ECE453 – Introduction to Computer Networks

Lecture 13 – Network Layer (V) -

1

Mobile IP

2

Stationary vs. Mobile

- Current Internet protocol suite assumes end-systems are stationary
- In end-to-end connection, if one end moves, the network session breaks, so does all the networking services layered on top of IP
- Solution?
- Option 1: completely redesign each layer of the protocol suite
- Option 2: provide additional services at the network layer in a backward compatible manner – mobile internetworking

3

"Mobility is essentially an address translation problem and is best resolved at the network layer"

4

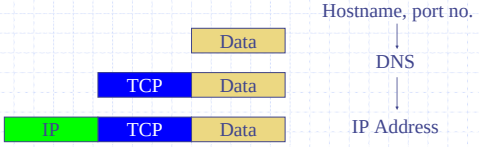
Internet Naming and Addressing

- Hierarchical addressing, can only be used within a domain of its definition. Therefore, the Internet address is location-dependent.
- Host names are location-independent, used as a way for applications to make reference to network entities
- DNS (a directory lookup operation)
  - Optimized for *access* operation (recursive query, caching, etc.), not for *update* operation

5

Fundamental Problem

- The IP address serves dual purposes
  - For the transport and application layer, it serves as end-point identifier
  - For the network layer, it is used as a routing directive



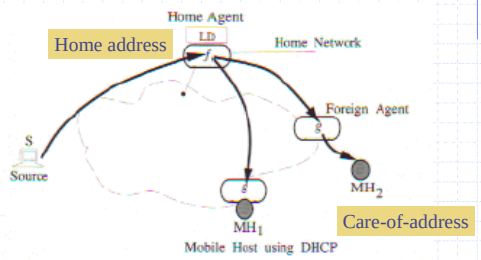
6

Two Tier Addressing

- Associate two internet addresses with each mobile host, decouple the dual role of an internet address
  - The first address component serves as a routing directive (dynamic)
  - The second component serves as an end-point identifier (remains static)

7

Mobile IP - Triangle routing



From [3]

8

Routing in Mobile Ad Hoc Networks (MANET)

Modified from Nitin H. Vaidya's tutorial at MobiCom 2001
http://www.cs.tamu.edu/faculty/vaidya/

9

Mobile Ad Hoc Networking - MANET

- A mobile, ad hoc network is an autonomous system of mobile hosts connected by wireless links.
- There is no static infrastructure such as base stations.
- No centralized administration
- Infrastructureless networking
- Each node is both an end-host and a router

10

Why Ad Hoc Networks ?

- Ease of deployment
- Speed of deployment
- Decreased dependence on infrastructure
- Many applications
  - Personal area networking (cell phone, laptop, ear phone, wrist watch)
  - Military environments (soldiers, tanks, planes)
  - Civilian environments (taxi cab network, meeting rooms, sports stadiums, boats, small aircraft)
  - Emergency operations (search-and-rescue, policing and fire fighting)

11

MANET Characteristics

- Dynamic topologies
- Bandwidth-constrained
  - congestion is typically the norm rather than the exception
- Energy-constrained operation
  - rely on batteries or other exhaustible means for their energy
- Limited physical security
  - increased possibility of eavesdropping, spoofing, and denial-of-service attacks
- Some envisioned networks (e.g. mobile military networks or highway networks) may be relatively large
  - e.g. tens or hundreds of nodes per routing area

12

Routing Protocols

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

13

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

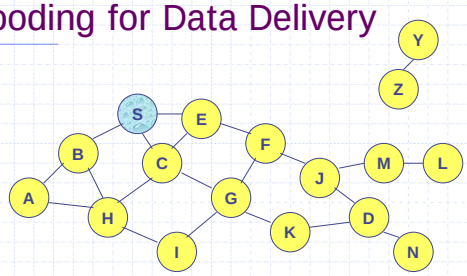
14

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

15

Flooding for Data Delivery



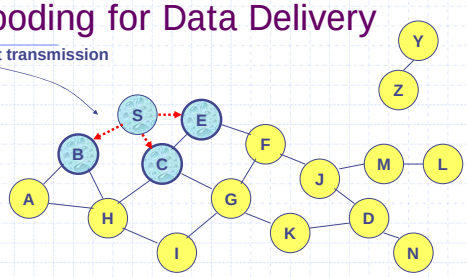
Represents a node that has received packet P

Represents that connected nodes are within each other's transmission range

16

Flooding for Data Delivery

Broadcast transmission

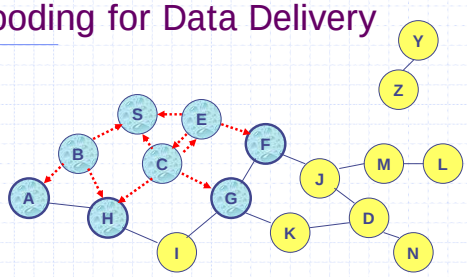


Represents a node that receives packet P for the first time

Represents transmission of packet P

17

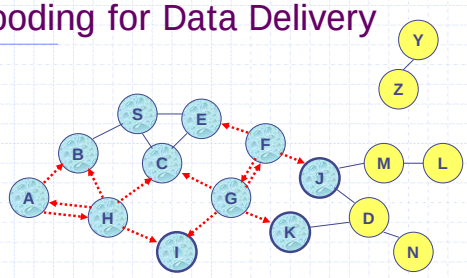
Flooding for Data Delivery



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

18

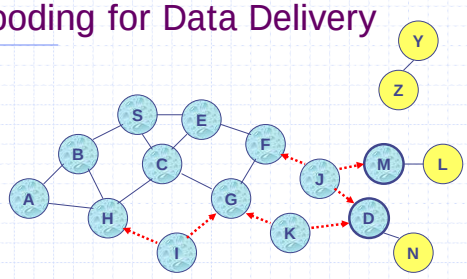
Flooding for Data Delivery



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

19

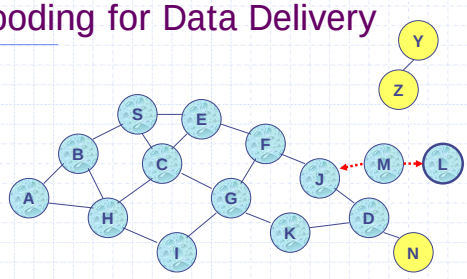
Flooding for Data Delivery



- 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

20

Flooding for Data Delivery



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

21

Flooding for Data Delivery: Advantages

- Simplicity
- May be more efficient than other protocols 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

22

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

23

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

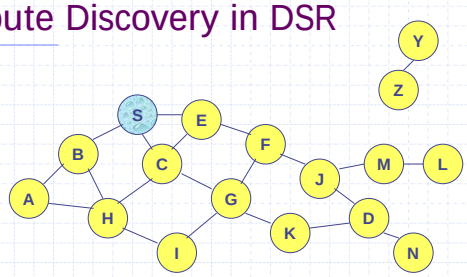
24

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

25

Route Discovery in DSR

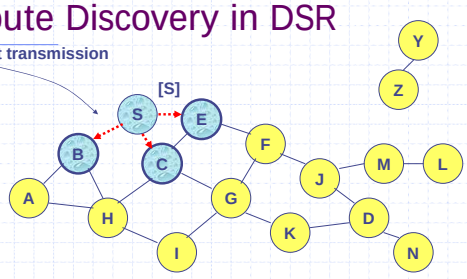


Represents a node that has received RREQ for D from S

26

Route Discovery in DSR

Broadcast transmission

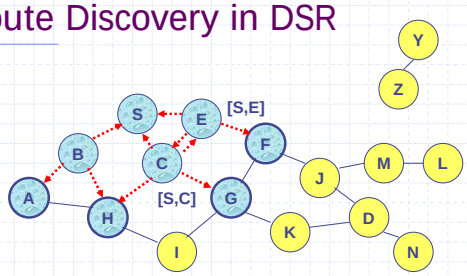


Represents transmission of RREQ

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

27

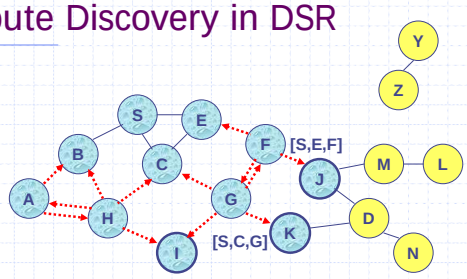
Route Discovery in DSR



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

28

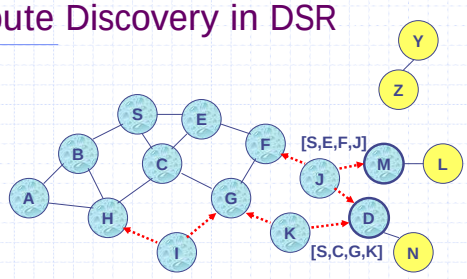
Route Discovery in DSR



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

29

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

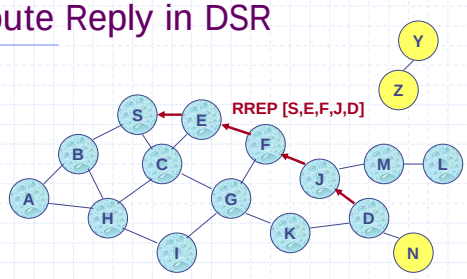
30

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

31

Route Reply in DSR



← Represents RREP control message

32

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 D from node S
  - 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)

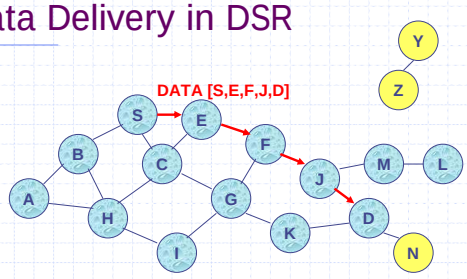
33

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

34

Data Delivery in DSR



Packet header size grows with route length

35