Routing and Transport in Mobile Ad hoc Networks

Slides from other sources used (notably, Nitin Vaidya’s excellent tutorial)
Mobile Ad Hoc Networks

- May need to traverse multiple links to reach a destination
Mobile Ad Hoc Networks (MANET)

- Mobility causes route changes
Why is Routing in MANET different?

- Full Self-configuration
  - No address hierarchy

- 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

- In sensor networks – nodes sleep/wake up/run out of energy

- New performance criteria may be used
  - route stability despite mobility
  - energy consumption
Communication Operations

Types: (n: network size)
- Unicasting: (1, 1) = (source, destination)
- Multicasting: (1, k), 1 < k < n
- Broadcasting: (1, n)
- Geocasting: (1, k in a region)
- Gossip: (n, n)
- Gathering: (k, 1)
- Fusion: a special type of gathering (with simple data processing at intermediate nodes)
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
Overview of Unicast Routing Protocols
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
Represents that connected nodes are within each other’s transmission range

Represents a node that has received packet P
Flooding for Data Delivery

Broadcast transmission

- Represents a node that receives packet P for the first time
- Represents transmission of packet P
Node H receives packet P from two neighbors:
potential for collision
Node C receives packet P from G and H, but does not forward it again, because node C has already forwarded packet P once.
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
Flooding for Data Delivery

- Node D does not forward packet P, because node D is the intended destination of packet P
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)
Flooding may deliver packets to too many nodes (in the **worst case**, all nodes reachable from sender may receive the packet)
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
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

- Possible low 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
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
Ad Hoc Routing Approaches

- Two types of Ad hoc routing protocols:
  1. Table-driven routing (proactive)
     - Try to maintain up-to-date info for all nodes
     - Periodic route-update messages propagate to all nodes
     - Advantage: route to a destination is always available
       - Disadvantage: high overhead; slow to converge
  2. On-demand routing (reactive)
     - Source discovers a path to destination only when needed
     - Path maintained until it breaks or is no longer necessary
     - Advantage: less overhead due to “route-messages”
       - Disadvantage: source must wait until route is discovered
Additional Classification

- Flat vs. Hierarchical

- Hybrid
  - Zone routing: Proactive routing in a node’s neighborhood + Reactive routing between neighborhoods
Additional Classification

- Hierarchical
  - Cluster-based
  - Connected minimum dominating set (NP-hard)
  - Virtual backbone
    - Subset of nodes hosts location databases
    - Virtual backbone between those nodes (non-position-based routing algorithm)
    - Send position update and query to the nearest backbone nodeB
    - Backbone node contacts the nodes of a (usually different) quorum
    - Timestamps to choose most current information
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.
Route Discovery in DSR

Represents a node that has received RREQ for D from S
Route Discovery in DSR

Broadcast transmission

[S] Represents transmission of RREQ

[X,Y] Represents list of identifiers appended to RREQ
Node H receives packet RREQ from two neighbors: potential for collision
Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once.
• 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

RREP [S,E,F,J,D]

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
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 F forwards Route Reply RREP [S,E,F,J,D], node F learns route [F,J,D] to node D.
- When node E forwards Data [S,E,F,J,D] it learns route [E,F,J,D] to node D.
- A node may also learn a route when it overhears Data packets.
Use of Route Caching

- When node S learns that a route to node D is broken, it uses another route from its local cache, if such a route to D exists in its cache. Otherwise, node S initiates route discovery by sending a route request.

- Node X on receiving a Route Request for some node D can send a Route Reply if node X knows a route to node D.

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

[S,E,F,J,D]  [E,F,J,D]

[S,J,D], [F,E,S]

[J,F,E,S]

[P,Q,R] Represents cached route at a node
(DSR maintains the cached routes in a tree format)
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
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.
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.
Route Caching: Caution!

- 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

- Effect doubly worse on TCP

- There is some work on improving cache validity
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
DSR-AODV Similarities

- Route Request: Forwarding/Response
  - Route request RREQ
  - Route Reply: RREP
  - Routing errors: RRER

- Path Reversal
  - Assumes bidirectional link symmetry

- Flooding
DSR-AODV Differences

- AODV is a Distance Vector algorithm
  - Not source routing: Routing information is stored in the node, not in the packet
  - Maintains at most one route for a single destination – Shortest path

- Sequence number
  - Ensures RREQs not forwarded unnecessarily
  - Keep up with a potentially dynamic network by maintaining the freshness of route information
AODV Routing Table

- Routing table of each node maintains
  - Next-Hop
  - Sequence number
  - Hop Count

- Values updated on receipt of RREQ, RREP, or RRER

- NIST Quick Guide to AODV
Link Quality Source Routing [Sigcomm 2004]

- Recall fading/nastiness of wireless propagation
- Big difference between hops – using number of hops as metric can lead to really bad behavior
- Solution – measure link quality and make it visible to routing protocol
- Possible link quality metrics
  - ETX (product of forward and backward delivery ratio) – MIT/roofnet project (Mobicom 2003)
  - Link RTT
  - Packet pair, etc..
  - ETX seems to work best
  - ETT and other newer metrics for measuring link quality
- LQSR (from microsoft) is an extended DSR with link
Location-Aided Routing (LAR) [Ko98Mobicom]

- Exploits location information to limit scope of route request flood
  - Location information may be obtained using GPS

- *Expected Zone* is determined as a region that is expected to hold the current location of the destination
  - Expected region determined based on potentially old location information, and knowledge of the destination’s speed

- Route requests limited to a *Request Zone* that contains the Expected Zone and location of the sender node
Expected Zone in LAR

\[ X = \text{last known location of node D, at time } t_0 \]

\[ Y = \text{location of node D at current time } t_1, \text{ unknown to node S} \]

\[ r = (t_1 - t_0) \times \text{estimate of D’s speed} \]
Request Zone in LAR

Network Space

Request Zone

A
B
S

X
Y
r
LAR

- Only nodes **within the request zone** forward route requests
  - Node A does not forward RREQ, but node B does (see previous slide)

- Request zone explicitly specified in the route request

- Each node must know its physical location to determine whether it is within the request zone
LAR

- Only nodes within the request zone forward route requests

- If route discovery using the smaller request zone fails to find a route, the sender initiates another route discovery (after a timeout) using a larger request zone
  - the larger request zone may be the entire network

- Rest of route discovery protocol similar to DSR
Proactive Protocols
Proactive Protocols

- Schemes discussed so far are reactive.
- Proactive schemes based on distance-vector and link-state mechanisms have also been proposed.
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.
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.
Optimized Link State Routing (OLSR)

- Nodes C and E are multipoint relays of node A

Node that has broadcast state information from A
Optimized Link State Routing (OLSR)

- Nodes C and E forward information received from A

Node that has broadcast state information from A
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
OLSR

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

- 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
Hybrid Protocols
Zone Routing Protocol (ZRP) [Haas98]

Zone routing protocol combines

- Proactive protocol: which pro-actively updates network state and maintains route regardless of whether any data traffic exists or not

- Reactive protocol: which only determines route to a destination if there is some data to be sent to the destination
ZRP

- All nodes within hop distance at most $d$ from a node X are said to be in the routing zone of node X.

- All nodes at hop distance exactly $d$ are said to be peripheral nodes of node X’s routing zone.
ZRP

- **Intra-zone routing**: Pro-actively maintain state information for links within a short distance from any given node
  - Routes to nodes within short distance are thus maintained proactively (using, say, link state or distance vector protocol)

- **Inter-zone routing**: Use a route discovery protocol for determining routes to far away nodes. Route discovery is similar to DSR with the exception that route requests are propagated via peripheral nodes.
ZRP: Example with
Zone Radius = \( d = 2 \)

S performs route discovery for D

Denotes route request
ZRP: Example with $d = 2$

S performs route discovery for D

E knows route from E to D, so route request need not be forwarded to D from E

Denotes route reply
ZRP: Example with $d = 2$

S performs route discovery for D

Denotes route taken by Data
Routing

- Protocols discussed so far find/maintain a route provided it exists.

- Some protocols attempt to ensure that a route exists by:
  - Power Control [Ramanathan00Infocom]
  - Limiting movement of hosts or forcing them to take detours [Reuben98thesis]
Performance of Unicast Routing in MANET

- Several performance comparisons
  [Broch98Mobicom, Johansson99Mobicom, Das00Infocom, Das98ic3n]

- While performance varies from protocol to protocol, in general:
  - Reactive has lower overhead when traffic density is low (small number of active routes) and mobility is moderate
  - Proactive better if traffic density is high and mobility is high

- Capacity of a path inversely proportional to number of hops (due to chain self interference)
Network Wide Broadcast
Applications

- Route discovery in reactive routing
- Route propagation in proactive routing
- Paging
- Event notification
- Needed for geocasting, multicast …
Problems with Flooding

- When node A broadcasts a route query, nodes B and C both receive it.
- B and C transmit at about the same time since they are reacting to receipt of the same message from A.
- This results in a high probability of collisions.
- Loss also occurs from fading/other interfering traffic.
Broadcast Storm Problem

- **Redundancy**: A given node may receive the same route request from too many nodes, when one copy would have sufficed
- Node D may receive from nodes B and C both
Solutions for Broadcast Storm

- **Probabilistic scheme:** On receiving a route request for the first time, a node will **re-broadcast (forward)** the request with **probability** \( p \)

- Also, re-broadcasts by different nodes should be staggered by using a collision avoidance technique (wait a random delay when channel is idle)
  - This would reduce the probability that nodes B and C would forward a packet simultaneously in the previous example
Solutions for Broadcast Storms

- **Counter-Based Scheme**: If node E hears more than $k$ neighbors broadcasting a given route request, before it can forward the request itself, then node E will not forward the request.

- **Intuition**: $k$ neighbors together have probably already forwarded the request to all of E’s neighbors.
Solutions for Broadcast Storms

- **Distance-Based Scheme:** If node E hears RREQ broadcasted by some node Z within physical distance $d$, then E will not re-broadcast the request.

- **Intuition:** Z and E are too close, so transmission areas covered by Z and E are not very different. If E re-broadcasts the request, not many nodes who have not already heard the request from Z will hear the request.
Summary: Broadcast Storm Problem

- Flooding is used in many protocols, such as Dynamic Source Routing (DSR)

- Problems associated with flooding
  - collisions
  - redundancy

- Collisions may be reduced by “jittering” (waiting for a random interval before propagating the flood)

- Redundancy may be reduced by selectively re-broadcasting packets from only a subset of the nodes