Today

- Unicast routing.

PAMAS [Observations]

- When A wakes up, overhears; sends probe on control channel.
- \( t_{\text{probe}}(l) \), \( l \) is maximum frame length.
- Xmitters finishing between \([l/2, l]\), respond with \( t \).
- If no collisions, A use \( t \).
- If no response, A probes \([3l/4, l]\), etc.

Announcements

- Project 1 due today.
- Kumar will lecture on multicast routing protocols.
Unicast Routing in MANETs

MANETs
- No fixed infrastructure!
- Multiple hops to reach destinations.
  - Route changes because of node movements.
- Radio used for communication.
  - Variable transmission.
  - Broadcast nature of radio.
  - Interference, fading, etc.

Mobility
- Many variations in mobility patterns:
  - Almost fixed (sensors, actuators).
  - Highly mobile (vehicles).
  - Discrete movements.
  - Continuous movements.
- Mobility Characteristics
  - Speed.
  - Direction.

Ad-Hoc Routing Requirements
- Distribution paths
  - Multi hop paths.
  - Loop free.
  - Minimal transmission data overhead.
- Self starting and adaptive to dynamic topology.
- Low consumption of memory, bandwidth, power.
  - Scalable with number of nodes.
  - Localized effects of link failure.
Many protocols have been proposed.
Some have been invented specifically for MANET.
Others adapted from protocols for wired networks.
No single protocol works well in all MANET environments!
Adaptive protocols?

Problems using DV or LS

DV protocols:
- May form loops: wasteful in wireless environment
  - Bandwidth and power.
- Loop avoidance may be complex

LS protocols:
- Higher storage and communication overhead.

Unicast routing classification

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.
Trade-Offs

- 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.

Trade-offs (Cont'd)

- Overhead of route discovery/maintenance.
  - Reactive protocols may have lower overhead since routes are determined only if needed.
  - Proactive protocols typically result in higher overhead due to continuous route updating.

Which approach achieves a better trade-off depends on the traffic and mobility patterns.

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; why?
- P reaches D if it is reachable from S.
- Node D does not forward P.
Flooding for Data Delivery

- 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

- 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 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 of Data: Advantages
- Simplicity.
- May be more efficient when rate of information transmission is low compared to topology changes.
  - 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: 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, D would not receive the packet at all.

Flooding of Control Packets

- Many protocols perform (potentially limited) flooding of control packets.
- Control packets are used for route discovery/maintenance.
- 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.

Dynamic Source Routing (DSR) [Johnson96]

- When node S wants to send a packet to D, but does not know a route to D, node S initiates a route discovery.
- 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

- 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 Reply in DSR

- Represents RREP control message.

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 can be sent by reversing the route in RREQ only if links are guaranteed to be bi-directional.
- If unidirectional (asymmetric) links are allowed, then RREP may need a route discovery for S from D.
- Unless D already knows a route to S.
- If a route discovery is initiated by D for a route to S, then the RREP is piggybacked on D's RREQ.
Processing RREP
- Node S on receiving RREP, caches the route.
- 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.

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

Data Delivery in DSR
- Packet header size grows with route length

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], F learns route [F,J,D] to D.
  - When node E forwards Data [S,E,F,J,D] it learns route [E,F,J,D] to node D
  - Nodes may also learn route when it overhears data.
Use of Route Caching

- When S learns that a route to D is broken, it uses another route from its local cache, if such a route to D exists in its cache; otherwise, S initiates route discovery.
- Node X on receiving a RREQ for some node D can send a RREP if X knows a route to D.
- Use of route cache
  - Can speed up route discovery.
  - Can reduce propagation of route requests.

Route Caching: 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.

Route Caching: Reduce Propagation of REQs

Assume that there is no link between D and Z. Route Reply (RREP) from node K limits flooding of RREQ.
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.

Route Caching: Beware!

- Stale caches can adversely affect performance.
  - With 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.
  - Adverse impact on TCP performance.

DSR: Advantages

- Routes maintained only between nodes who need to communicate.
- Reduces overhead of route maintenance.
- Route caching can further reduce route discovery overhead.
- Single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches.

DSR: Disadvantages

- Packet header size grows with route length.
- 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.
DSR: Disadvantages

- Increased contention if too many route replies come back due to nodes replying using their local cache.
- “RREP” storm problem.
- Reply storm may be eased by preventing a node from sending RREP if it hears another RREP with a shorter route.

DSR: Disadvantages

- An intermediate node may send RREP 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.
  - Static timeouts.
  - Adaptive timeouts based on link stability.

Ad Hoc On-Demand Distance Vector Routing [Perkins99]

- 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 nodes, so that data packets do not have to contain routes.
- Like DSR, AODV is reactive.

AODV

- Route Requests (RREQ) are forwarded similarly to DSR.
  - When a node re-broadcasts a RREQ, it sets up a reverse path pointing towards the source.
  - AODV assumes symmetric (bi-directional) links.
- When the intended destination receives a RREQ, it replies by sending a RREP.
- RREPs travel along the reverse path set-up when RREQ is forwarded.
Route Requests in AODV

- Represents a node that has received RREQ for D from S

AODV Route Discovery: Observations

- RREQ contains source and destination IP address, current dest. seq. number, and broadcast id (incremented for every RREQ).
- Source IP + bcast id uniquely identifies RREQ; nodes don't forward recently seen RREQs.
- RREQ processing: node creates reverse route table entry for RREQ source with TTL.
- If node has "unexpired" route to destination in its table with sequence number >= RREQ's, replies to RREQ with Route Reply (RREP) back to source.
- Otherwise, broadcast RREQ onward.
Destination Sequence Number

- When node D receives route request with destination sequence number N, D will set its sequence number to N, unless it is already larger than N.
- Node’s own sequence number is monotonically increasing.
- Sequence number is incremented after neighborhood topology change.

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.
- Node D does not forward RREQ, because node D is the intended target of the RREQ.
Route Reply in AODV

- In intermediate node has current route to destination, responds to RREQ with RREP.
- RREP contains source and destination IP, current sequence number, number of hops to destination.
  - If destination, then destination seq. #.
  - Else, node's current record of destination's seq. #.
- Node receiving RREP sets up forward path to destination.
  - If multiple RREPs received, node forwards first one. Later RREPs discarded unless greater seq. # or smaller # of hops.

Route Reply Example

Forward Path Setup in AODV

Forward links are setup when RREP travels along the reverse 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.
- Routing table entry maintaining a forward path is purged if not used for active route timeout interval.
- If no 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

- Link failures are propagated by means of Route Error messages, which also update destination sequence numbers.
  - RERR lists destinations now unreachable.
  - If upstream node has neighbors as precursors for the affected destinations, it broadcasts RERR.
  - Nodes receiving the RERR update cost to destination to infinity and forward RERR if needed.
  - Upon receiving RERR, source will initiate route discovery if still needs route.

## 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.

## Link Failure Detection

- Hello messages: neighbor nodes periodically exchange hello messages.
- Absence of hello message is used as an indication of link failure.
- Alternatively, failure to receive several MAC-level ACKs may be used as an indication of link failure.
Sequence Numbers in AODV

- To avoid using old/broken routes.
- To determine which route is newer.

Optimization: Expanding Ring Search

- RREQs are initially sent with small Time-to-Live (TTL) field, to limit their propagation.
- DSR also includes a similar optimization.
- If no RREP is received, then larger TTL tried.

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.
Flooding of Control Packets

- How to reduce the scope of the route request flood?

Location-Aided Routing (LAR) [Ko98Mobicom]

- Exploits location information to limit scope of route request flood.
- Location information may be obtained using GPS.
- **Expected Zone**: region expected to hold the current location of the destination.
- Expected region based on old location information, and knowledge of destination's speed.
- Route requests limited to a **Request Zone** that contains Expected Zone and location of 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**: area containing the destination's expected location and the location of the sender node.
LAR

- Only nodes within request zone forward RREQs.
  - Node A does not forward RREQ, but node B does.
  - Request zone explicitly specified in the RREQ.
  - Each node must know its physical location to determine whether it is within the request zone.

- If route discovery using smaller request zone fails to find a route, sender initiates another route discovery (after a timeout) using larger request zone.
  - Larger request zone may be the entire network.
  - Rest of route discovery protocol similar to DSR.

LAR Variations: Adaptive Request Zone

- Each node may modify the request zone included in the forwarded request
- Modified request zone may be determined using more recent/accurate information, and may be smaller than the original request zone

Adaptive Request Zones
LAR Variations: Implicit Request Zone

- In the previous scheme, RREQ explicitly specified request zone.
- **Alternative approach**: node X forwards RREQ received from Y if X is deemed to be closer to expected zone as compared to Y.
- The motivation is to attempt to bring the RREQ physically closer to the destination node after each forwarding.

More on LAR...

- Basic LAR assumes that, **initially**, location information for X becomes known to Y only during route discovery.
- This location information is used for future route discovery. Why?

**Variations**

- Location information can also be piggybacked on any message from Y to X.
- Y may also proactively distribute its location.
- Similar to other protocols (e.g., DREAM, GLS).

LAR Summary

- **Disadvantages**: Nodes need to know their physical locations. Choice of request zone.
So far...

- All protocols discussed so far perform some form of flooding.
- Now we will consider protocols which try to avoid flooding.

Link State Routing
[Huijema95]

- 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]

- Overhead of flooding link state information reduced by having fewer nodes forward the information.
- Broadcast from X only forwarded by its multipoint relays (MPRs).

MPRs

- 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 know their 2-hop neighbors.
- MPRs of X are 1-hop neighbors of X covering X’s 2-hop neighbors.
Optimized Link State Routing (OLSR)

- C and E are multipoint relays of A.

Node that has broadcast state information from A

Nodes C and E forward information received from A.

Node that has broadcast state information from A

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

Node that has broadcast state information from A

OLSR

- OLSR is proactive.
- It floods information through MPRs.
- Flooded information contains links connecting nodes to respective MPRs.
  - I.e., node sends info on nodes that selected it as their MPR.
  - Periodic HELLO messages inform nodes which other nodes selected it as their MPR.
- Routes used by OLSR only include multipoint relays as intermediate nodes.
Hybrid Protocols

ZRP [Haas98]

Zone Routing Protocol combines:
- Proactive protocol: which pro-actively updates network state and maintains routes 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.

Routing Zone

- All nodes within hop distance of at most $d$ from node $X$ are said to be in the routing zone (RZ) of $X$.
- All nodes at hop distance exactly $d$ are said to be peripheral nodes of $X$'s routing zone.
- Each node maintains its own RZ.

ZRP “Hybridness”

- Limits scope of proactive procedure to a node’s local neighborhood.
- Limits scope of topology changes to local neighborhood.
- Reactive protocol executed for routes to destination far-away.

Routing Zone
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: Uses reactive 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 $D$
- $E$ knows route from $E$ to $D$, so route request need not be forwarded to $D$ from $E$
- Denotes route reply
- Denotes route request
- Denotes route taken by Data