Lecture 5
Mobile Ad-Hoc Networks: Routing

Reading:

- "Routing Protocols for Ad Hoc Wireless Networks," in *Ad Hoc Wireless Networks: Architectures and Protocols*, Chapter 7.
- D. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts," Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, Dec. 1994.
- E. Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," *IEEE Personal Communications Magazine*, April 1999, pp. 46-55.
- J. Broch, D. Maltz, D. Johnson, Y.-C. Hu, and J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," *Proc. Mobicom '98*, Oct. 1998.
- S. Singh, M. Woo, and C. Raghavendra, "Power-Aware Routing in Mobile Ad Hoc Networks," *Proc. Mobicom '98* , Oct. 1998.

Mobile Ad-Hoc Networks (MANETs)

- Definition
  - “A collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or standard support services.”
- Ad-hoc network topology is dynamic—nodes enter and leave the network continuously
- No centralized control or fixed infrastructure to support network configuration or reconfiguration
- Example scenarios for MANETs
  - Meetings
  - Emergency or disaster relief situations
  - Military communications
  - Wearable computers
  - Sensor networks

MANETs (cont.)

- Mobile nodes have limited communication range
  - Reduces battery drain
  - Enables spatial reuse of limited bandwidth → increased network capacity
- To connect all nodes in the network, each node is a
  - Packet source
  - Packet sink
  - Router
- Nodes must route packets for other nodes to keep the network fully connected
- In MANETs, *routing* must be addressed

MANETs (cont.)

- Route-finding:
  - Want to determine an “optimal” way to find “optimal” routes
- Dynamic links
  - Broken links must be updated when a node moves out of communication range with another node
  - New links must be formed when a node moves into communication range with another node
  - Based on this new information, routes must be modified
- Frequency of route changes a function of node mobility

Conventional Routing Protocols for Wired Networks

- Distance vector routing
  - Each router has a table giving the distance from itself to all possible destinations
  - Each router periodically broadcasts its table to its neighbors
    - Neighbors will update their tables based on this information to ensure they are using the shortest route to reach each destination
  - To route a packet, router checks table to find next hop to destination
  - Tradeoff in how often routing tables are exchanged
    - Too often → large amount of overhead, excess BW and computational resources used
    - Too infrequent → sub-optimal or invalid routes (stale routes)
    - Can send routing table updates whenever information in the table changes due to a new link or a broken link

Conventional Routing Protocols (cont.)

- Link state routing
  - Each router has a complete view of the topology of the entire network
  - “Cost” associated with each link
  - Router monitors cost of link to each neighboring router
    - When cost changes, this information is sent to all routers in the network
    - Each router has a consistent view of the network
  - Each router can compute the shortest path from itself to the destination
    - Incoming packet forwarded along this path
  - Link state protocols
    - Converge more quickly than distance vector protocols
    - Require more BW and compute power than distance vector protocols

Problems with using Conventional Routing in MANETs

- Unidirectional links
  - A can communicate with B does not always imply B can communicate with A
- Redundant links
  - In wired networks, only one or a small number of routers connecting two networks
  - In wireless networks, may be several “gateway” nodes between a source and a sink due to wireless channel properties
    - Several redundant paths may be generated
    - Waste of BW, computation, and storage

Problems with using Conventional Routing in MANETs

- Periodic routing updates
  - Cost of sending routing updates (BW, energy) is much greater in a wireless network than in a wired network
  - Routing updates required even if nothing has changed
  - In highly-connected network, routing updates may collide
  - Mobiles cannot enter “sleep” state b/c need to hear all routing updates → wastes energy

Problems with using Conventional Routing in MANETs

- Dynamic nature of ad-hoc networks
  - Wired networks relatively stable
    - Occasionally links go down or come up or congestion changes the cost of a link
  - Wireless network links continuously changing due to node mobility and environmental conditions
    - Convergence to stable routes may be too slow to produce useful information if routing updates not sent often enough
    - If routing updates sent too often, wastes battery of mobiles and channel bandwidth

Routing Protocols for MANETs

- Route discovery and route maintenance
- Route discovery
  - Initial discovery of valid route from source to destination
  - Source node can send a query for a destination node
  - Only destination node responds to query
  - If destination located in source's transmission range, destination responds and link established
    - No periodic routing updates needed
    - Approach must be extended to case where destination node not in source node's transmission range
  - Want an approach that is simple and efficient

Route Discovery (cont.)

- One approach is to perform controlled flooding of the query
  - Nodes receiving query will append their address to the route being recorded in the packet header and broadcast updated packet to all neighbors
    - When a node receives a query, it checks to see if its address is already in the header (indicating this packet was already flooded by this node)
    - If address present, node drops packet
  - Each query labeled with unique “request ID”
    - Each node keeps a cache with request ID’s of packets it has already forwarded
    - Discards packets with request ID listed in node’s cache
    - Avoids duplicate queries sent throughout the network
  - Node only propagates first copy of each route request packet it sees

Route Discovery (cont.)

- Typically source and destination will not be far away in an ad-hoc network
  - Can add a TTL (time to live) to route request
  - Each node reduces the TTL by one when it propagates the request
  - If the TTL hits zero, the route request packet is dropped
- When query reaches destination
  - Destination sends response back using route in packet header if available
  - Destination sends response back to node from which it received route request
- Route discovery information can be piggybacked onto data such as TCP connection packets
  - Reduces latency (e.g., start-up time for TCP connection)
  - Increases overhead, since packets flooded throughout network

Route Discovery (cont.)

- Intermediate nodes can cache routes discovered
  - Can use these routes if want to send a packet to a node listed in route
  - Reduces overhead in terms of number of route request packets required
- Nodes can operate in “promiscuous” mode
  - Listen to all packets exchanged on network
  - Cache routes listed in packets

Route Maintenance

- Nodes can determine broken links through ACK/NACK included with most protocols
- If link broken
  - Node that detects broken link reports this information back to sending node
  - Or node can try to fix the broken link by sending out its own route request to the destination
- If no ACK/NACK present in the link-layer protocol, nodes can listen to channel to determine if next hop transmits packet or not
  - If do not hear forwarding of packet, assume link lost
- Explicit routing acknowledgements can also be used to determine the state of links

Proactive vs. Reactive Routing

- Proactive routing: nodes continuously evaluate and update routes
  - Periodic updates
  - Triggered updates—when a link changes
  - Efficient if routes used often
  - Large amount of overhead
  - Similar to conventional routing protocols
- Reactive routing: nodes evaluate and update routes only when they are needed
  - When a node has a packet to send, it checks to see if it has a valid route
  - If no valid route known, node must send out a route-request message to obtain a valid route (controlled flooding of the network)
  - Data sent using valid route
  - Efficient if routes not used often

Proactive Routing Protocols

- Each node maintains consistent, up-to-date routing information in the form of a table with the next-hop to reach every node in the network
- Changes in link state transmitted throughout the network to update each node’s routing table
- Proactive routing protocols
  - DSDV
  - CGSR

DSDV

- Destination-sequenced distance-vector (DSDV)
  - Each node maintains a table with
    - All possible destination nodes
    - Number of hops required to reach that node
    - Next hop along route to that node
    - Sequence number
  - Sequence number used to distinguish new routes from old routes
  - Routing table updates transmitted throughout network
- “Full dump” routing updates
  - Large packet that carries all routing information
  - Transmitted infrequently when little change in existing links
- “Incremental” routing updates
  - Contains only information that has changed since last routing update

DSDV (cont.)

- Route broadcast packet transmitted with
  - Address of destination
  - Number of hops to reach destination
  - Sequence number of information
  - Sequence number of broadcast packet
- Used to update tables at intermediate nodes
  - If sequence number of update same as sequence number of information in a node’s table, uses the route with the shortest path
  - If update newer, node replaces its information with the updated route

Clusterhead Gateway Switch Routing (CGSR)

- Clustering multihop approach
- Cluster head controls nodes in cluster
  - Nodes within cluster use CDMA-type SS code to avoid inter-cluster interference
  - Cluster head can control channel access
- Cluster head selection algorithm within cluster
  - Can perform minimum cluster changes to reduce overhead
  - E.g., only change cluster head if cluster head moves out of cluster or another cluster head moves into cluster
- DSDV used as underlying routing mechanism

CGSR (cont.)

- Nodes send data to cluster head
- Cluster head sends data to “gateway” nodes
- Gateway nodes route packet to new cluster head
- Packet goes from cluster head → gateway → cluster head until it reaches destination’s CH
- Each node keeps “cluster member table” that contains CH node for each mobile in network
  - Updates sent as in DSDV

Reactive Routing Protocols

- Routes created only when needed
- Requires “route discovery” and “route maintenance”
- Also called “source-initiated on-demand routing”
- Goal is to minimize the amount of overhead compared with proactive routing at the expense of latency in finding a route when it is needed
- Reactive routing protocols
  - AODV
  - DSR

AODV

- Ad-hoc on-demand distance vector (AODV)
  - Node needing to find a route to a destination broadcasts a route request (RREQ) to its neighbors
  - Neighbors broadcast RREQ to their neighbors until destination found or intermediate node has recent information about a route to the destination
  - Each RREQ uniquely identified by source’s ID and a sequence number
  - Intermediate nodes keep track of neighbor from which RREQ came to establish valid reverse path
- Destination or intermediate node sends (unicast) route reply “RREP” back to neighbor from which RREQ came
- Intermediate nodes set up routing information based on nodes from which they receive RREP packet
  - These routes contain timers and will expire if not used

AODV (cont.)

- Route maintenance
  - Source node moves
    - Send new RREQ to destination
  - Intermediate node moves
    - Upstream neighbor propagates link failure notification message to source
    - Source can send new RREQ to find valid route
- “Hello” messages used to inform nodes of neighbors
  - Can be used to ensure link kept alive
  - Can contain information about a node’s neighbors to give information about topology

DSR

- Dynamic Source Routing (DSR)
- Similar to AODV but entire route maintained within packet header
  - Intermediate nodes do not need to keep routing information to route packets
  - No periodic route advertisements needed
- Intermediate nodes propagating a “route request’” append their ID to the “route record” in the packet header
- When packet reaches destination or node with valid cached route to destination, “route reply” returned
  - If destination node, send “route record” in “route reply”
  - If intermediate node, append cached route to destination to “route record” in “route reply”

DSR (cont.)

- “Route reply” returned along
  - Cached path to source if available
  - Reverse route of “route record” if symmetric links assumed
  - Piggybacked with a “route request” to the source node
- Route maintenance
  - “Route error” messages used to propagate information about broken links
  - All cached routes with broken links removed
  - Nodes can use promiscuous mode to listen to all traffic on channel
    - Can update their route caches based on information from packets
    - Can send gratuitous “route reply” to source if node knows a better route to destination
  - If intermediate node determines that next hop in “route record” unreachable, can replace this route with a cached route

Comparison of Protocols

- Proactive approaches
  - More efficient when routes used often
  - Assures routes ready when needed
  - Requires periodic route updates (overhead)
  - Node mobility affects entire network as routing update
- Reactive approaches
  - More efficient when routes used occasionally
  - Require node to first find route before data can be transmitted
  - Periodic route updates not required
  - Can have localized route discovery to deal with node mobility

Comparison (cont.)

- Simulations by CMU (Broch et al.)
  - Reactive protocols can deliver many more packets than proactive protocols when node mobility high
    - Proactive protocols have too many routing updates triggered and routes cannot converge
  - Overhead of reactive protocols depends on node mobility
    - DSR has less overhead than AODV
    - Due to intermediate node caching routes and requiring fewer “route requests” to be sent throughout the network
  - Overhead of DSDV constant (periodic updates)
  - When node mobility low, DSDV performs much better than when high
    - Reactive protocols still have lower overhead and better packet delivery ratios

Comparison (cont.)

- Overall conclusions:
  - DSDV performs well only in low-mobility situations
    - Even then, overhead still high
  - DSR and AODV perform well under all mobility situations
    - DSR has lowest packets overhead
    - If overhead includes packet header (overhead in bytes), AODV performs better than DSR due to smaller headers
    - However, header overhead might be less costly than packet overhead due to cost to obtain channel access, MAC/PHY headers, etc.

Current Research in Routing for MANETs

- Hybrid proactive-reactive approaches
- Multicast
- QoS support
  - How can guarantees be provided in such a dynamic environment?
- Resource-aware routing
  - Use metrics besides shortest-path for routing decisions
  - Low power routing
  - Try to avoid network partitioning
- Location-based routing

Power Aware Routing

- Where is energy needlessly expended in routing protocols?
  - Overhearing transmission of packets not intended for the node
  - Contention
  - Overhead in route finding and route maintenance
- Promiscuous mode
  - Some protocols take advantage of nodes overhearing transmissions to other node to gather more information
  - Improves routing (more up-to-date routing information)
  - Large amount of energy required to receive and decode entire packet
- Contention requires power
  - Channel sensing
  - ACK schemes
  - Retransmissions

Power Aware Routing (cont.)

- Route finding and maintenance
  - Overhead packets transmitted throughout network to find optimal routes
  - Many “useless” packets transmitted
- Routing metrics
  - Most MANET routing protocols use “shortest-hop” as optimizing metric for determining “good” routes
  - Other metrics
    - Minimum latency
    - Link quality
    - Location stability
    - Power of intermediate nodes

Power Aware Routing (cont.)

- Why use power as a metric?
  - Can over-use intermediate nodes
    - Causes nodes to run out of energy early
    - Increases contention around overused node
  - Increases system lifetime
  - Reduces chance of partitioning network
- Goal in power-aware routing: to increase network lifetime / time until network partition by evenly distributing energy load
  - Problem similar to load balancing
  - How should routes be chosen to ensure nodes overall energy dissipation kept low while not overly-utilizing any individual node?

Routing Metrics That Incorporate Power

- Shortest-hop
  - Fewer hops → less energy dissipation
  - Downside: does not evenly distribute energy load
- Energy consumed/packet
  - If little traffic, this is the same as shortest hop
  - If large amount of traffic, energy for contention will ensure packet routed around high-load areas
  - If E(i,j) = energy to transmit packet from node i to node j (including reception energy), this metric tries to minimize:

$$e_k = \sum_{i=1}^{j-1} E(i, j)$$

  - Energy per packet model
    - $E(i,j) = \alpha + \beta f(d_{ij}) + \gamma f(\text{congestion})$
    - If large amount of traffic, f(congestion) will cause packet to be routed around traffic, possibly causing a longer route to be taken
    - Drawback: does not take into account relative node energies

Routing Metrics That Incorporate Power (cont.)

- Cost/packet
  - Route packets around nodes with low energy
  - $f_i(x_i)$ = node cost of node i given that it has already expended x_i energy
  - Describes penalty to node (and hence to entire network) if packet routed through node
  - Minimize total cost to send packet: $$c_k = \sum_{i=1}^{j-1} f_i(x_i)$$
  - Choose f_i to reflect battery lifetime remaining
    - If node has little energy left, f_i large
    - E.g., $f_i(x_i) = \alpha x_i$
  - Advantages of this approach
    - Can incorporate battery model in metric
    - Increase time to network partition
    - Congestion reduced due to distributed routes
  - Disadvantages of this approach
    - Does not automatically avoid nodes with highest cost

Routing Metrics That Incorporate Power (cont.)

- Maximum node cost
  - Can develop a metric $f_i(x_i)$ that determines cost of routing a packet through node i
  - Choose path whereby maximum node cost is minimized
- Time to network partition
  - Can minimize time to network partition by finding "cut-set" nodes
    - Removing all of these nodes results in network partitioning
    - Want to evenly distribute energy load among all these nodes
  - Hard to optimize for this metric and maintain low delay and high throughput
  - Can perform a round-robin distribution of packets to nodes in cut-set if all packets the same length
    - Ensures equal power drain among all the critical nodes
  - Can approximate this solution with a minimum cost/packet algorithm

Simulation Results for Power Aware Routing (Singh et al.)

- No extra packet delay recorded using power-aware routing
- Even though routes longer, avoid congestion → fewer retransmissions needed, shorter waiting time to transmit packet, etc.
- Power-aware routing beneficial for
  - Large networks
    - If the network is too small, there are not many alternative routes to choose from
  - Moderate network loads
    - If network lightly loaded, shortest path algorithm is fine
    - If network heavily loaded, cost of contention outweighs any power savings
  - Dense networks
    - These networks have more alternative routes than sparse networks
- Node cost function $f_i(x_i)$ has significant affect on energy savings

Discussion

- What other methods could we use to reduce power for ad-hoc networks?
- What other metrics might be important in determining routes?
- How could routing protocols be adapted to account for multiple metrics and/or metrics that change importance over the lifetime of the ad-hoc network?
- What network properties will affect “quality” of routing protocol?