

Mobile Ad Hoc Networks

Prof. Krishna Moorthy Sivalingam, Ph.D.
Professor, Dept. of CSE, IIT Madras

skrishnam@iitm.ac.in, krishna.sivalingam@gmail.com
<http://www.cse.iitm.ac.in/~skrishnam>

Based on Tutorials by (Used with permission):
Prof. Nitin H. Vaidya, University of Illinois at Urbana-
Champaign

1

Tutorial Outline

- Introduction
- Unicast routing
- Implementation Results
- Standards activities

2

Introduction

3

Mobile Ad Hoc Networks

- A network of hosts, connected by wireless links
 - Hosts are mobile

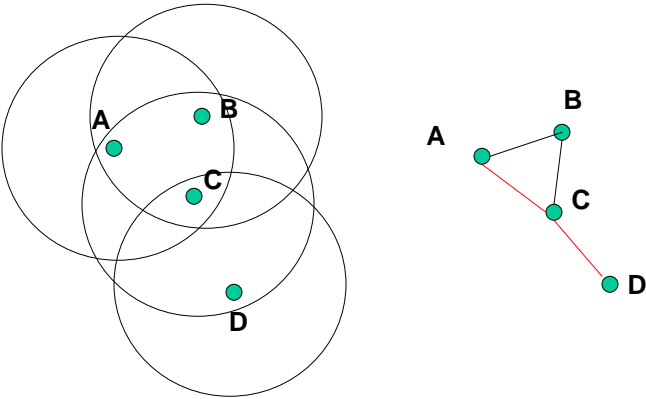
- Network established without a pre-existing infrastructure

- Routes between nodes may potentially contain multiple hops

4

Multi-hop transmission

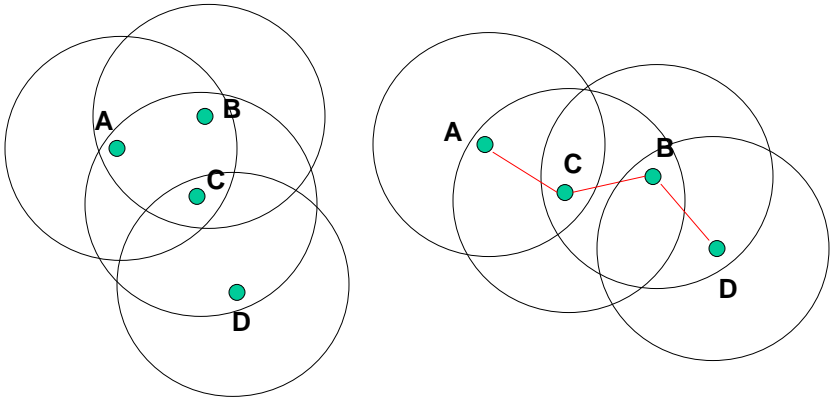
- May need to traverse multiple links to reach a destination



5

Mobility

- Mobility causes route changes



6

Advantages of Ad Hoc Networks

- Ease of deployment
- Speed of deployment
- Decreased dependence on infrastructure

7

Many Applications

- Military environments
 - soldiers, tanks, planes
- Emergency operations
 - Disaster recovery
 - Search-and-rescue
 - Policing and fire fighting
- Civilian environments
 - Taxi cab network
 - Conference venues
 - Meeting rooms
 - Sports stadiums
 - Boats, small aircraft

8

MANET 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)

9

Variations, contd.

- Traffic characteristics may differ in different ad hoc networks
 - bit rate
 - timeliness constraints
 - reliability requirements
 - unicast / multicast / geocast
 - host-based addressing / content-based addressing / capability-based addressing

- May co-exist (and co-operate) with an infrastructure-based network

10

Variations, contd.

- Mobility patterns may be different
 - people sitting at an airport lounge
 - citywide taxi cabs
 - military movements
 - personal area network

- Mobility characteristics
 - speed
 - predictability
 - direction of movement
 - pattern of movement
 - uniformity (or lack thereof) of mobility characteristics among different nodes

11

Challenges

- Limited wireless transmission range
- Time-varying wireless link characteristics: unreliable
- Broadcast nature of the wireless medium
 - Hidden terminal problem and broadcast storms
- Packet losses due to transmission errors
- Mobility-induced route changes
- Mobility-induced packet losses
- Battery constraints
- Potentially frequent network partitions
- Ease of snooping on wireless transmissions (security issues)

12

The Holy Grail

- A one-size-fits-all solution
 - Perhaps using an adaptive/hybrid approach that can adapt to situation at hand
- Difficult problem
- Many solutions proposed trying to address a sub-space of the problem domain

13

MANET Protocol Stack

- Physical Layer: 2.4/5.8 Ghz, FHSS/DSSS, OFDM, OFDMA, MIMO, Directional Antenna, etc
- MAC Layer: CSMA, CSMA/CA, RTS/CTS, TDMA with Scheduling Algorithm
- Routing Layer: Addressing; DSR, AODV, OLSR, TORA, ZRP, LAR, etc.
 - Unicast, Broadcast, Multicast, Reliable Multicast, Geocast
- Transport Layer: UDP, TCP, RTP, etc.
- Cross-cutting functions:
 - Power-awareness, energy-conservation
 - Security of control and data packets

14

Unicast Routing in Mobile Ad Hoc Networks

15

Why is Routing in MANET different ?

- Host mobility
 - link failure/repair due to mobility may have different characteristics than those due to other causes
- Rate of link failure/repair may be high when nodes move fast
- New performance criteria may be used
 - route stability despite mobility
 - energy consumption

16

Unicast Routing Protocols

- 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

17

Wired Network Routing Protocols

- Distance Vector Protocols, e.g. Bellman-Ford
 - Each node maintains a routing table, with shortest distance to every other node and the next hop to that node
 - Each node **LOCALLY** exchanges the entire routing table (i.e. **GLOBAL** info) with only its 1-hop neighbors
 - Each node updates path/cost to all network nodes based on costs reported by neighbors
 - Used in RIP, etc
- Link State Protocols
 - Each node maintains link state information about all its 1-hop links
 - Each node **BROADCASTS** globally packets containing link-state information (i.e. **LOCAL** info)
 - Each node constructs network topology and runs shortest-path algorithms (e.g. Dijkstra's algorithm)
 - Used in OSPF, etc.

18

Ideal Routing algorithm

- Fully Distributed; Minimal Global State Maintenance
- Minimal Routing Protocol Control Overhead
- Fast Adaptation to Frequent Topology Changes
 - Converge to Optimal Routes Faster
- Route Computation and Maintenance at a node must depend upon a small number of nodes
- Loop-Free Routes; and Freedom from Stale Routes
- No. of Packet Collisions minimized by limiting the number of broadcasts made by each node
- Optimally use scarce resources (power, memory, bandwidth)
- Support QoS and Real-time traffic needs

19

Routing Protocols

- Proactive protocols
 - Determine routes independent of traffic pattern
 - Traditional link-state and distance-vector routing protocols are proactive
- Reactive protocols
 - Determine and maintain routes only when needed
- Hybrid protocols

20

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

21

Flat vs Hierarchical

- Flat (Single Tier)
 - All nodes belong to one tier

- Two-Tier Hierarchy
 - Nodes in Tier 1 send traffic to a designated node
 - This can be single or multi-hop path
 - Designated nodes form Tier 2
 - Packet is routed via Tier 2 nodes to Tier 2 node serving destination node
 - Tier 2 can use different technology from Tier 1
 - Longer-range, higher-BW links
 - WiFi + WiFi (long-range)
 - WiFi+WiMAX

22

Overview of Unicast Routing Protocols

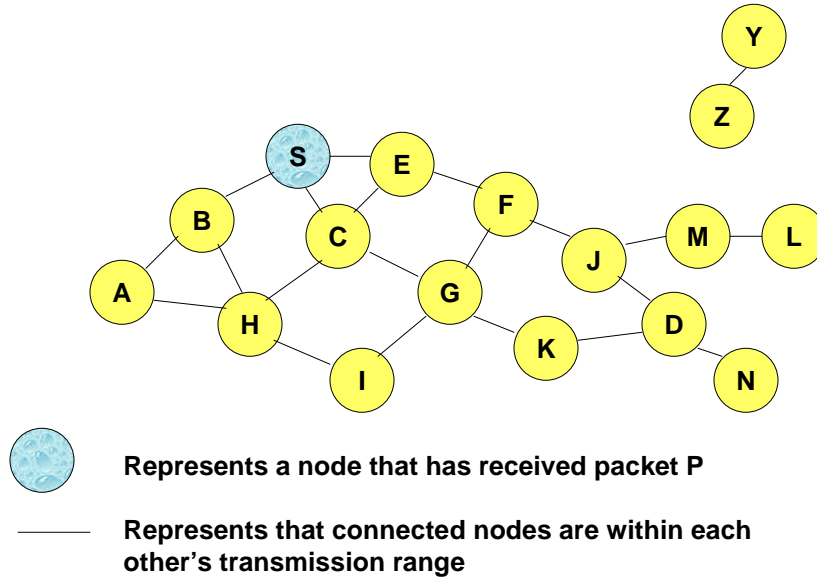
23

Flooding for Data Delivery

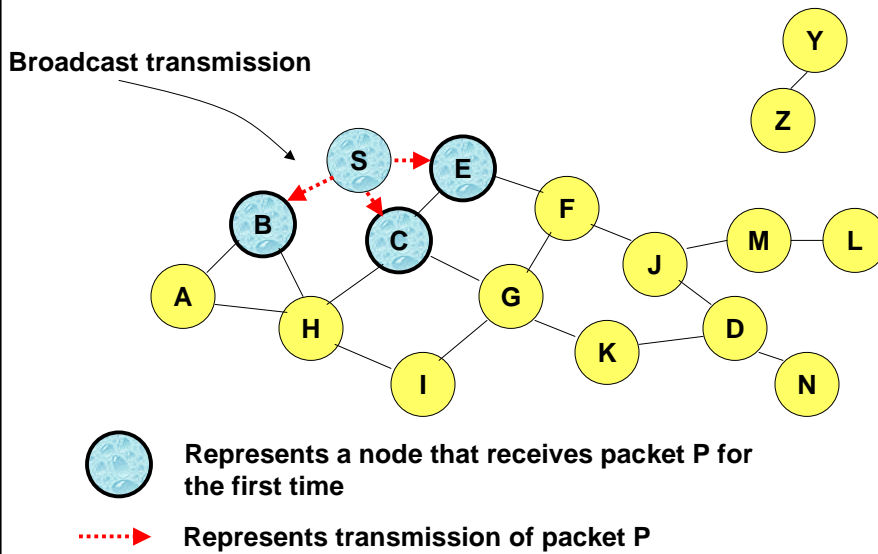
- Sender S broadcasts data packet P to all its neighbors
- Each node receiving P forwards P to its neighbors
- Sequence numbers used to avoid the possibility of forwarding the same packet more than once
- Packet P reaches destination D provided that D is reachable from sender S
- Node D does not forward the packet

24

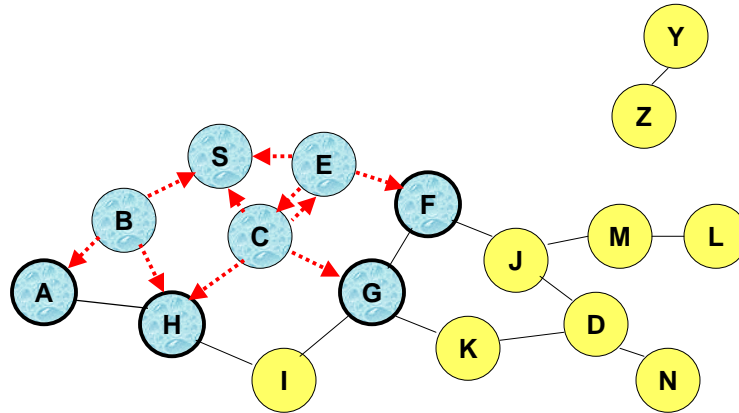
Flooding for Data Delivery



Flooding for Data Delivery



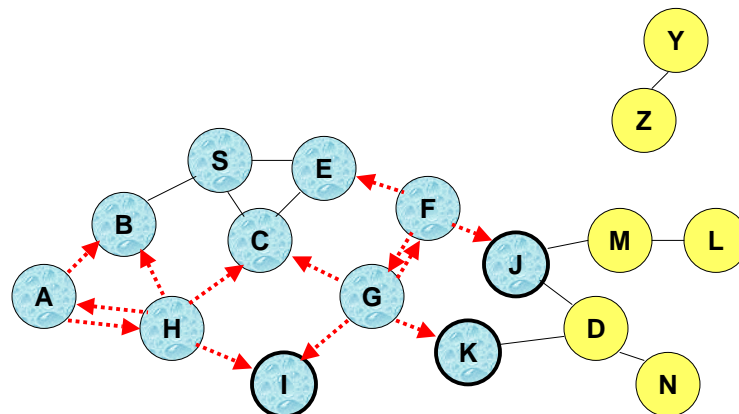
Flooding for Data Delivery



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

27

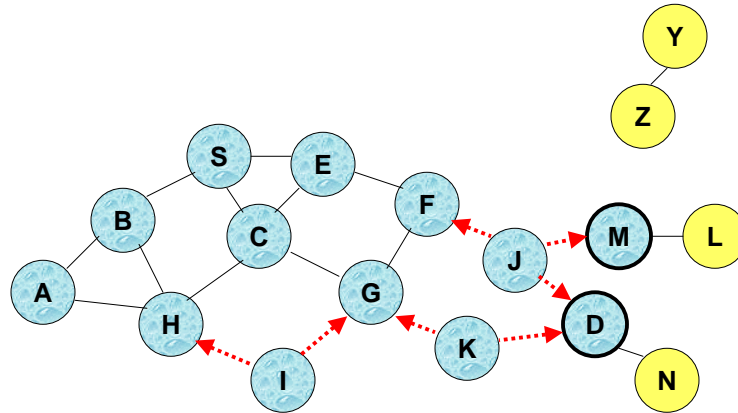
Flooding for Data Delivery



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

28

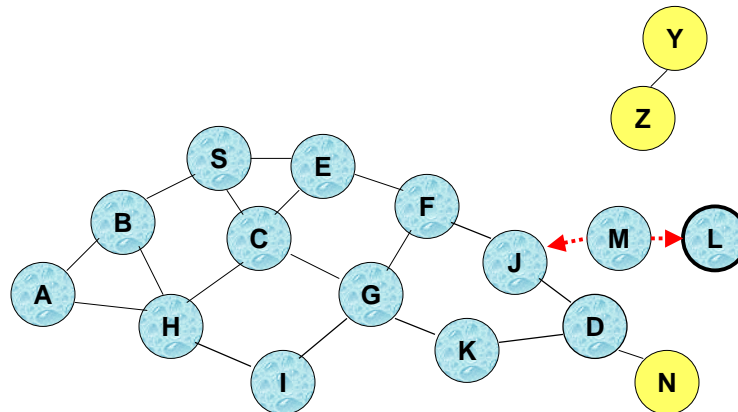
Flooding for Data Delivery



- Nodes J and K both broadcast packet P to node D
- Since nodes J and K are **hidden** from each other, their transmissions may collide
⇒ Packet P may not be delivered to node D at all, despite the use of flooding

29

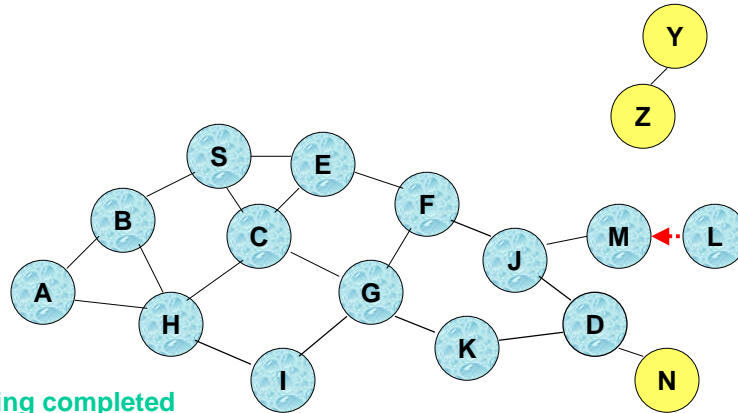
Flooding for Data Delivery



- Node D **does not forward** packet P, because node D is the **intended destination of packet P**

30

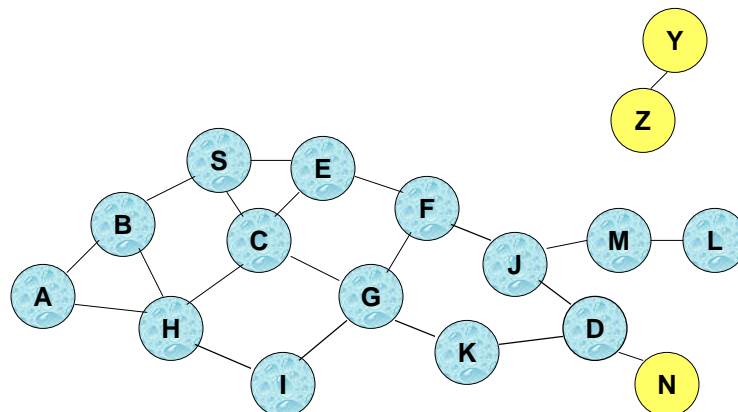
Flooding for Data Delivery



- Flooding completed
- Nodes **unreachable** from S do not receive packet P (e.g., node Z)
- Nodes for which all paths from S go through the destination D also do not receive packet P (example: node N)

31

Flooding for Data Delivery



- Flooding may deliver packets to too many nodes (in the **worst case**, all nodes reachable from sender may receive the packet)

32

Flooding for Data Delivery: Advantages

- Simplicity
- May be more efficient when rate of information transmission is low enough that the overhead of explicit route discovery/maintenance incurred by other protocols is relatively higher
 - this scenario may occur, for instance, when nodes transmit **small data packets** relatively infrequently, and many topology **changes occur** between consecutive packet transmissions
- Potentially higher reliability of data delivery
 - Because packets may be delivered to the destination on multiple paths

33

Flooding for Data Delivery: Disadvantages

- Potentially, very high overhead
 - Data packets may be delivered to too many nodes who do not need to receive them
- Potentially lower reliability of data delivery
 - Flooding uses broadcasting -- hard to implement reliable broadcast delivery without significantly increasing overhead
 - Broadcasting in IEEE 802.11 MAC is unreliable
 - In our example, nodes J and K may transmit to node D simultaneously, resulting in loss of the packet
 - in this case, destination would not receive the packet at all

34

Flooding of Control Packets

- Many protocols perform (potentially *limited*) flooding of **control** packets, instead of **data** packets
- The control packets are used to discover routes
- Discovered routes are subsequently used to send data packet(s)
- Overhead of control packet flooding is **amortized** over data packets transmitted between consecutive control packet floods

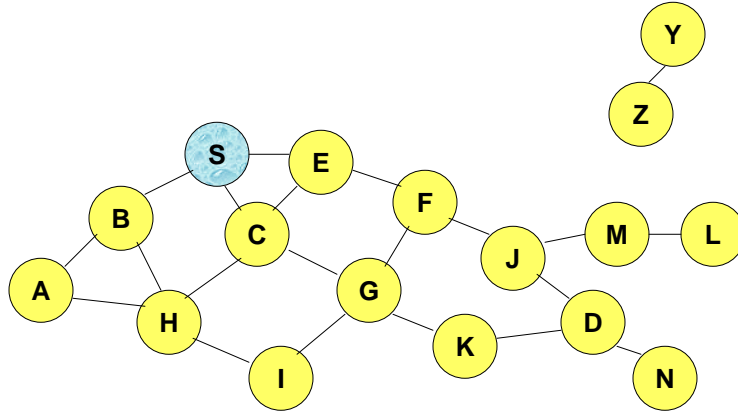
35

Dynamic Source Routing (DSR) [Johnson96]

- 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

36

Route Discovery in DSR

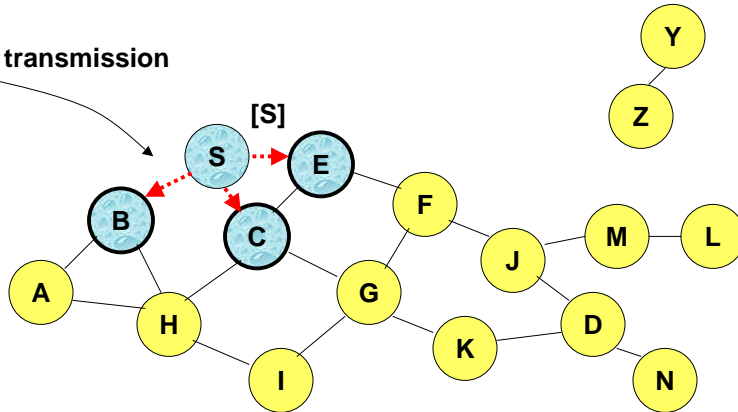


Represents a node that has received RREQ for D from S

37

Route Discovery in DSR

Broadcast transmission

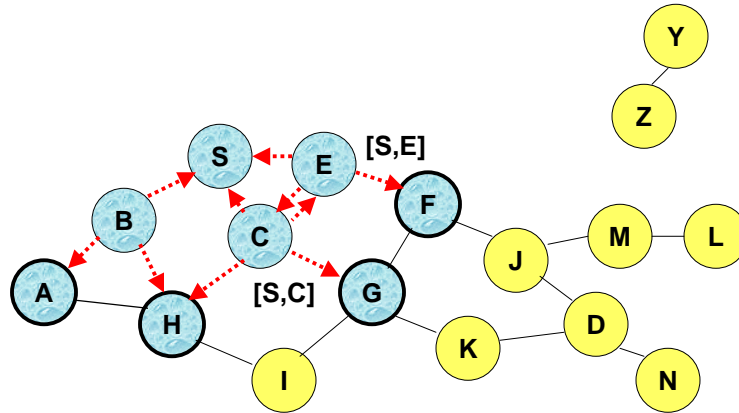


.....▶ Represents transmission of RREQ

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

38

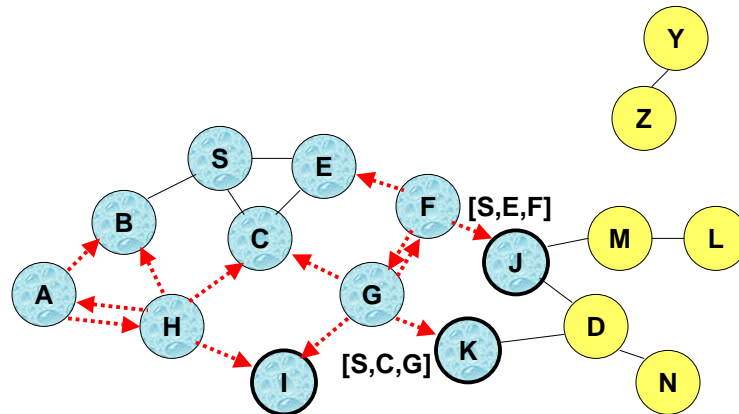
Route Discovery in DSR



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

39

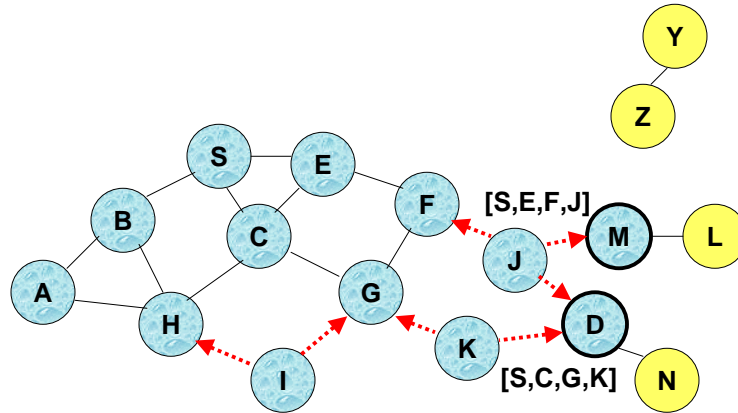
Route Discovery in DSR



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

40

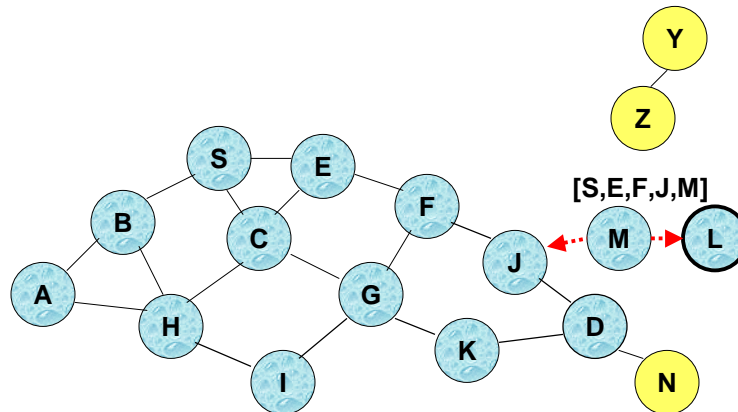
Route Discovery in DSR



- Nodes J and K both broadcast RREQ to node D
- Since nodes J and K are **hidden** from each other, their **transmissions may collide**

41

Route Discovery in DSR



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

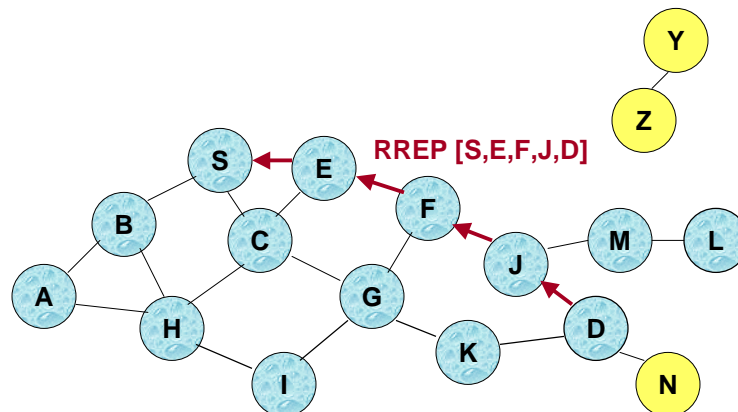
42

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

43

Route Reply in DSR



← Represents RREP control message

44

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)

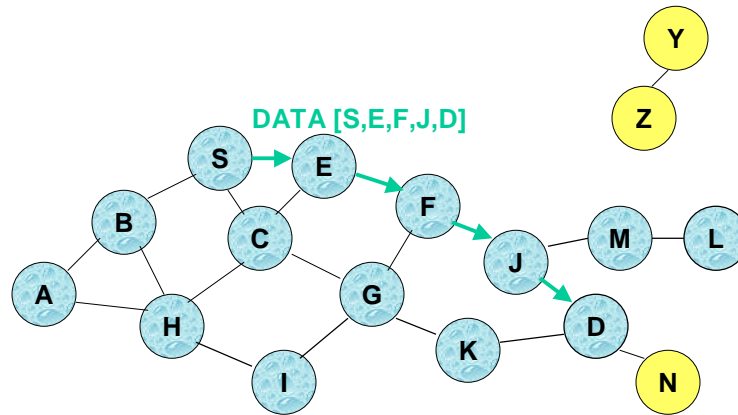
45

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

46

Data Delivery in DSR



Packet header size grows with route length

47

When to Perform a Route Discovery

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

48

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

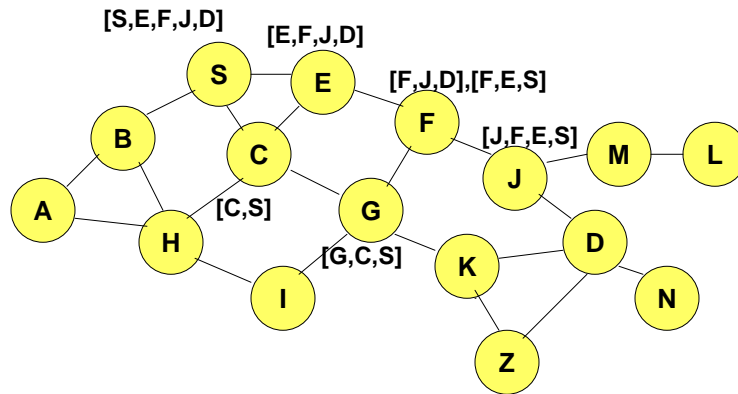
49

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

50

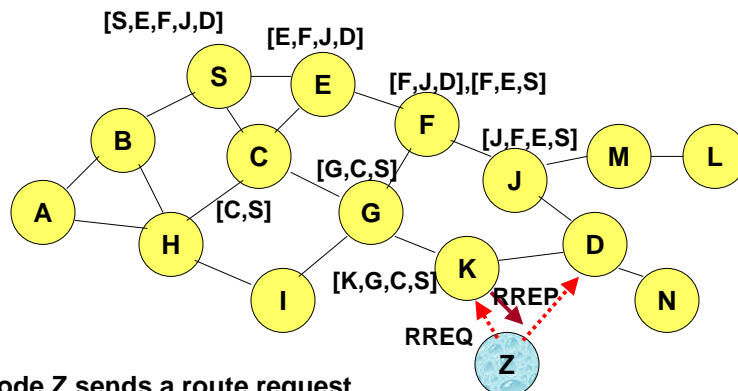
Use of Route Caching



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

51

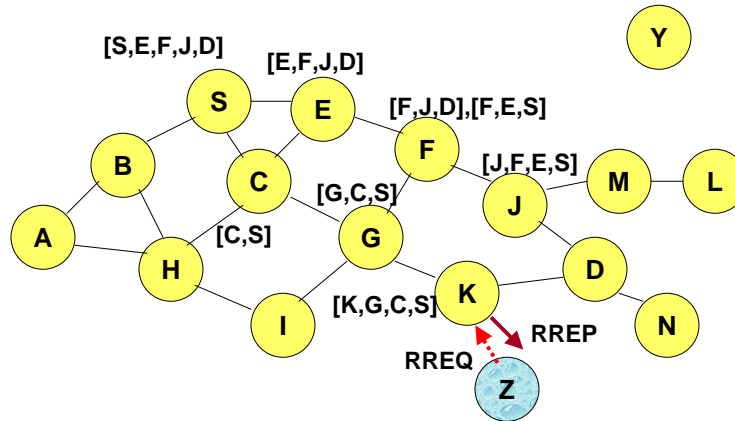
Use of Route Caching: Can Speed up Route Discovery



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

52

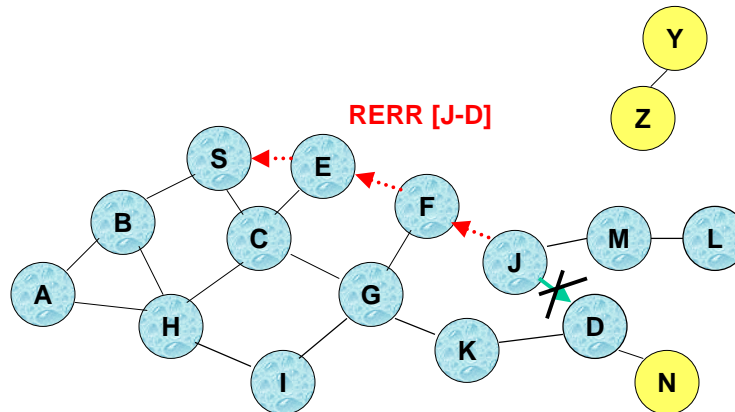
Use of Route Caching: Can Reduce Propagation of Route Requests



Assume that there is no link between D and Z.
Route Reply (RREP) from node K **limits flooding** of RREQ.
In general, the reduction may be less dramatic.

53

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

54

Route Caching: Beware!

- Stale caches can adversely affect performance
- With passage of time and host mobility, cached routes may become invalid
- A sender host may try several stale routes (obtained from local cache, or replied from cache by other nodes), before finding a good route

55

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

56

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

57

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.
- For some proposals for cache invalidation, see [Hu00Mobicom]
 - Static timeouts
 - Adaptive timeouts based on link stability

58

Flooding of Control Packets

- How to reduce the scope of the route request flood ?
 - LAR [Ko98Mobicom]
 - Query localization [Castaneda99Mobicom]
 - Based on link quality strength (forward requests from senders with high signal quality)
- How to reduce redundant broadcasts ?
 - The Broadcast Storm Problem [Ni99Mobicom]

59

Ad Hoc On-Demand Distance Vector Routing (AODV) [Perkins99Wmcsa]

- 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

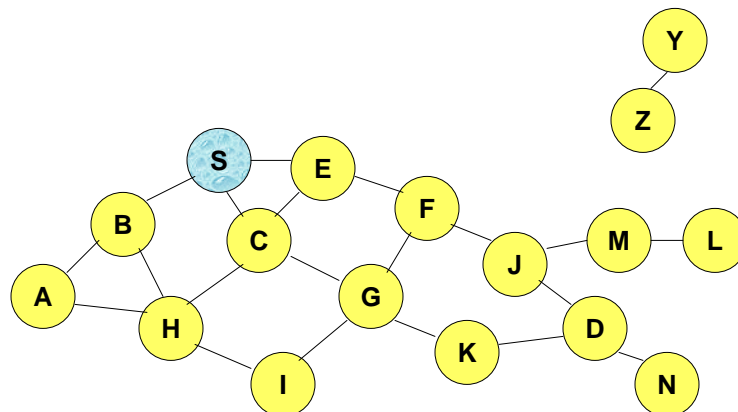
60

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

61

Route Requests in AODV

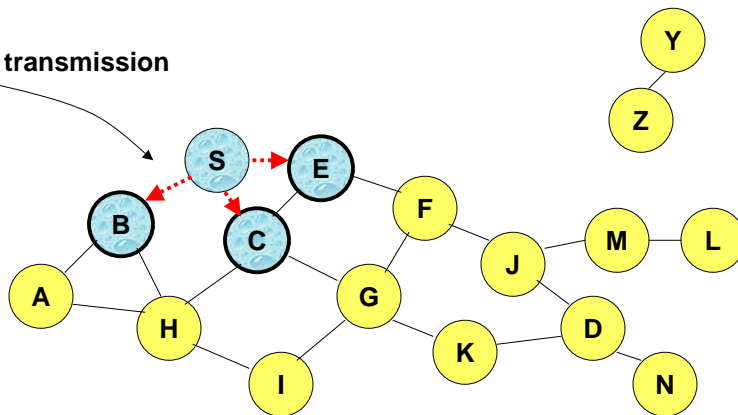


Represents a node that has received RREQ for D from S

62

Route Requests in AODV

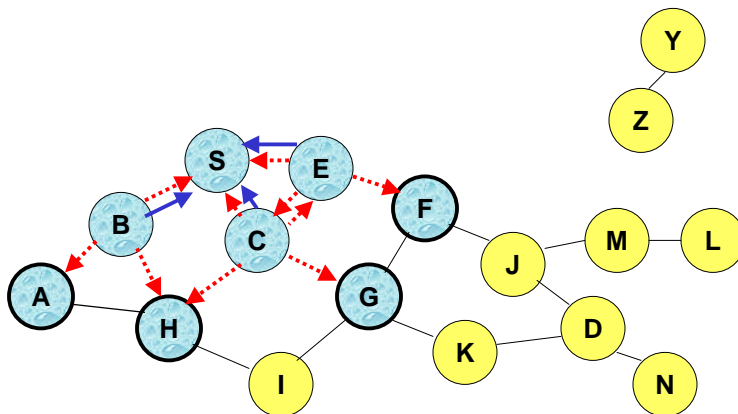
Broadcast transmission



.....▶ Represents transmission of RREQ

63

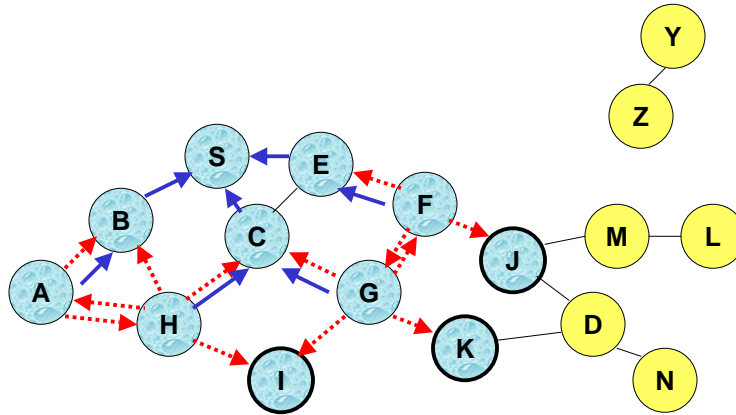
Route Requests in AODV



← Represents links on Reverse Path

64

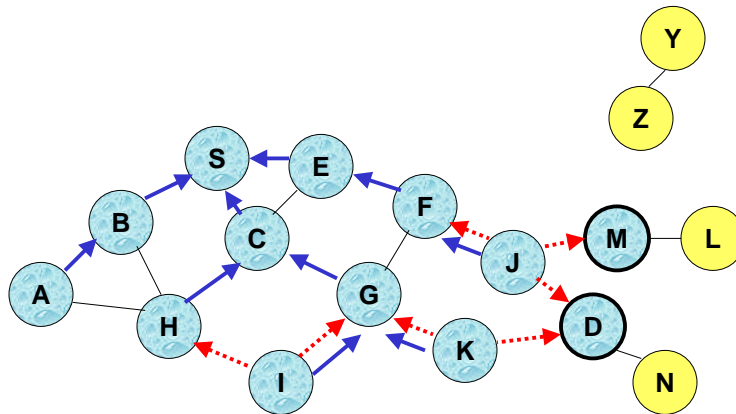
Reverse Path Setup in AODV



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

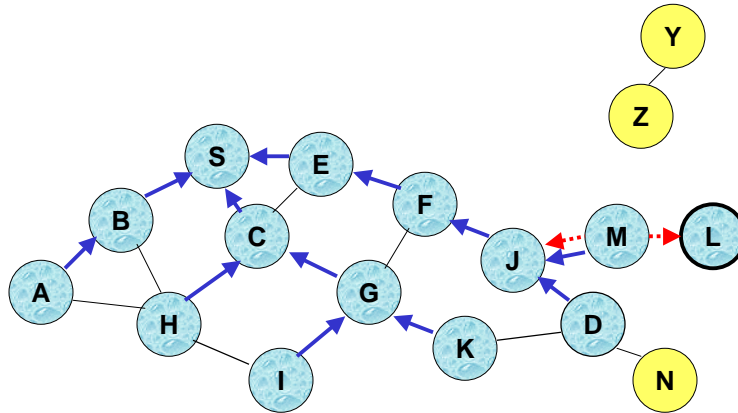
65

Reverse Path Setup in AODV



66

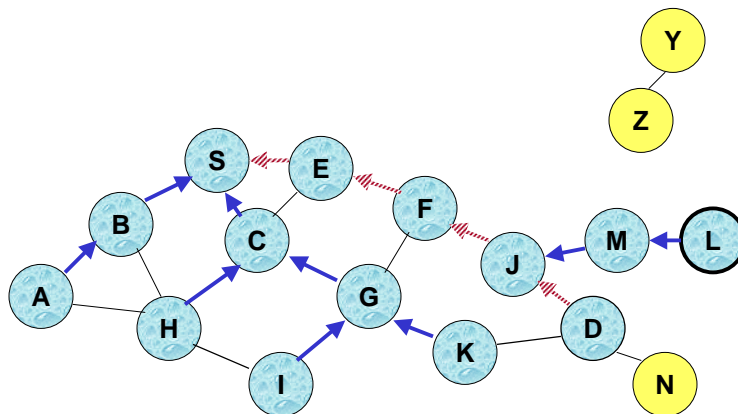
Reverse Path Setup in AODV



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

67

Route Reply in AODV



 Represents links on path taken by RREP

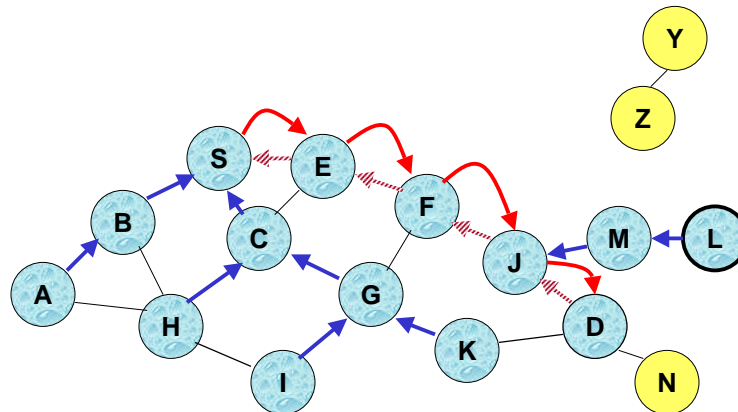
68

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 as high as DSR
 - 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

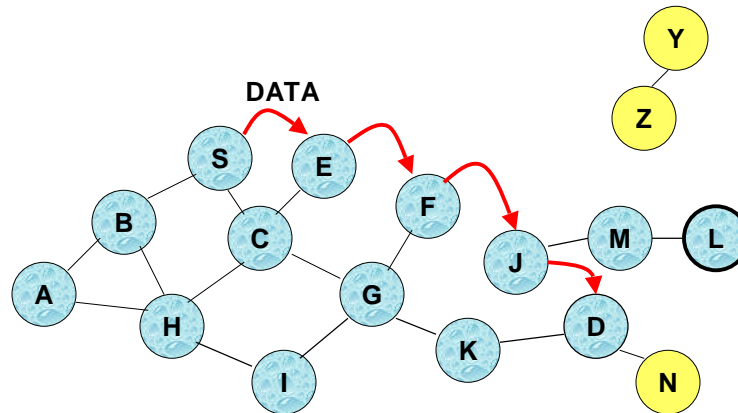
69

Forward Path Setup in AODV



70

Data Delivery in AODV



Routing table entries used to forward data packet.

Route is **not** included in packet header.

71

Summary: AODV

- 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
- Unused routes expire even if topology does not change

72

Proactive Protocols

- Most of the schemes discussed so far are reactive
- Proactive schemes based on distance-vector and link-state mechanisms have also been proposed

73

Link State Routing [Huitema95]

- 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

74

Optimized Link State Routing (OLSR)

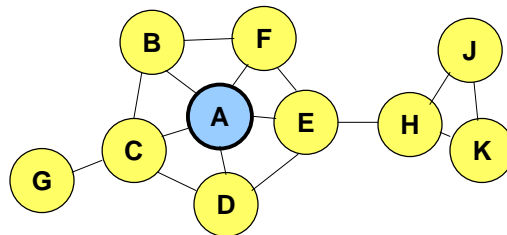
[Jacquet00ietf, Jacquet99Inria]

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

75

Optimized Link State Routing (OLSR)

- Nodes C and E are multipoint relays of node A

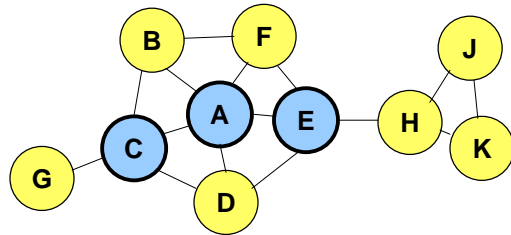


Node that has broadcast state information from A

76

Optimized Link State Routing (OLSR)

- Nodes C and E forward information received from A

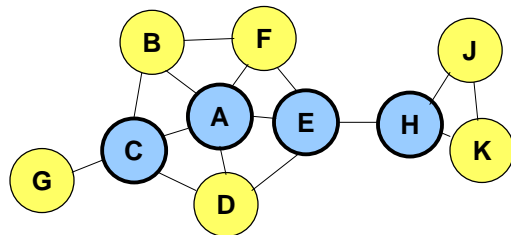


Node that has broadcast state information from A

77

Optimized Link State Routing (OLSR)

- Nodes E and K are multipoint relays for node H
- Node K forwards information received from H
 - E has already forwarded the same information once



Node that has broadcast state information from A

78

OLSR

- OLSR floods information through the multipoint relays
- The flooded itself is fir links connecting nodes to respective multipoint relays
- Routes used by OLSR only include multipoint relays as intermediate nodes

79

Destination-Sequenced Distance-Vector (DSDV) [Perkins94Sigcomm]

- Each node maintains a routing table which stores
 - next hop towards each destination
 - a cost metric for the path to each destination
 - a destination sequence number that is created by the destination itself
 - Sequence numbers used to avoid formation of loops
- Each node periodically forwards the routing table to its neighbors
 - Each node increments and appends its sequence number when sending its local routing table
 - This sequence number will be attached to route entries created for this node

80

Destination-Sequenced Distance-Vector (DSDV)

- Assume that node X receives routing information from Y about a route to node Z



- Let $S(X)$ and $S(Y)$ denote the destination sequence number for node Z as stored at node X, and as sent by node Y with its routing table to node X, respectively

81

Destination-Sequenced Distance-Vector (DSDV)

- Node X takes the following steps:



- If $S(X) > S(Y)$, then X ignores the routing information received from Y
- If $S(X) = S(Y)$, and cost of going through Y is smaller than the route known to X, then X sets Y as the next hop to Z
- If $S(X) < S(Y)$, then X sets Y as the next hop to Z, and $S(X)$ is updated to equal $S(Y)$

82

Unicast Routing: Summary

- Several protocols and numerous variations have been proposed and analyzed
- Each protocol will be suitable for a particular combination of network topology, mobility patterns and traffic patterns/requirements

- Besides unicast traffic:
 - Multicast: sending message to a group of interested users
 - Geocast: sending message to a group of users in a specific region
- Other variations, based on power-aware routing, etc. also studied
- Security of routing and data packets is also critical and usually addressed separately

83

Capacity of Ad Hoc Networks

84

MANET Capacity

- Consider a single channel shared by n nodes
 - Throughput per node: $1/n$, on average
- Consider a IEEE 802.11 a/g channel at 54 Mbps
 - With single user: around 25-30 Mbps due to MAC overhead
- Piyush Gupta and P.R.Kumar, 2000
 - Unit disk with n nodes; no mobility
 - Throughput per node: $O(1/\sqrt{n})$
- Li et.al., 2001
 - For a chain (linear) of ad hoc nodes, ideal capacity: $1/4$ of channel; simulation yields capacity of $1/7$ of channel
- Grossglauser and Tse, 2002:
 - Distribute packets to many intermediate nodes that relay packet to destination when destination comes nearby
 - Throughput per node: $O(1)$
- Piyush Gupta and P.R.Kumar, 2005
 - With multi-user coding, Throughput per node: $O(1)$

85

MANET Capacity, Contd.

- Das et.al., 2004:
 - Simulated network of 100 nodes with 2 Mbps radio, large enough to allow 7 simultaneous transmissions
 - Throughput per node: Few tens of Kbps
- Results from Kiran Chauhan's M. Tech. thesis (2009) based on ns2
 - No mobility considered
 - AODV, DSDV and DSR considered
- Results from ongoing work based on OPNET
 - Mobility considered
 - AODV, DSR, OLSR, TORA

86

Capacity of Fixed Ad Hoc Networks

[Gupta00it]

- n nodes in area A transmitting at W bits/sec using a fixed range (distance between a random pair of nodes is $O(\sqrt{n})$)

- Bit-distance product that can be transported by the network per second is

$$\Theta (W \sqrt{A n})$$

- Throughput per node

$$\Theta (W / \sqrt{n})$$

87

Capacity of Mobile Ad Hoc Networks

[Grossglauser01Infocom]

- Assume random motion
- Any two nodes become neighbors once in a while
- Each node assumed sender for one *session*, and destination for another *session*
- Relay packets through at most one other node
 - Packet go from S to D directly, when S and D are neighbors, or from S to a relay and the the relay to D , when each pair becomes neighbor respectively
- Throughput of each session is $O(1)$
 - Independent of n

88

Continues from last slide ...

- Delay in packet delivery can be large if $O(1)$ throughput is to be achieved
 - Delay incurred waiting for the destination to arrive close to a relay or the sender
- Trade-off between delay and throughput

89

Measured Capacity [Li01MobiCom]

- Confirms intuition
- In fixed networks, capacity is higher if average distance between source-destination pairs is small

90

Measured Scaling Law [Gupta01]

- Measured in static networks
- Throughput declines worse with n than theoretically predicted
- Due to limitations of existing MAC protocols
 - Unable to exploit “parallelism” in channel access

91

Capacity

- How to design MAC and routing protocols to approach theoretical capacity ?
- Open problem

92

Implementation Issues

93

Existing Implementations

- Several implementations apparently exist (see IETF MANET web site) and Wikipedia
- Most implementations focus on unicast routing
- Network simulator impl. available for AODV, DSR, OLSR, TORA, etc.
- Linux implementations available for: AODV, DSR, OLSR, TORA
- NIST.gov's mLab implementation, including Secure Routing and Intrusion Detection for MANETs
 - <http://csrc.nist.gov/groups/SNS/manet/projects.html>
- One Laptop per Child program
- Swedish Terranet AB's cell-phone based ad hoc network

94

DARPA TTNT Program Demo

- DARPA's Tactical Target Networking Technology (TTNT) Program Demo in 2005
- Fifteen terminals connecting multiple aircraft with a static ground center and three mobile ground nodes
- http://www.darpa.mil/ipto/Programs/ttnt/docs/TTNT_Demo.pdf
- Demo highlights
 - Transmit data at 2 Mbps over 100 n. miles
 - Network capacity of 10 Mbps
 - Transmit data in less than 2ms
 - Multi-hop routing from aircraft to ground nodes
- Data traffic: VoIP, Still Images, Streaming video, Internet access, Chat, Email

95

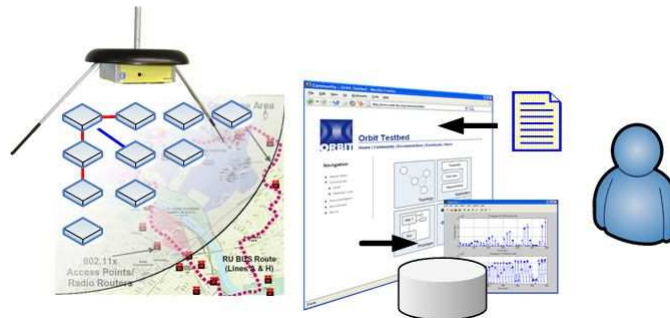
Canadian Navy Ad Hoc Net

- Ad Hoc Network for: "tactical data exchanges, enhanced situational awareness and collaborative planning"
- Features: "built-in text chat, comprehensive signal display and a remote control graphic user interface"
- Rockwell Collins to supply radios and networking technology
- <http://www.rockwellcollins.com/news/page11813.html> (July 2009)

96

ORBIT Testbed

- Wireless Network Emulator (indoor) consisting of 400 802.11 a/b/g radios, from Rutgers Univ., USA
- Network topology dynamically reconfigured via web interface
- Available to both US and outside-US educational institutions
- Virtual Mobility of nodes supports Brownian motion or random waypoint model



Courtesy: <http://www.orbit-lab.org/attachment/wiki/WikiStart/orbit-overview.jpg>

97

DARPA IT-MANET Program

- Objective: To develop “**information theory to describe MANET capacity limits and tradeoffs**”
- Most of current capacity analysis is based on limited assumptions (e.g. no mobility)
- Understand the benefits of network coding, layerless architecture, and distributed optimization
- FLOWS Project: Stanford, MIT, Caltech and UIUC
- Nequit Project: UT Austin, MIT, Northwestern, etc.

98

Related Standards Activities

99

Internet Engineering Task Force (IETF) Activities

- IETF manet (**Mobile Ad-hoc Networks**) working group
 - <http://www.ietf.org/html.charters/manet-charter.html>

- IETF mobileip (**IP Routing for Wireless/Mobile Hosts**) working group
 - <http://www.ietf.org/wg/concluded/mobileip.html>

100

IETF MANET WG Group: Status

| Protocol | RFC Number | Date |
|--------------------------------|-------------|-----------|
| AODV | 3561 | Jul. 2003 |
| OLSR | 3626 | Oct. 2003 |
| TBRPF | 3684 | Feb. 2004 |
| DSR | 4728 | Feb. 2007 |
| Packet Msg. Format | 5444 | Feb. 2009 |
| Rep. Multi-Time Value | 5497 | Mar. 2009 |
| IANA Allocations | 5498 | Mar. 2009 |
| Dynamic MANET On-demand (DYMO) | | Mar. 2009 |
| OLSR v2 | | Sep. 2009 |

101

Related Standards Activities

- IEEE 802.11 and IEEE 802.11s
- BlueTooth
- HomeRF
- Hiperlan/2

102

Future of MANET

- Military, Disaster Recovery Applications

- Extensions considered in different forms:
 - Vehicular Ad Hoc Networks (VANET)
 - Intelligent Vehicular Ad Hoc Networks (inVANET: IEEE 802.11p; DSRC/WAVE)
 - Wireless Mesh Networks (IEEE 802.11s)
 - Delay Tolerant Networks (DTN)
 - Wireless Sensor Networks

103

Results based on ns2 and OPNET implementations is in separate presentation.

Thank you !!

For more information, send e-mail to
Krishna Sivalingam at
krishna.sivalingam@gmail.com
skrishnam@iitm.ac.in

104