CS6504

Mobile Computing

Dr. Ayman Abdel-Hamid

Computer Science Department

Virginia Tech

Routing Protocols in MANETs – Part I

Outline

- •Routing Protocols for Ad hoc Networks
- •Example of a reactive routing protocol
  - ➢AODV: *Ad hoc On-demand Distance Vector Routing*

Taxonomy of Routing Protocols

- •One classification → Proactive, Reactive, or Hybrid
- •Another classification
  - ➢*Single-scope*
    - ✓No distinction of nearby and faraway nodes
    - ✓Lower complexity
  - ➢*Multi-scope*
    - ✓Distinguish nodes by their relative position
    - ✓More resources devoted to maintaining topology information of more nearby nodes
    - ✓*Flat* or *hierarchical*
      - ❑Flat schemes do not require specialized nodes such as a route gateway, or a group leader

AODV 1/2

- •Create routes only when desired by the source node
- •Source initiates a *route discovery process* within the network
- •Route discovery process is completed once a route is found or all possible route permutations have been examined
- •Once a route found, maintain using a *route maintenance procedure*
- •Borrows an idea from a proactive routing protocol DSVD (*Destination -Sequence Distance-Vector routing*)
  - ➢Store a sequence number for each destination
  - ➢The sequence number aids in distinguishing between stale routes and new ones (no routing loops)
    - ✓*Source sequence number* used to maintain fresh information about reverse route to source
    - ✓*Destination sequence number* used to specify freshness of route

AODV 2/2

•Routing table entry in AODV contains among others

- ➢Destination IP Address
- ➢Destination Sequence Number
- ➢Network Interface
- ➢Hop Count (number of hops needed to reach destination)
- ➢Next Hop
- ➢Lifetime (expiration or deletion time of the route). *Each time a routing entry is used to forward data, the value is reset to current time + some constant*

Path Discovery 1/3

•Broadcast a route request (RREQ) packet to neighbors, which forward to their neighbors, and so on, until either destination or an intermediate node with a “fresh enough” route to the destination is located

•Intermediate nodes can reply to RREQ *if have route to destination whose corresponding destination sequence number is greater than or equal to that contained in RREQ* (most recent sequence number source has for destination)

•Each node maintains its own sequence number, and a broadcast ID (incremented for every initiated RREQ)

•Some fields in RREQ:

- ➢source address, source sequence number, broadcast ID
- ➢destination address, destination sequence number
- ➢hop count (incremented if RREQ rebroadcast)

Path Discovery 2/3

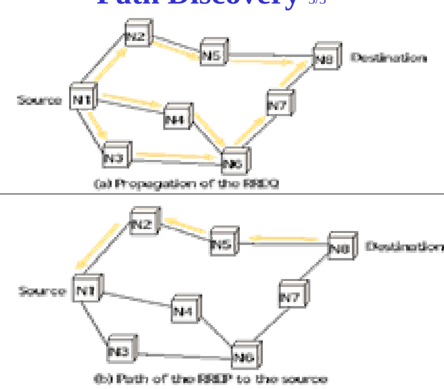
•*While forwarding RREQ*

- ➢Intermediate nodes record in routing table, address of neighbor from which first RREQ packet is received (establish a reverse path to source)
- ➢Discard later copies of same RREQ (RREQ identified by source IP address + broadcast ID)

•*Destination or Intermediate with fresh enough route*

- ➢Unicast a route reply (RREP) to the neighbor form which it received RREQ
- ➢RREP routed back using reverse path
- ➢Nodes along the path establish forward routing entries towards destination
- ➢Some fields in RREP: destination address, destination sequence number, source address, hope count, lifetime)

Path Discovery 3/3



Route Maintenance 1/2

•*If a source moves during active session*: reinitiate route discovery to find a new route

•*If a node along route moves*: upstream neighbor notices the move and propagates a route error message (RERR), to be propagated until reaches source.

- For every destination, maintain a list of *precursor nodes*
- The list of precursors in a routing table entry contains those neighboring nodes to which a route reply was generated or forwarded, and nodes which have forwarded data packets on this route
- Some fields in RERR: Unreachable destination address, unreachable destination sequence number

Route Maintenance 2/2

•In order to maintain local-connectivity, can periodically send HELLO messages

- HELLO messages are local broadcasts (TTL of 1, hence not rebroadcast) to inform each mobile node of other nodes in its neighborhood (unsolicited RREP containing identity and sequence number)
- Not mandatory

Sequence Number Maintenance 1/2

•Destination sequence number is updated at a node *whenever a node receives new information about the sequence number from RREQ, RREP, or RERR messages that may be received related to that destination*

•A destination increments its sequence number when

- *Immediately before a node originates a route discovery* → prevents conflicts with previously established reverse routes towards the originator of a RREQ
- *Immediately before a destination node originates a RREP in response to a RREQ* → update its own sequence number to the maximum of its current sequence number and the destination sequence number in the RREQ packet.

Sequence Number Maintenance 2/2

•*A node may change the sequence number in the routing table entry of a destination only if*

- it is itself the destination node, and offers a new route to itself, or
- it receives an AODV message with new information about the sequence number for a destination node, or
- the path towards the destination node expires or breaks.

Outline

•Example of reactive routing protocol

➢DSR: *Dynamic Source Routing*

DSR

•On-demand routing based on the concept of source routing

•*Source routing* is a technique where the sender of a packet can specify the route that the packet should follow through the network

•For DSR

•Each data packet sent carries in its header the complete ordered list of nodes through which the packet must pass

•Other nodes forwarding or overhearing these packets may cache such route information for future use

•Mobile nodes required to maintain route caches (contain source routes)

•Two major phases: Route discovery and Route maintenance

Route Discovery 1/4

•When a packet is to be sent to Destination

➢Check route cache to locate an unexpired route, if found, use to send packet

➢If no route, broadcast a *Route Request* packet (destination address, source source address, unique identification number)

•At each receiving node

➢Check whether a valid route exists, if not append own address to the *route record* of the packet and broadcast through outgoing links

➢To limit number of propagated route requests, forward if not been seen before, and the node's address does not already appear in the record route

Route Discovery 2/4

•Destination or Intermediate with unexpired route

➢The packet by now contains a route record yielding the sequence of hops taken

➢Generate Route Reply

➢If destination, place route record from route request into route reply

➢If intermediate, append cached route to route record and then generate route reply

•The entity generating the route reply needs a route back to the initiator of the request

➢If route found in route cache, use

➢If symmetric links are supported, reverse route from route request

➢If symmetric links not supported, initiate a route discovery to initiator and piggyback the route reply on new route request

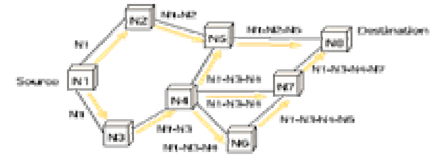
Route Discovery 3/4

•Save a copy of data packet in a *Send buffer* awaiting the outcome of route discovery

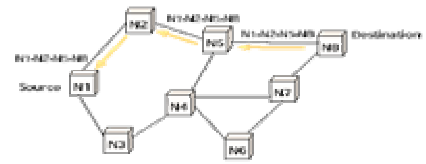
•After residing in buffer for an amount of time, discard

•Use exponential back-off to limit route requests for same target when no route reply is received

Route Discovery 4/4



(a) Building of the route record during route discovery



(b) Propagation of the route reply with the route record

Route Maintenance 1/2

•When originating or forwarding a packet using a source route, each node responsible for confirming packet has been received by next hop along source route

- ➢Retransmit packet (up to some max) until confirmation received

•Acknowledgments

- ➢No cost to DSR through link-level ACK in IEEE 802.11
- ➢Passive ACK (overhearing next hop transmitting packet to next hop)
- ➢A DSR-specific software ACK to be returned by next hop

Route Maintenance 2/2

•If no receipt confirmation

- ➢Return a *Route Error* message to original sender of packet, identifying link over which packet could not be forwarded (use any cached route, or initiate a route discovery to sender)

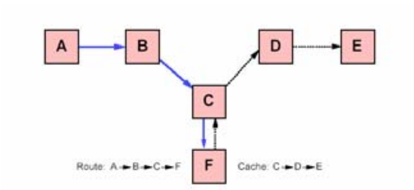
•Source node removes broken link from cache

•Retransmission of original packet is function of upper layer protocols such as TCP

Route Discovery Optimizations 1/2

•An Intermediate node does not generate the route reply if concatenated route plus current route record would create a duplicate. In this case, the edited route does not contain the intermediate node

•Intermediate node discards the request

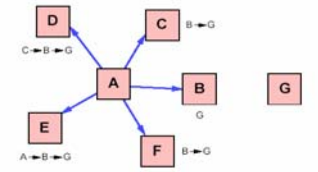


Route Discovery Optimizations 2/2

•*Avoiding route reply storms*

•Provided the node can put the NIC into *promiscuous receive mode*, it delays sending its own Route Reply for a short period while listening to see if the initiating node will use a shorter route

➢Promiscuous receive mode: able to receive all packets on the link, including those not addressed to it at the link layer (disabling link-level address filtering)



Route Maintenance Optimizations

•Packet Salvaging: salvage the data packet that caused the route error rather than discarding it

➢Search own cache for a route to destination, if found, replace route record with own route record from cache

➢Flag packet as being salvaged

•Route Shortening: send gratuitous Route Reply message to sender

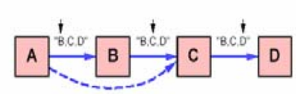


Figure 6: Node **C** notices that the source route to **D** can be shortened, since it overheard a packet from **A** intended first for **B**.