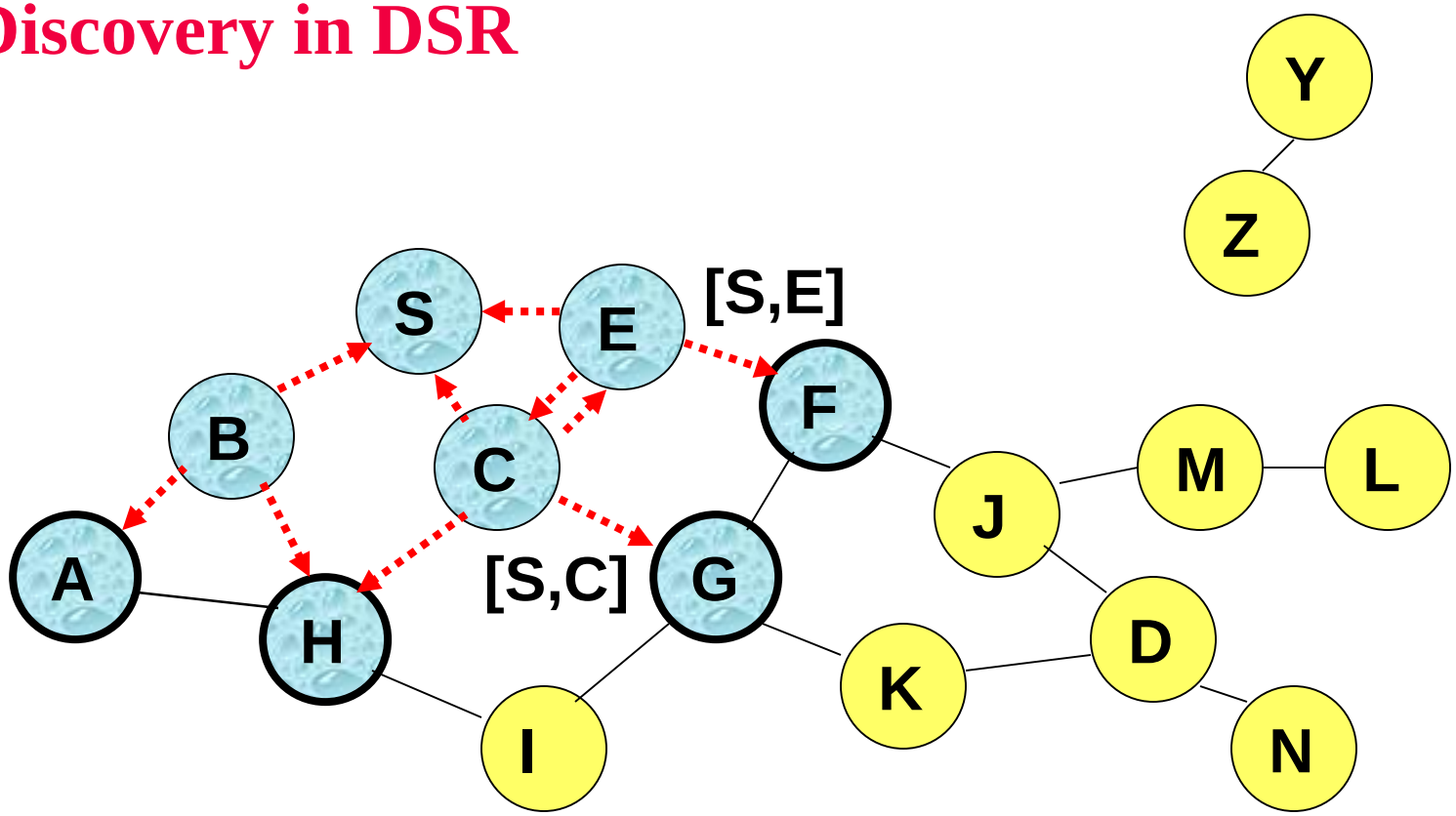
Route Discovery in DSR



Represents transmission of RREQ

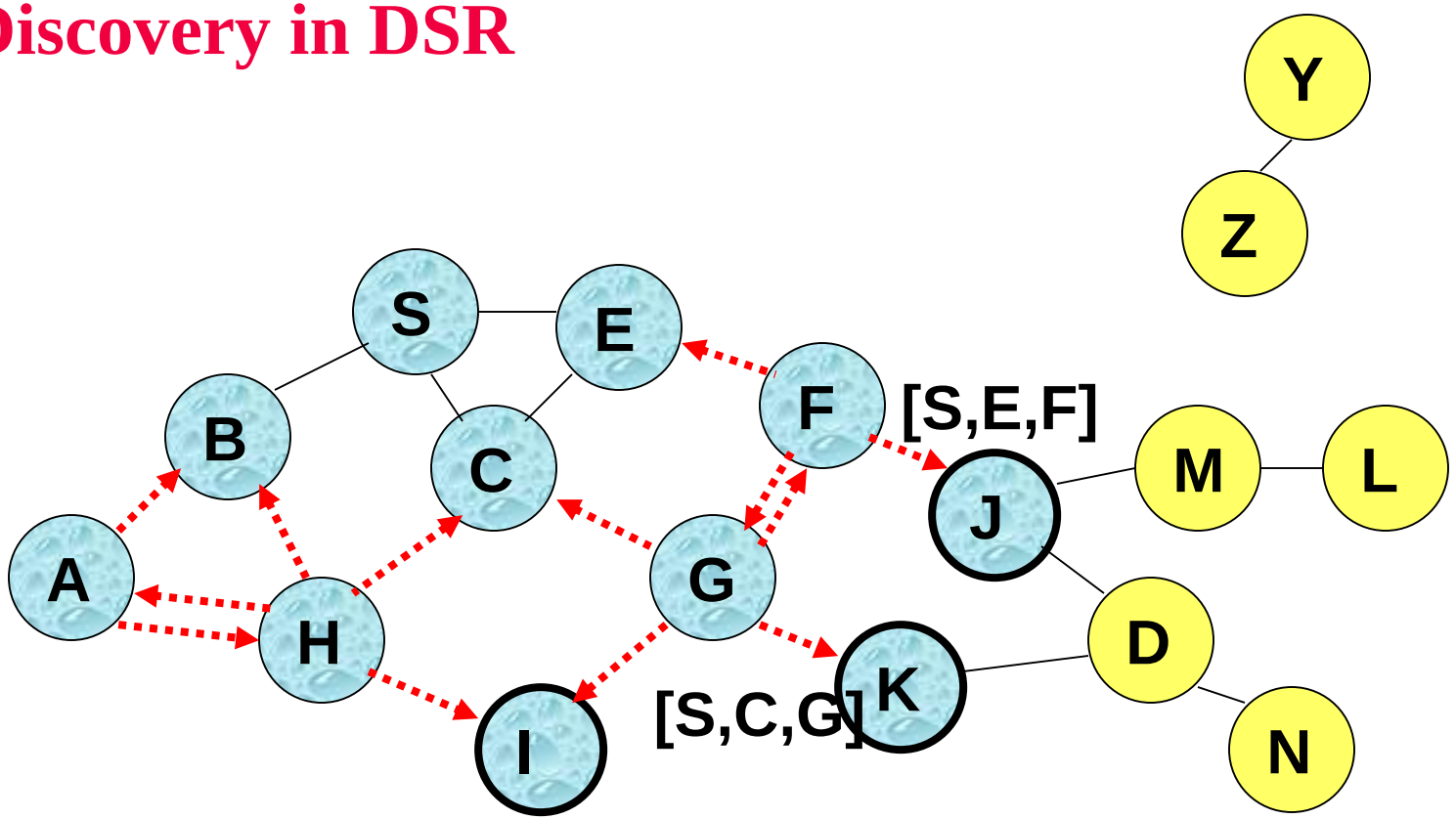
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



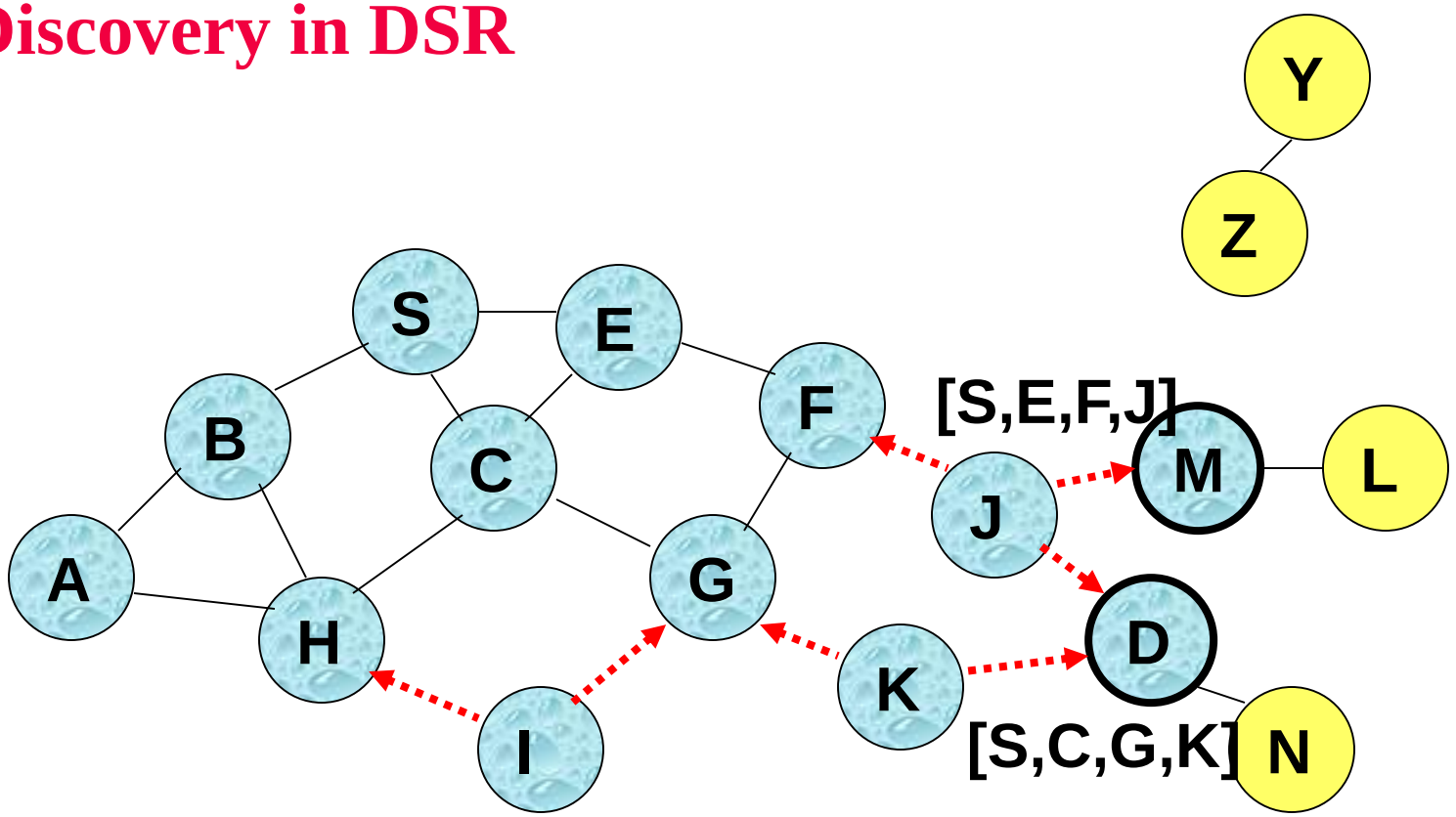
- Node H receives packet RREQ from two neighbors: potential for collision

Route Discovery in DSR



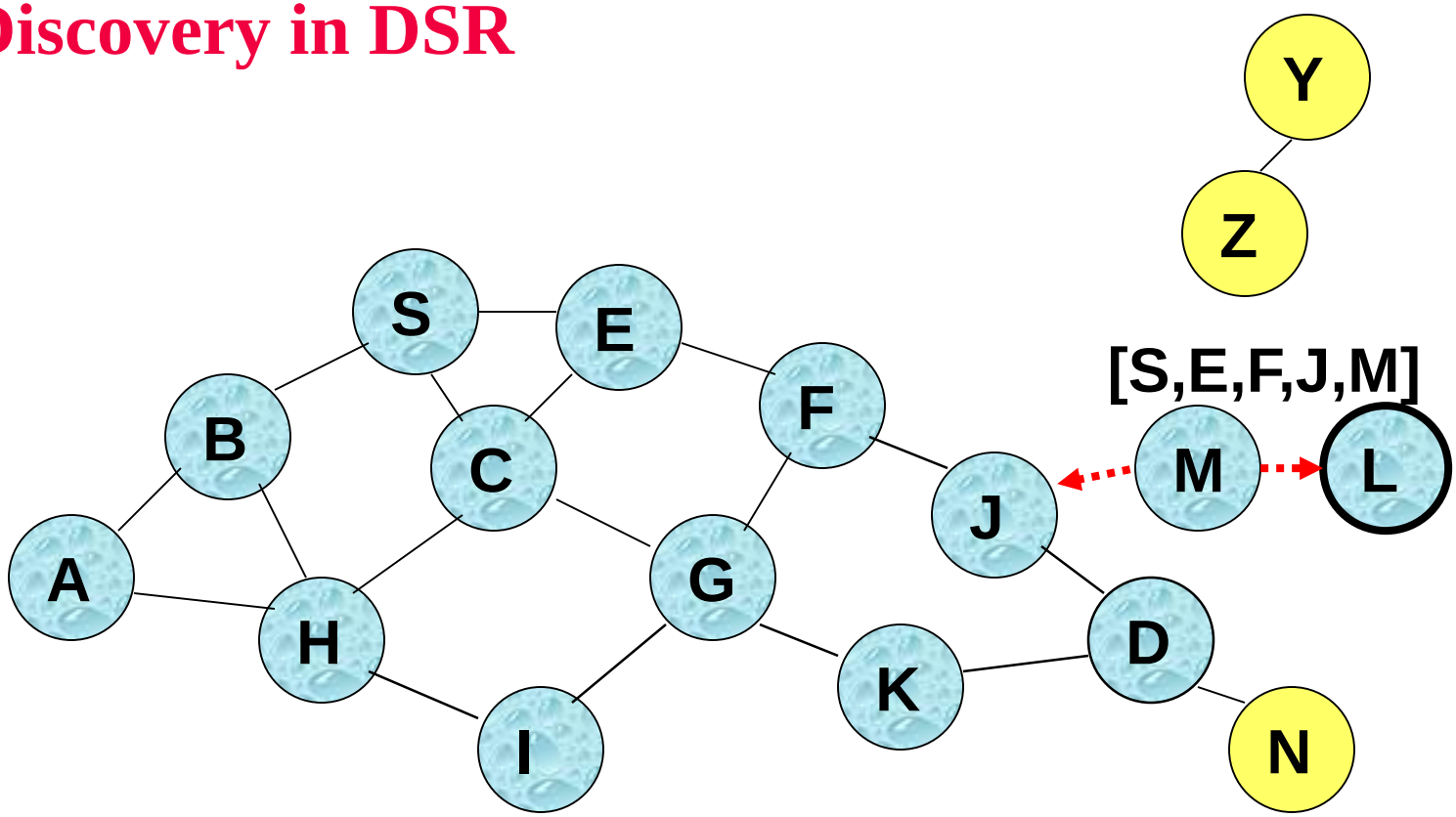
- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

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

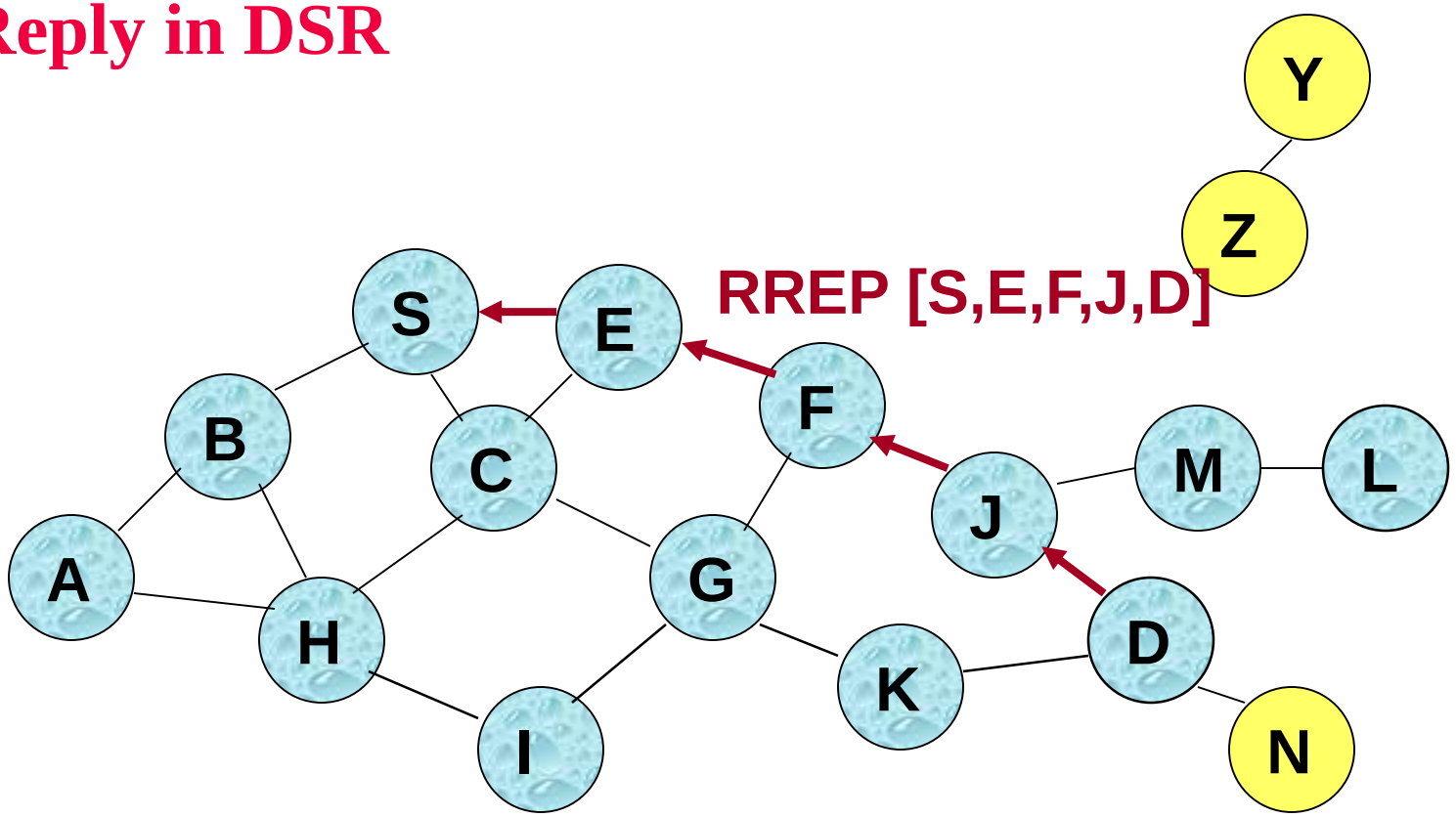


- Node D does not forward RREQ, because node D is the intended target of the route discovery

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

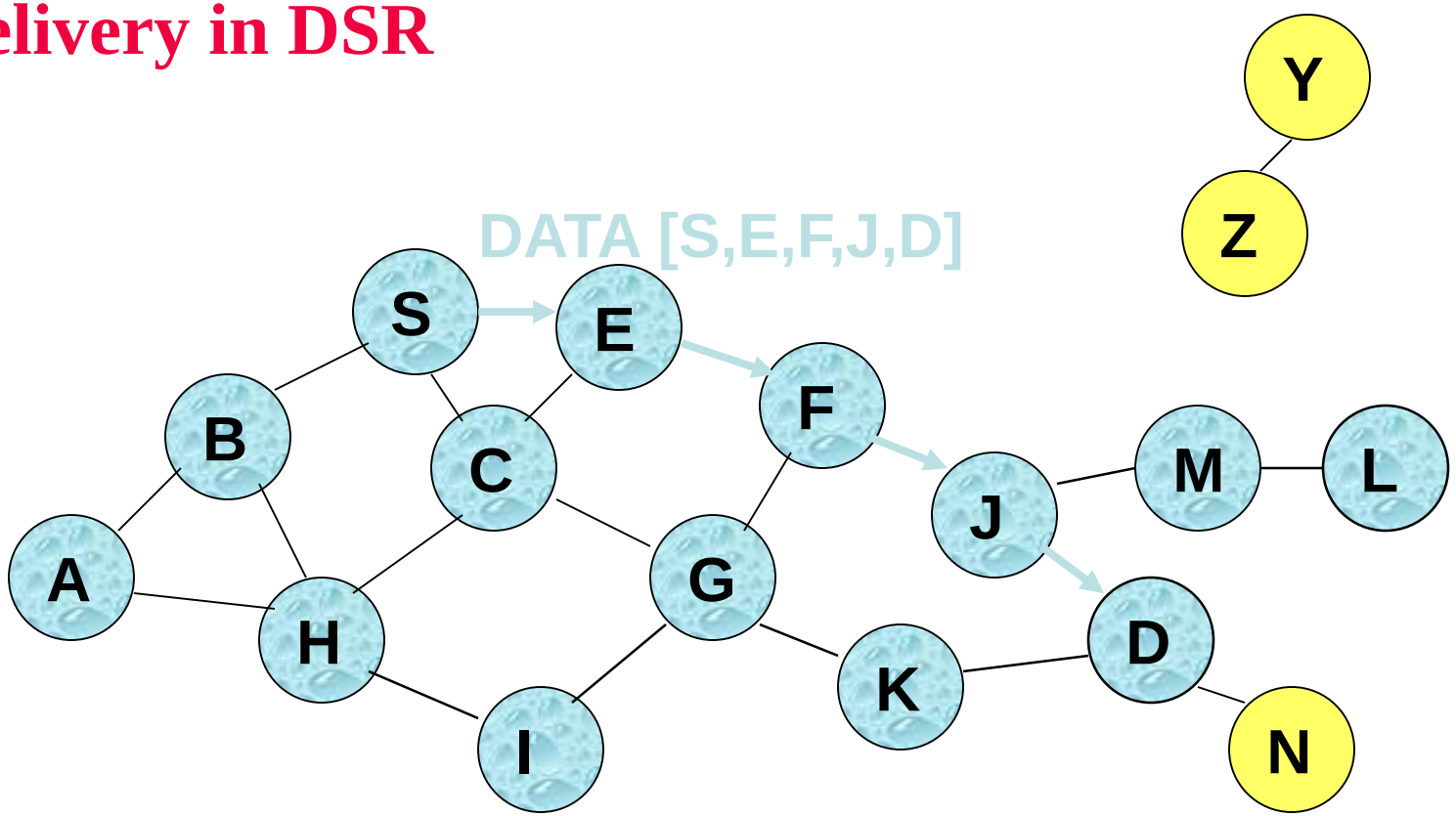
Route Reply in DSR

- 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

Data Delivery in DSR

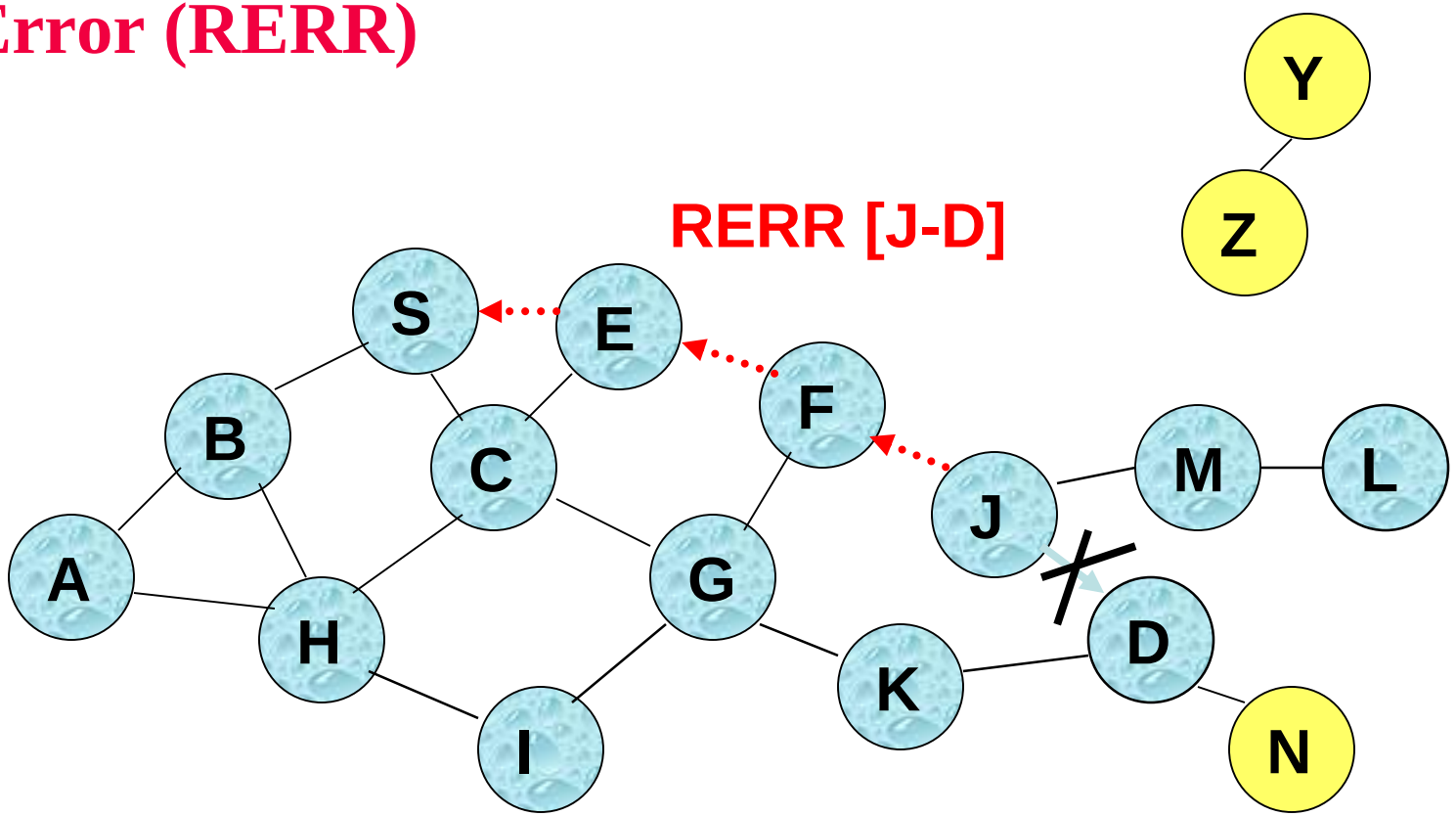


Packet header size grows with route length

When to Perform a Route Discovery

- When node S wants to send data to node D, but does not know a valid route node D

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 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
- 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
  - Reply storm may be eased by preventing a node from sending RREP if it hears another RREP with a shorter route

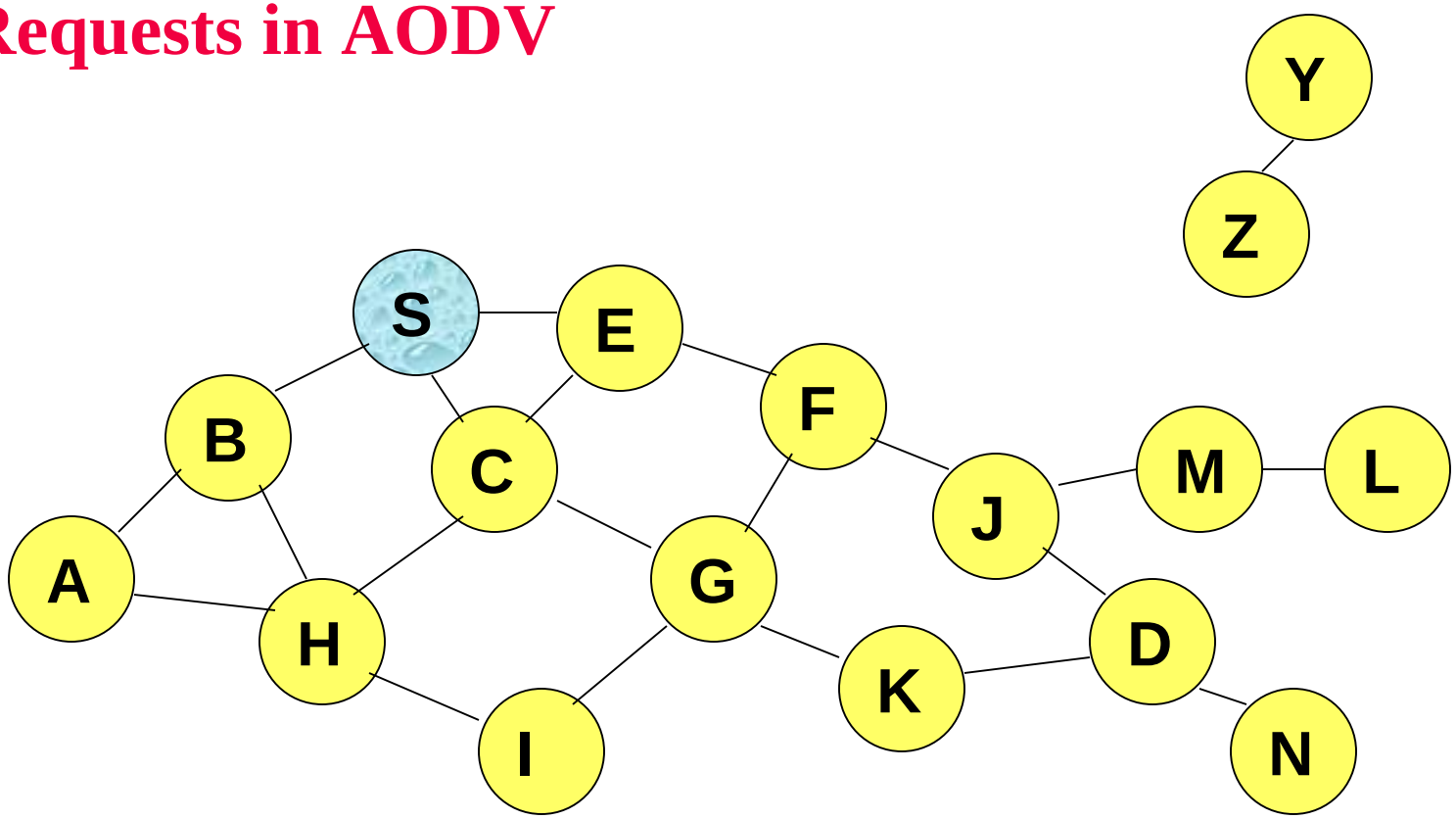
Dynamic Source Routing: Disadvantages

- An intermediate node may send Route Reply using a stale cached route, thus polluting other caches
- This problem can be eased if some mechanism to purge (potentially) invalid cached routes is incorporated.

AODV

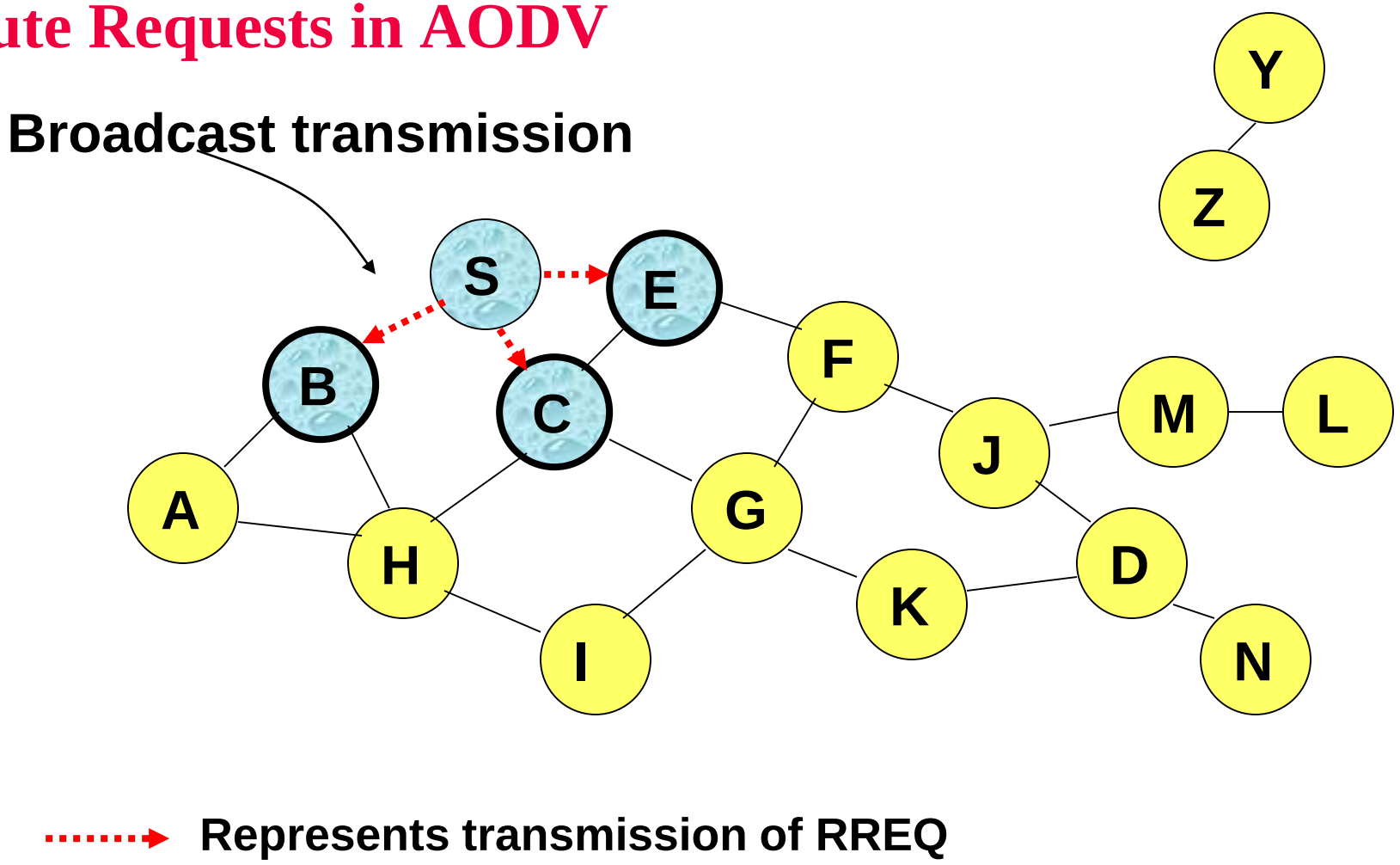
- Route Requests (RREQ) are forwarded via flooding
- When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source
  - AODV assumes symmetric (bi-directional) links
- When the intended destination receives a Route Request, it replies by sending a Route Reply
- Route Reply travels along the reverse path set-up when Route Request is forwarded

Route Requests in AODV

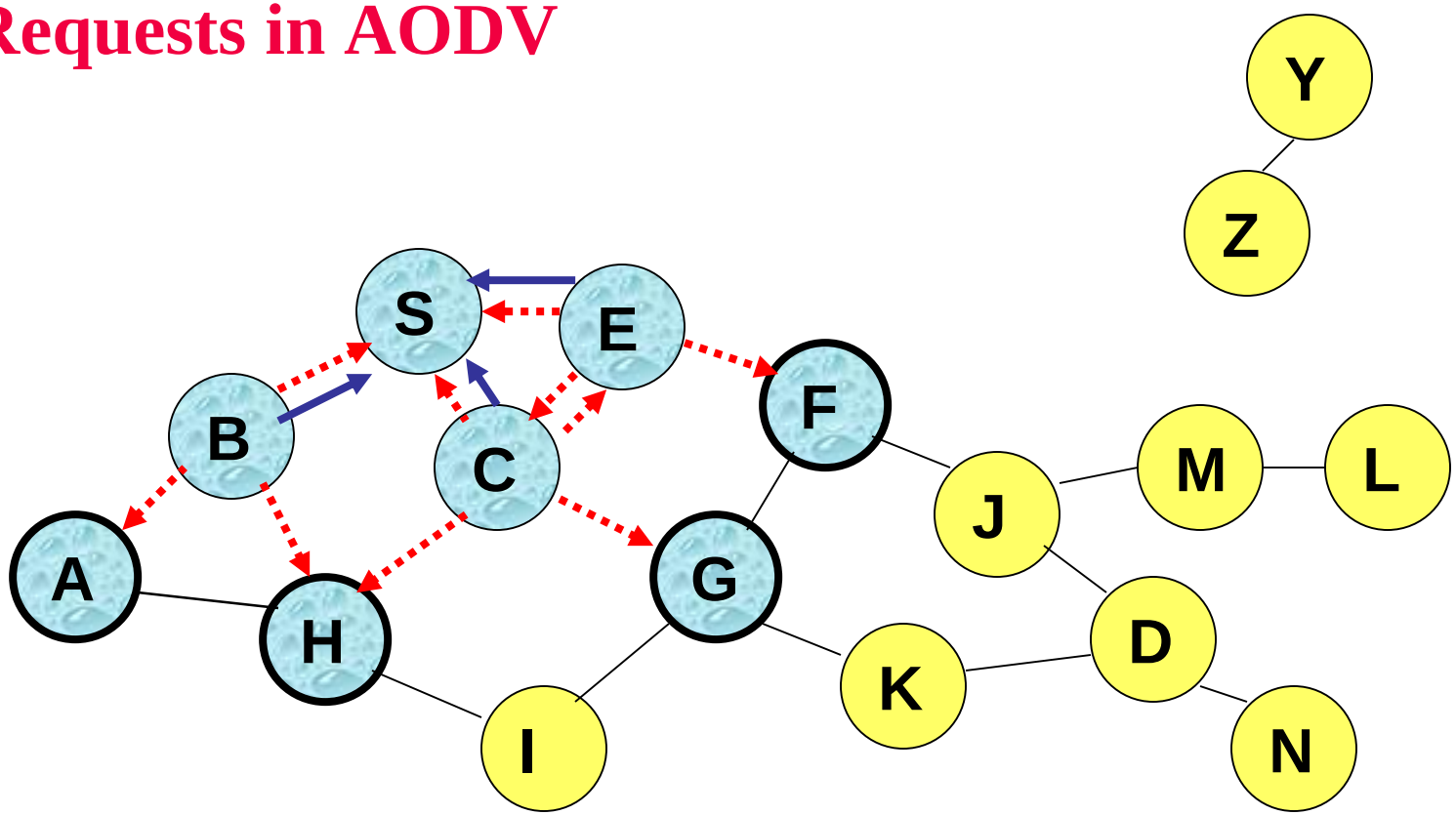


Represents a node that has received RREQ for D from S

Route Requests in AODV

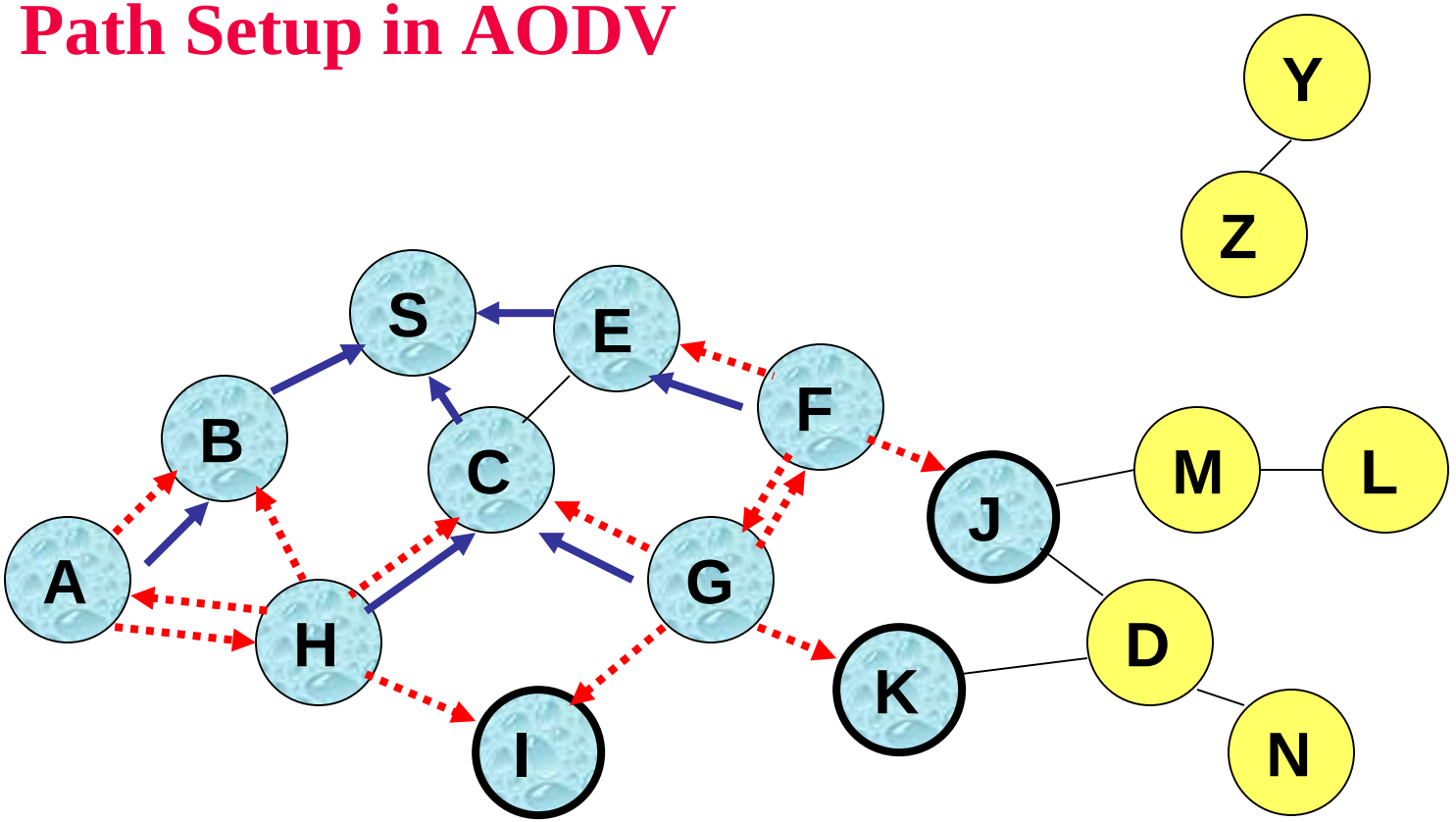


Route Requests in AODV



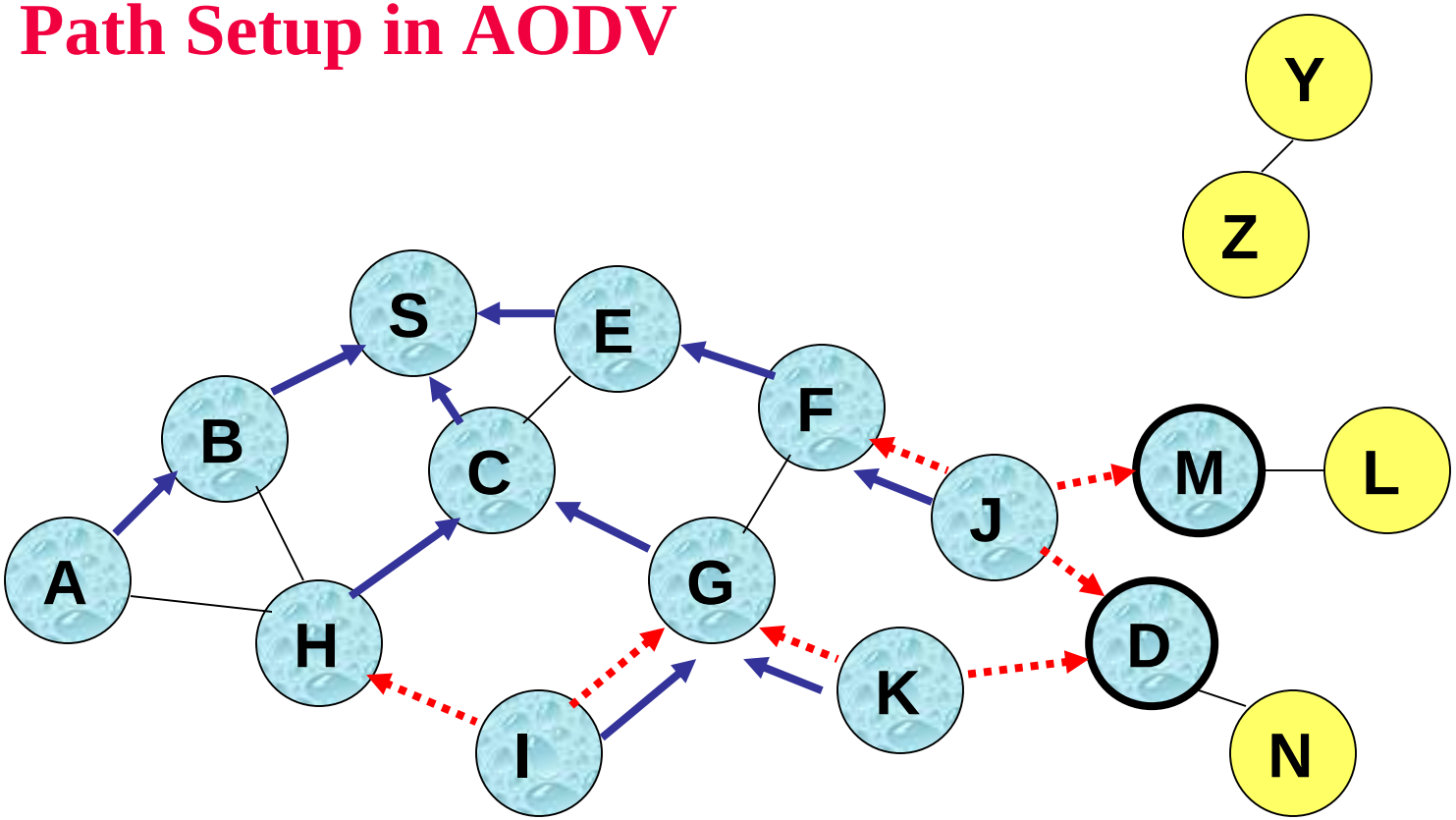
Represents links on Reverse Path

Reverse Path Setup in AODV

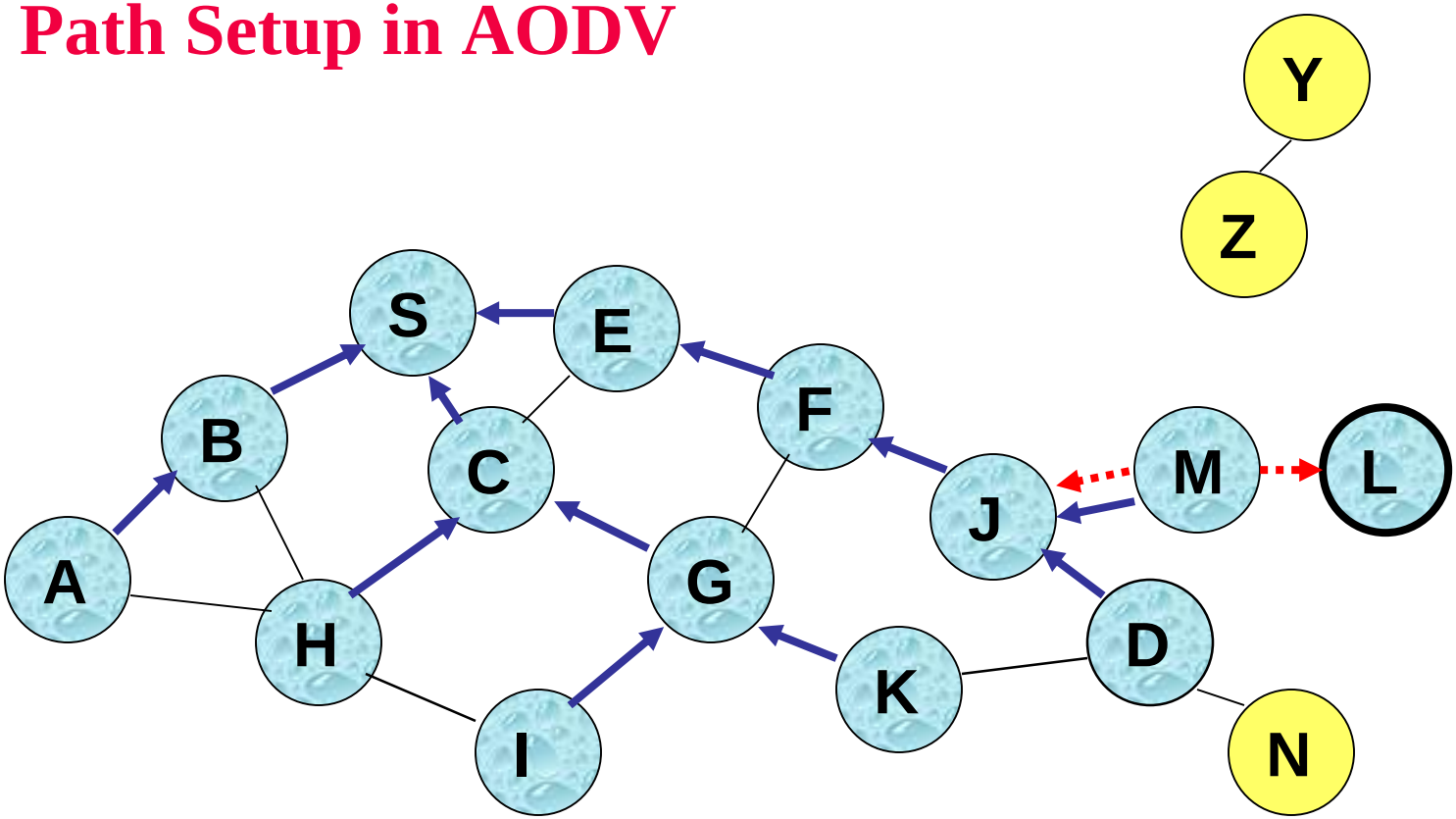


- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

Reverse Path Setup in AODV

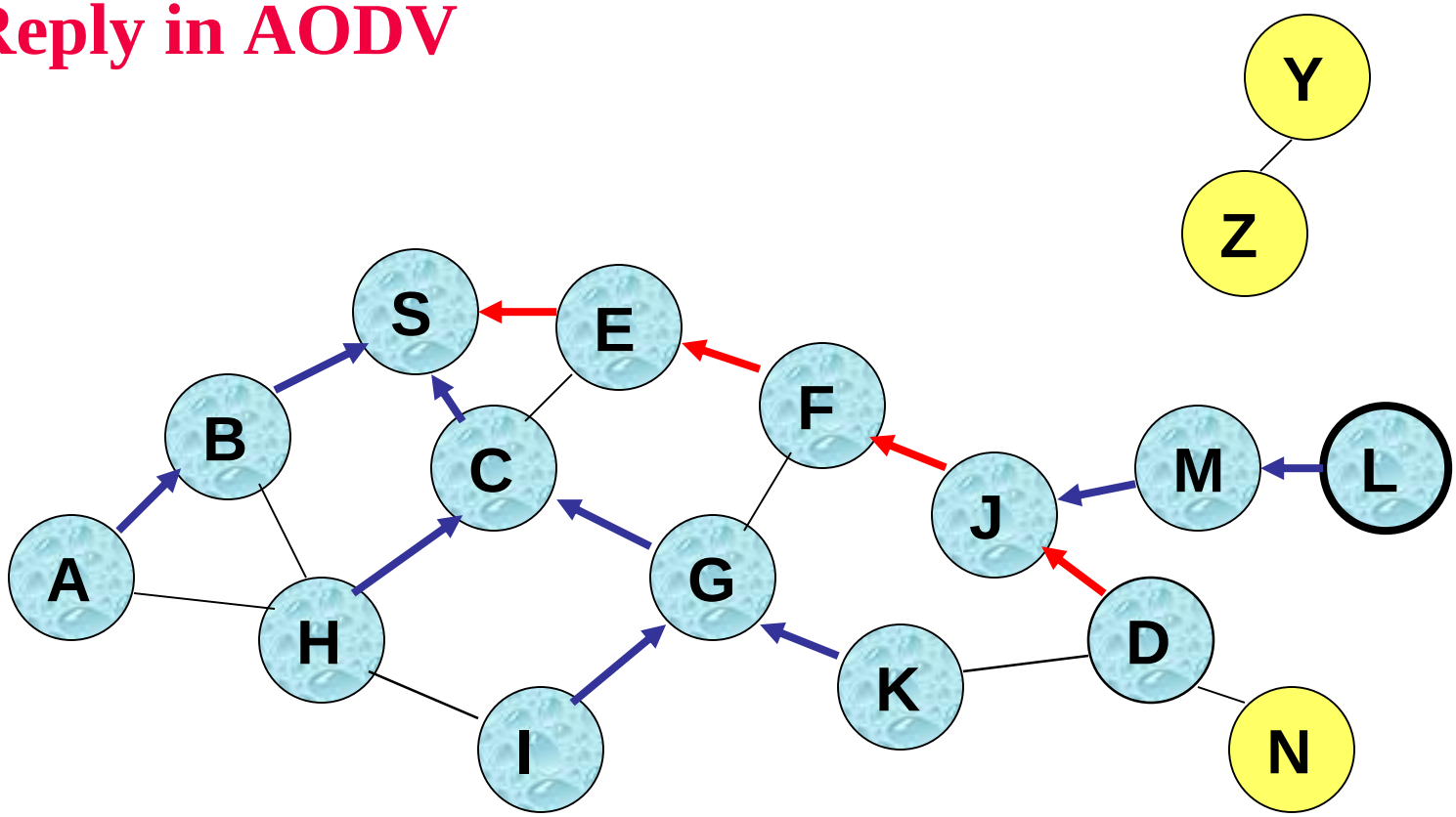


Reverse Path Setup in AODV



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

Route Reply in AODV

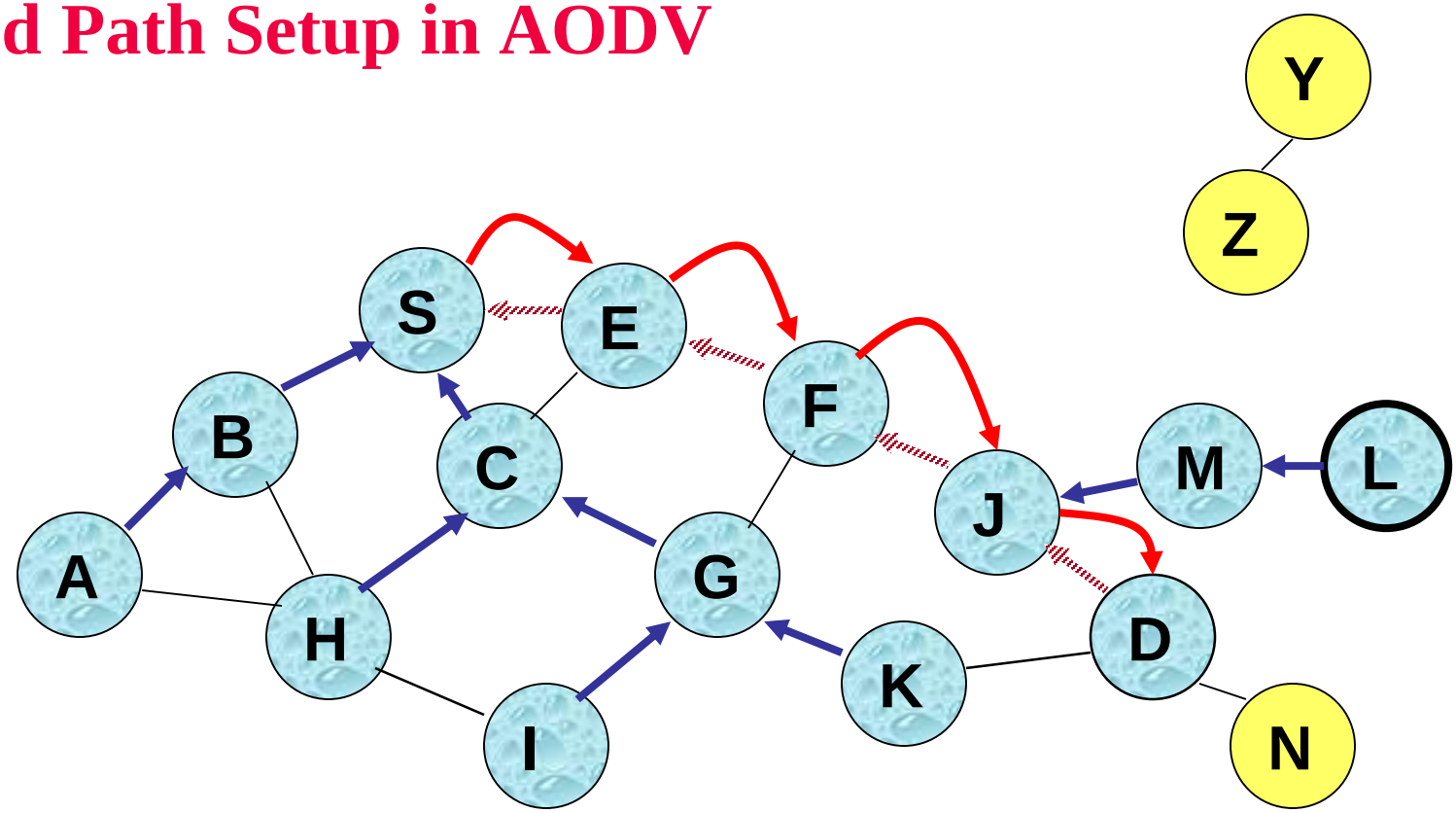


← Represents links on path taken by RREP

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 not very high
  - A new Route Request by node S for a destination is assigned a higher destination sequence number. An intermediate node which knows a route, but with a smaller sequence number, cannot send Route Reply

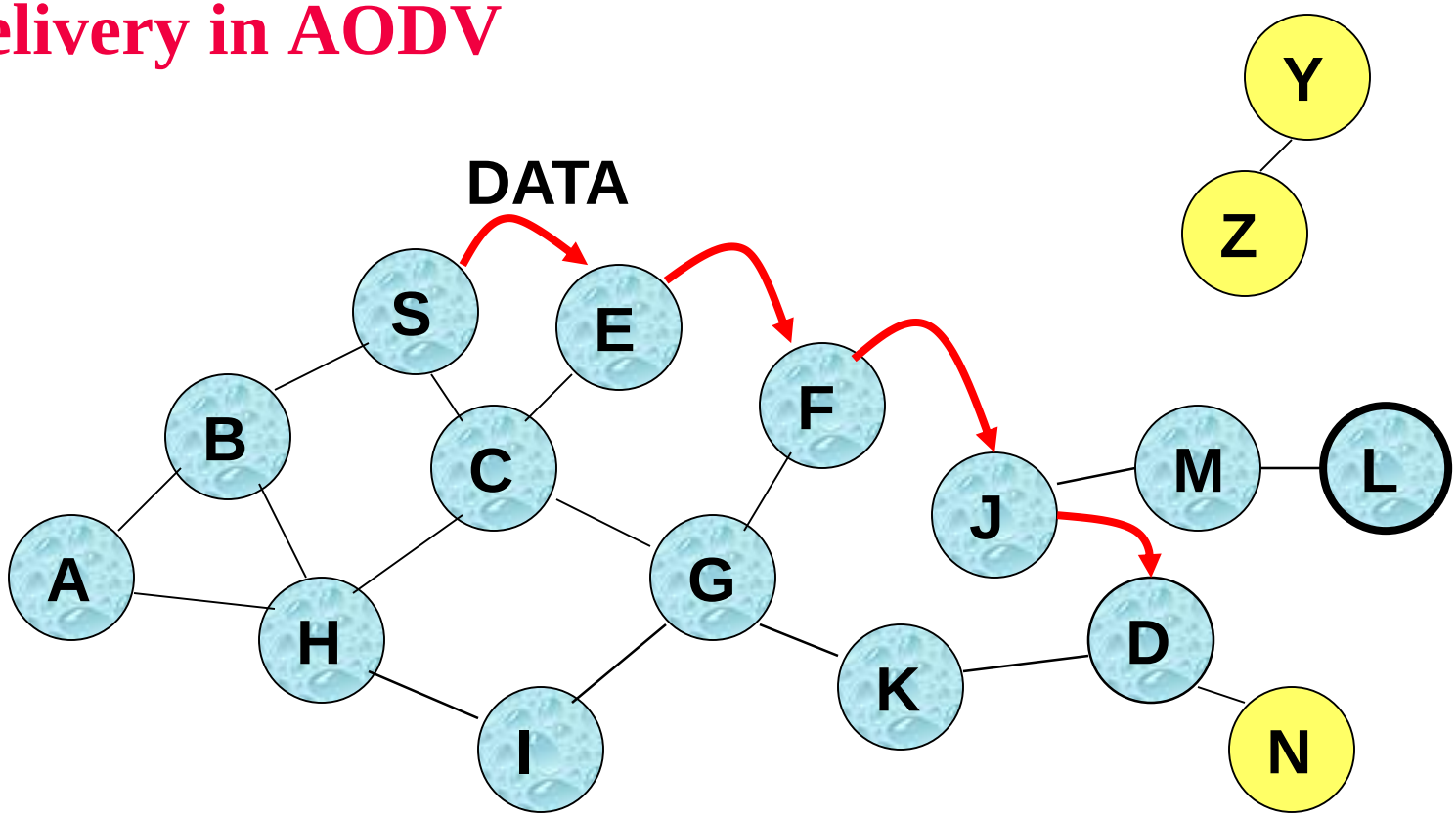
Forward Path Setup in AODV



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 *not* included in packet header.

Timeouts

- A routing table entry maintaining a reverse path is purged after a timeout interval
  - timeout should be long enough to allow RREP to come back

- A routing table entry maintaining a forward path is purged if *not used* for a *active_route_timeout* interval
  - if no is data being sent using a particular routing table entry, that entry will be deleted from the routing table (even if the route may actually still be valid)

Link Failure Reporting

- 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
- 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 messages, which also update destination sequence numbers

Route Error

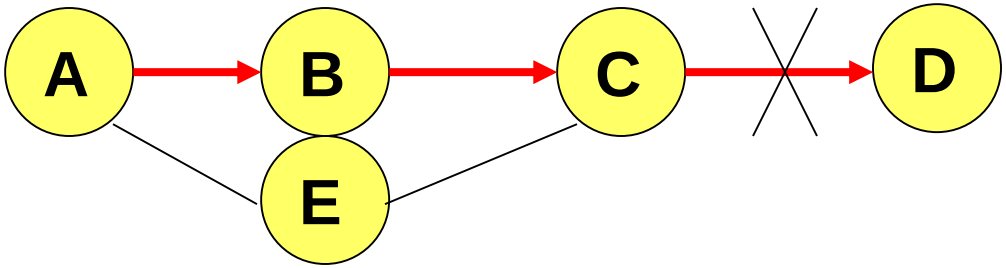
- When node X is unable to forward packet P (from node S to node D) on link (X,Y), it generates a RERR message
- Node X increments the destination sequence number for D cached at node X
- The incremented sequence number *N* is included in the RERR
- When node S receives the RERR, it initiates a new route 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

Link Failure Detection

- *Hello* messages: Neighboring nodes periodically exchange hello message
- Absence of hello message is used as an indication of link failure
- Alternatively, failure to receive several MAC-level acknowledgement may be used as an indication of link failure

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

- Packet forwarding via forwarding table/routing table
- 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
  - Other protocols may maintain several routes for a single destination
- Unused routes expire even if topology does not change

Comparing DSR and AODV

- Qualitatively: very similar
- Quantitatively: simulations (the DSR people are to "blame" for the mobility extensions in NS2)
  - Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y., and Jetcheva, J. 1998. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *Proceedings of the 4th Annual ACM/IEEE international Conference on Mobile Computing and Networking* (Dallas, Texas, United States, October 25 - 30, 1998). Cited by over 5960+ papers and counting…
  - Provided implementations of DSR, AODV, Tora, DSDV
- Results:
  - Metrics?
  - Outcomes?

Optimized Link State Routing Protocol (OLSR)

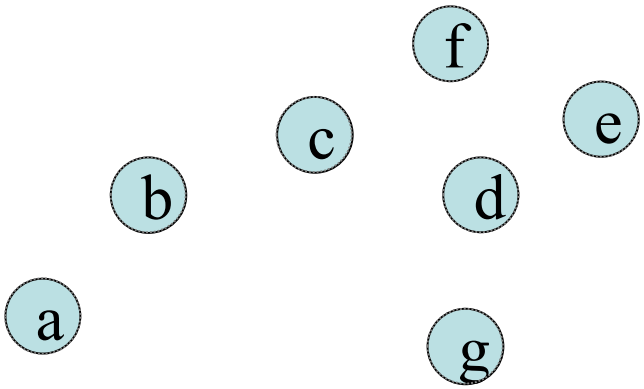
- An optimization of the classical link state routing protocol.
- It is a proactive routing protocol for MANETs.
- The key concept used in the protocol is that of Multi-Point Relays (MPRs)
  - Each node selects a set of its neighbor nodes as MPRs
  - Only nodes selected as such MPRs are responsible for forwarding control traffic intended for diffusion into the entire network.
  - Only nodes selected as MPRs are responsible for declaring link state information in the network.
  - And as a third optimization, an MPR node declares only links between itself and its MPR selectors (nodes that have selected it as MPR)

OLSR II

- OLSR works on periodic exchange of protocol messages.
- OLSR implements different types of messages:
  - HELLO message
  - TC (Topology Control) message
- OLSR has four steps:
  - Neighbor detection
  - MPR selection
  - Topology discovery
  - Route computation

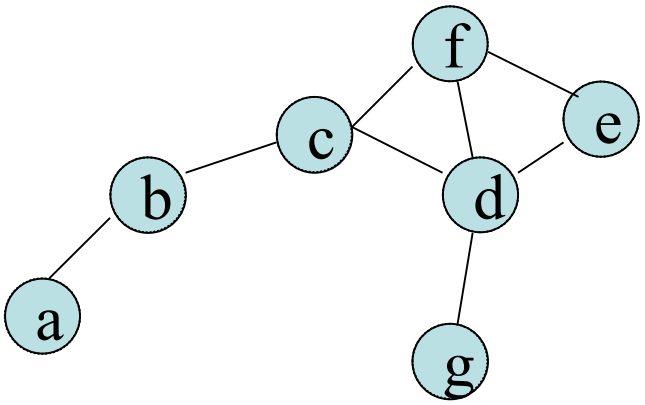
HELLO Message

- Each node generates a HELLO message advertising its entire 1-hop neighborhood.
- As nodes receive HELLO messages from other nodes, they collect information about 1-hop and 2-hop neighbors.



HELLO Message

- Each node generates a HELLO message advertising its entire 1-hop neighborhood.
- As nodes receive HELLO messages from other nodes, they collect information about 1-hop and 2-hop neighbors.



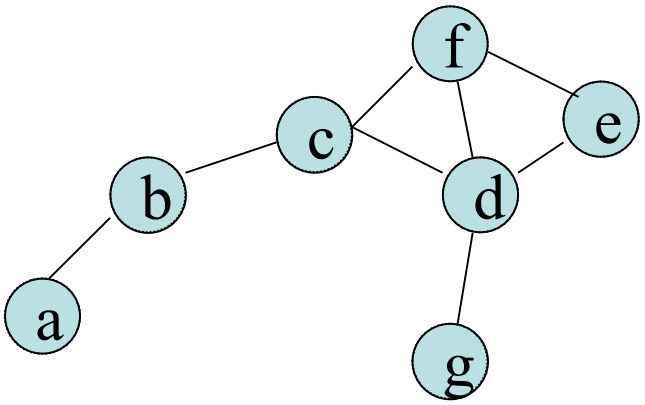
At node C

1-hop Neighbor Set
b
f
d

2-hop Neighbor Set
a
e
g

MPRs Selection

- MPR selection is the key point in OLSR.
- Each node selects a set of its neighbor nodes as MPRs.
- Each node selects its MPR set from its 1-hop neighbors.
- This set is selected such that it covers (transmission range) all 2-hop neighbors.
- The smaller the MPR set is, the less overhead the protocol introduces.



At node c

1-hop Neighbor Set
b
f
d

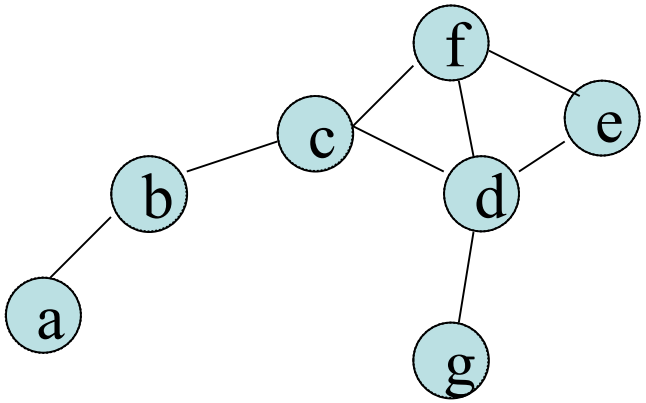
2-hop Neighbor Set
a
e
g

MPR Set
b
d

TC Message

- Only nodes selected as MPRs are responsible for declaring link state information in the network.
- Only nodes selected as such MPRs are responsible for forwarding control traffic intended for diffusion into the entire network.
- An MPR node declares only links between itself and its MPR selectors.
- As nodes receive TC messages from other nodes, they collect information about the topology.
- They use this information for route calculation and constructing the routing table.
- each node will have a partial knowledge of the topology (links to its neighbors and between its MPRs and MPR Selectors.

Example



Node a

MPR Set
b

Node b

MPR Set
c

Node c

MPR Set
b
d

Node f

MPR Set
c
d

Node d

MPR Set
c

Node g

MPR Set
d

Node e

MPR Set
d

Node b MPR Selector Set
a
c

Node c MPR Selector Set
b
f
d

Node d MPR Selector Set
c
f
g
e

Multicast: Motivation

- Many applications for ad hoc networks require one-to-many and many-to-many communication
- Multicast protocols are intended to efficiently support such communication patterns
- Multicasting well researched in fixed networks (i.e., the Internet), building efficient distribution structures (typically a multicast tree)
- Ad hoc networks: dynamic topology makes it harder to maintain distribution structure with low overhead

Motivation (cont.)

- MANET specific protocols are being proposed
  - MAODV: multicast extensions for AODV, establishes shared tree
  - ODMRP: multicast-only protocol, based on per-source mesh
  - ADMR: completely on-demand, per-source tree
- Own study:
  - Study multicasting protocols
  - Develop a protocol that achieves high packet delivery ratio with low overhead

Multicast Protocol Performance

- Multicast protocols perform poorly (packet delivery ratio below 90%) as network topology changes more often (nodes move with higher speed and/or pause less)
- Multicast protocols also often do not scale well with number of multicast senders and/or number of multicast receivers
- Open question how to build efficient multicast routing protocols in a MANET (tree vs. mesh, single tree vs. source-based tree, etc.)
- Quite a bit of work on efficient broadcast protocols, rather than simplistic flooding approach, as broadcasting control messages inherent part of many routing protocols

Are Multicast Protocols Right Choice?

- Broadcast protocols only explored for broadcast purposes, but can also be employed for multicasting
- Another alternative is to use unicasting, creating appropriate number of 1-to-1 communication pairs
- Own study:
  - Compare unicast, multicast, and broadcast protocols under same scenarios
  - Evaluate under one-to-many and many-to-many communication patterns

Simulation Results: Summary I

	1 Sender		2 Sender		5 Sender		10 Sender	
	PDR	**Latency**	**PDR**	**Latency**	**PDR**	**Latency**	**PDR**	**Latency**
10 Receiver	FLOOD		AODV		BCAST		BCAST	
	0.998	0.023	0.996	0.024	0.998	0.023	0.996	0.024
20 Receiver	FLOOD		BCAST		BCAST		BCAST	
	0.998	0.025	0.996	0.112	0.998	0.025	0.996	0.112
30 Receiver	FLOOD		BCAST		BCAST		BCAST	
	0.996	0.025	0.994	0.113	0.996	0.025	0.994	0.113
40 Receiver	FLOOD		BCAST		BCAST		ADMR	
	0.996	0.026	0.994	0.113	0.996	0.026	0.994	0.113
50 Receiver	FLOOD		BCAST		BCAST		ADMR	
	0.996	0.025	0.994	0.110	0.996	0.025	0.994	0.110

Best Protocol (based on PDR), 1 m/s maximum speed

Simulation Results: Summary II

	1 Sender		2 Sender		5 Sender		10 Sender	
	PDR	**Latency**	**PDR**	**Latency**	**PDR**	**Latency**	**PDR**	**Latency**
10 Receiver	FLOOD		FLOOD		BCAST		BCAST	
	0.999	0.023	0.993	0.029	0.999	0.023	0.993	0.029
20 Receiver	FLOOD		FLOOD		BCAST		BCAST	
	0.999	0.023	0.993	0.028	0.999	0.023	0.993	0.028
30 Receiver	FLOOD		ODMRP		BCAST		BCAST	
	0.999	0.023	0.994	0.012	0.999	0.023	0.994	0.012
40 Receiver	FLOOD		ODMRP		BCAST		BCAST	
	0.999	0.023	0.994	0.012	0.999	0.023	0.994	0.012
50 Receiver	FLOOD		FLOOD		BCAST		BCAST	
	0.999	0.022	0.993	0.028	0.999	0.022	0.993	0.028

Best Protocol (based on PDR), 20 m/s maximum speed

Broadcast Protocols Competitive

- Broadcast protocols work well. BCAST and FLOOD are almost always as good as or better than other protocols, though sometimes impose higher packet latency.
- Protocol overhead lower/competitive with best multicast protocol
- For a single multicast sender, FLOOD is the obvious choice, for increasing number of multicast senders BCAST has the edge over FLOOD
- ADMR performs very well in the presence of many multicast senders, (is optimal choice in two scenarios under low mobility), with BCAST being runner-up. All other protocols perform poorly in these scenarios.
- The choice of an optimal multicasting solution is largely independent of the mobility rate.

QoS Routing in MANET

- Find routes satisfying QoS constraints
- Link state metrics should be available and manageable
- Link quality changes quickly and continuously due to node movement and surrounding changes
- Computational cost and protocol overhead affect the performance of the QoS routing protocol
- Protocol performance evaluation is complex

Proactive QoS Routing

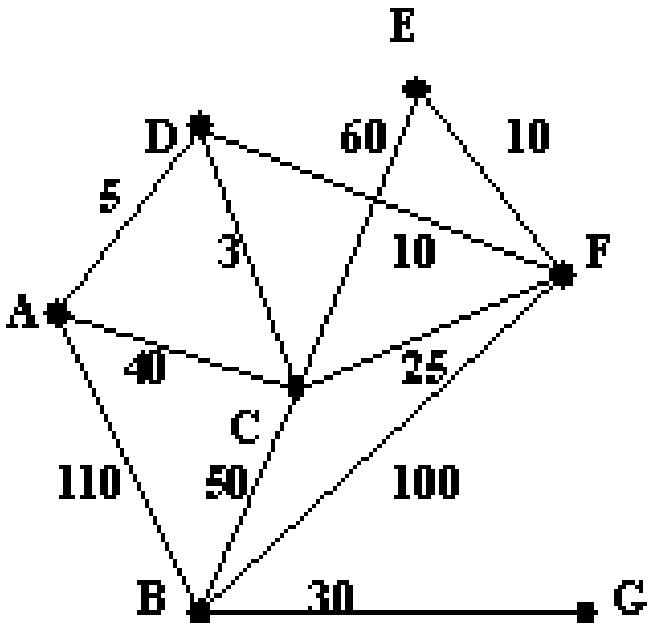
- Advantages
  - suitable for the unpredictable nature of Ad-Hoc networks
  - suitable for the requirement of quick reaction to QoS demands
  - makes call admission control possible
  - avoids the waste of network resources
- Disadvantages
  - introduces additional protocol overhead
  - trade-off between the QoS performance and traditional protocol performance

But..

Little work has been done to analyze the impact of the additional overhead on pro-active QoS routing ➔ studied QoS extensions to OLSR in joint project with CRC

OLSR Revisited

- Selects MPR to cover 2-hop neighbors
- Exchanges neighbor/MPR information in Hello message
- Generates and relays TC message to broadcast topology information
- Reduces control overhead by limiting MPR set
- In the graph, B selects C as MPR



QoS Versions of OLSR

- OLSR protocol does not guarantee to find the best bandwidth route
- Three heuristics are proposed to enhance OLSR in bandwidth aspect
- The heuristics select good bandwidth neighbor as MPR
- Based on evaluation in static network scenarios, heuristic 2 is chosen: best-bandwidth neighbours are selected as MPRs until 2-hop neighbourhood is covered
  - In the previous network topology, B selects A,F as MPRs
- Update link state only if changed significantly (x% from last value)

Analysis of Results I: Gains

- Outperforms the original OLSR protocol in bandwidth aspect
- In a dense network, the 40% OLSR finds the best bandwidth route
- In a sparse network, the 20% OLSR finds the best bandwidth route
- There is a trade-off, so must select routing algorithms based on the request of the data application

Analysis of Results II: Costs

- More MPRs are selected; more TC messages are generated and relayed
- The additional control messages increase the network load
- The overlap of 2-hop neighbors covered by MPRs causes TC collision

As a Result...

QoS versions of OLSR have lower packet delivery rate and more delay than the original OLSR algorithms, especially for 20% OLSR in high speed movement scenario

Open/Additional Issues in Routing

- Energy-efficient routing protocols, multipath routing
- New routing metrics to deal with specifics of wireless channel/radio capabilities
  - "shortest path/minimal hop count is not enough"
  - ETX: channels are lossy, account for potential packet retransmissions
  - MTM: multirate channels – more shorter hops may be better than fewer long, low rate, hops
  - Radios can switch between channels, reduces interference among adjacent hops
- More "realistic" model of network
  - Not all nodes are the same, should route through more powerful nodes
  - Scalability: form and maintain clusters
  - MANETs are not standalone, will have Internet gateways – use those to "route for free"
- Traffic pattern predictable in mesh networks (to/from gateway): build tree routed in gateway)

Transport in MANET

Again, many issues, mostly to do with TCP:

Performance

Fairness

In Conclusion (MANET)

Many Challenges Yet to be Addressed

- Issues other than routing have received much less attention
  - Comment from one conference: "there is, yet again, another routing paper, oh no….." ☺
  - However: there are still interesting problems as well (some of my PhD students work on specific issues too)
  - Also, see comment by Ed Knightly
- Other interesting problems:
  - Applications for MANET
  - Address assignment, node configuration → network management
  - Support for real-time multimedia traffic (QoS)
  - Security and access control
  - Service discovery
  - Improving interaction between protocol layers (cross-layer design)
  - Integration with other wireless/wired technologies
  - Network Coding to improve throughput