S-72.333 Postgraduate Course in Radio Communications
Spring 2004

Routing in Mobile Ad-Hoc Networks

Mervi Berner 13.05.2004
mervi.berner@iki.fi

Contents

Ad hoc Routing Protocols:

table driven and on-demand [1]

Comparisons [1]

Security [2]

Summary [1,2]

References

Homework

Ad Hoc Routing Protocols

- ***Table-driven protocols***: maintain up-to-date routing information from each node to every other node in the network; differences in number of necessary routing-related tables, methods by which changes in network structure are broadcasted
- ***Source-initiated on-demand routing****:* routes only created when desired by the source node; route discovery process initiated: process completed once a route is found or all possible route permutations have been examined; route established → maintained by route maintenance procedure until either the destination becomes inaccessible along every path from the source or until the route is no longer desired

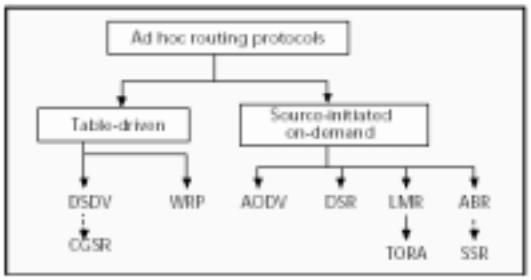


Table-Driven Routing Protocols

The Destination-Sequenced Distance-Vector Routing protocol (DSDV)

- Bellman-Ford routing mechanism (freedom from loops)
- Routing table (each node):
  - all possible destinations, number of hops to each destination, sequence number assigned by the destination node
  - updates transmitted periodically
- Types of packets:
  - ***full dump:*** all available routing information, multiple network protocol data units (NPDUs), transmitted infrequently during occasional movement
  - ***incremental:*** information which has changed since the last full dump, standard-size NPDU, nodes maintain an additional table where incremental routing information packets stored
- New route broadcasts:
  - address of the destination, number of hops to reach the destination, sequence number of the information received regarding the destination, a new sequence number unique to the broadcast
  - the route labeled with the most recent sequence number is always used

Table-driven Routing Protocols

Clusterhead Gateway Switch Routing (CGSR)

- A cluster head controls a group of ad hoc nodes, a cluster head selection algorithm is utilized to elect a node as the cluster head using a distributed algorithm within the cluster
- Disadvantage: frequent cluster head changes can affect routing protocol performance -> Least Cluster Change (LCC) clustering algorithm: cluster heads only change when two cluster heads come into contact, or when a node moves out of contact of all other cluster heads.
- DSDV as the underlying routing scheme; modifies DSDV by using a hierarchical ***cluster-head-to-gateway*** routing approach to route traffic from source to destination.
- "Cluster member table": destination cluster head; broadcast periodically; update on reception
- Routing table: determines the next hop to reach the destination.
- Reception of a packet: node consult its cluster member table and routing table to determine the nearest cluster head along the route to destination, and checks its routing table to determine the next hop used to reach the selected cluster head.

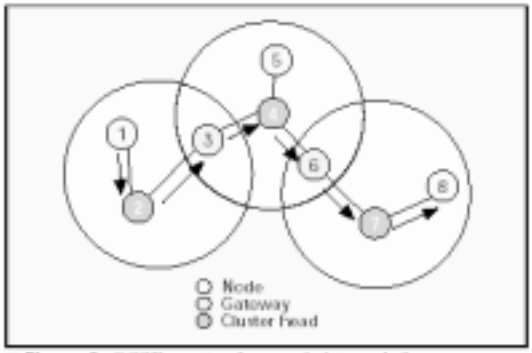


Figure 2. *CGSR: routing from node 1 to node 8.*

Table-driven Routing Protocols

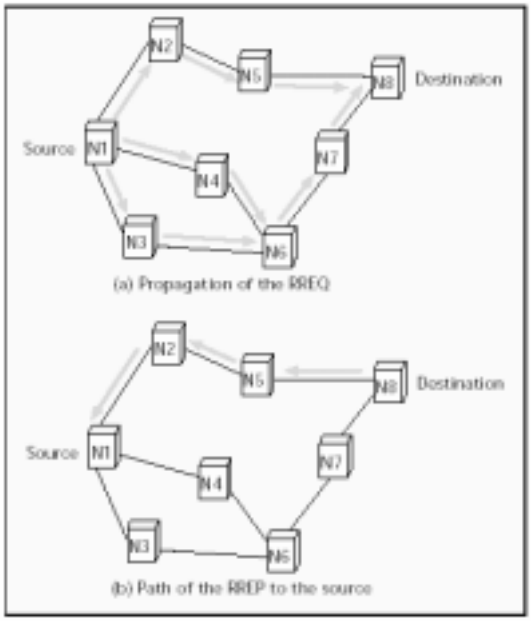
The Wireless Routing Protocol (WRP)

- **Four tables**: Distance table, Routing table, Link-cost table, Message retransmission list (MRL) table
- Each entry of the MRL: sequence number of the update message, retransmission counter, acknowledgment-required flag vector (entry/neighbor), list of updates sent in the update message
- **Update messages**; inform link changes, sent only between neighboring nodes and contains a list of updates (the destination, the distance to the destination, and the predecessor of the destination), and a list of responses (which mobiles should ACK the update)
- ***Hello*** **message**; send within a specified time period to ensure connectivity or from a new node
- Loop freedom: routing nodes communicate the distance and second-to-last hop information for each destination
- 'class of path-finding algorithms'; exception: avoids the "count-to-infinity" problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbors

Source-initiated On-Demand Routing Protocols

The Ad Hoc On-Demand Distance Vector (AODV)

- Improvement on DSDV (on demand)
- ***Path discovery* process**: route request (**RREQ**) broadcast to the neighbors (broadcast ID and node's IP address). Source node includes the most recent sequence number it has for the destination. During RREQ forwarding, intermediate nodes record in their route tables the address of the neighbor from which the first copy of the broadcast packet is received -> establishing a ***reverse path***.
- The destination node responds by unicasting a route reply (**RREP**) packet back to the neighbor from which it first received the RREQ. As the RREP is routed back along the reverse path, nodes along this path set up forward route entries (active forward route) in their route tables.
- If a node along the route moves, its upstream neighbor notices the move and propagates a *link failure notification* message (an RREP with infinite metric) to each of its active upstream neighbors to inform them of the erasure of that part of the route. This *notification* is forwarded until the source node is reached. The source node may then choose to reinitiate route discovery.
- Use of *hello* messages optional



Source-initiated On-Demand Routing Protocols

The Dynamic Source Routing (DSR)

- **Route caches** (source routes that mobile is aware, entries updated as new routes learned)
- **Route discovery**: route cache (route to destination known) or route discovery initiated by broadcasting a *route request* packet (address of the destination, source node's address, unique identification number). If node does not have a route to destination, it adds its own address to the *route record* of the packet and then forwards the packet. A *route reply* is generated when the route request reaches the destination. By the time the packet reaches the destination, it contains a route record yielding the sequence of hops taken. If the node generating the route reply is the destination, it places the route record contained in the route request into the route reply.
- **Route maintenance**:
  - *Route error* packets: generated at a node when the data link layer encounters a fatal transmission problem. When a route error packet is received, the hop in error is removed from the node's route cache and all routes containing the hop are truncated at that point.
  - *Acknowledgments*: used to verify the correct operation of the route links.

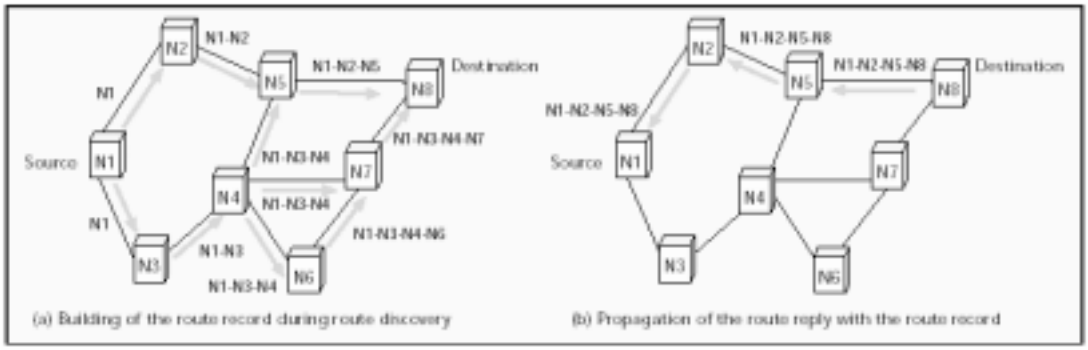


Figure 4. *Creation of the route record in DSR.*

Source-initiated On-Demand Routing Protocols

The Temporally Ordered Routing Algorithm (TORA)

- Link reversal concept, provides multiple routes
- Localization of control messages to a very small set of nodes near the occurrence of a topological change, nodes need to maintain routing information about adjacent (one-hop) nodes.
- Basic functions: Route creation, Route maintenance, Route erasure. During the route creation and maintenance phases, nodes use a "height" metric to establish a directed acyclic graph (DAG) rooted at the destination. Thereafter, links are assigned a direction (upstream or downstream) based on the relative height metric of neighboring nodes. In times of node mobility the DAG route is broken, and route maintenance is necessary to reestablish a DAG rooted at the same destination. Upon failure of the last downstream link, a node generates a new reference level which results in the propagation of that reference level by neighboring nodes, effectively coordinating a structured reaction to the failure. Links are reversed to reflect the change in adapting to the new reference level. This has the same effect as reversing the direction of one or more links when a node has no downstream links.
- Timing important; "height" metric is dependent on the logical time of a link failure, all nodes have synchronized clocks.
- TORA's metric comprises five elements: Logical time of a link failure, unique ID of the node that defined the new reference level, reflection indicator bit, propagation ordering parameter, unique ID of the node. The first three elements collectively represent the reference level. A new reference level is defined each time a node loses its last downstream link due to a link failure. TORA's route erasure phase essentially involves flooding a broadcast *clear packet* (CLR) throughout the network to erase invalid routes.
- Potential for oscillations to occur, especially when multiple sets of coordinating nodes are concurrently detecting partitions, erasing routes, and building new routes based on each other.

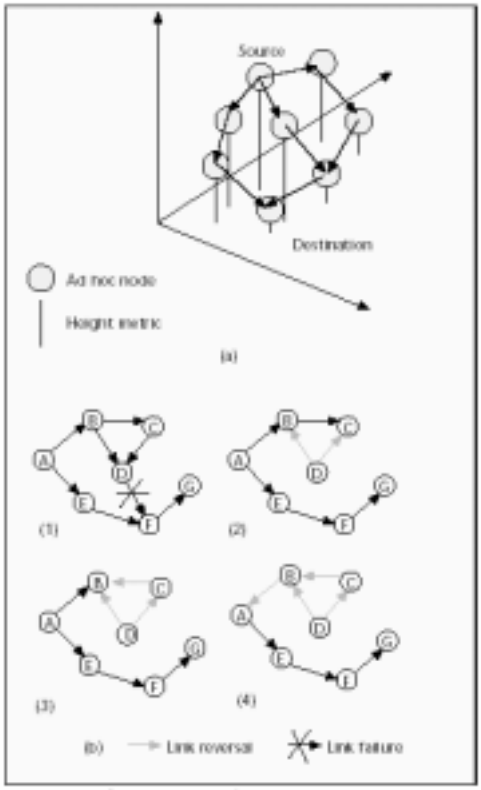


Figure 5. *a) Route creation (showing link direction assignment); b) route maintenance (showing the link reversal phenomenon) in TORA.*

Source-initiated On-Demand Routing Protocols

The Associativity-Based Routing (ABR)

- **'*degree of association stability*'**: connection stability of one node with respect to another node over time and space; basis for route selection. Each node periodically generates a beacon. The associativity tables are updated and the associativity tick of the current node with respect to the beaconing node is incremented by neighboring nodes. Associativity ticks are reset when the neighbors or the node itself move out of proximity.
- The **route discovery** phase: broadcast query and await-reply (BQ-REPLY) cycle. Node broadcasts a BQ message in search of mobiles that have a route to the destination. All nodes receiving the query append their addresses, associativity ticks with their neighbors, and QoS information to the query packet. A successor node erases its upstream node neighbors' associativity tick entries and retains only the entry concerned with itself and its upstream node. In this way, each resultant packet arriving at the destination will contain the associativity ticks of the nodes along the route to the destination. The destination selects the best route by examining the associativity ticks along each of the paths. When multiple paths have the same overall degree of association stability, the route with the minimum number of hops is selected. The destination then sends a REPLY packet back to the source along this path. Nodes propagating the REPLY mark their routes as valid. All other routes remain inactive.
- **Route reconstruction (RRC)**: partial route discovery, invalid route erasure, valid route updates, and new route discovery. Movement by the source results in a new BQ-REPLY process. The RN[1] message is a route notification used to erase the route entries associated with downstream nodes. When the destination moves, the immediate upstream node erases its route and determines if the node is still reachable by a localized query (LQ[*H*]) process, [*H* , hop count from the upstream node to the destination]. If the destination receives the LQ packet, it REPLYs with the best partial route; otherwise, the initiating node times out and the process backtracks to the next upstream node. Here an RN[0] message is sent to the next upstream node to erase the invalid route and inform this node that it should invoke the LQ[*H*] process. If this process results in backtracking more than halfway to the source, the LQ process is discontinued and a new BQ process is initiated at the source.
- **Route deletion** (full broadcast): the source node initiates a route delete (RD) broadcast so that all nodes along the route update their routing tables

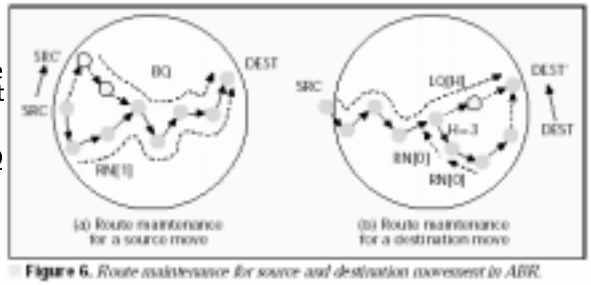


Figure 6. *Route maintenance for source and destination movement in ABR.*

Source-initiated On-Demand Routing Protocols

Signal Stability-Based Adaptive Routing protocol (SSR)

- Selects routes based on the signal strength between nodes and a node's location stability (choosing routes that have "stronger" connectivity).
- Two cooperative protocols: the Dynamic Routing Protocol (DRP) and the Static Routing Protocol (SRP):
  - **DRP** is responsible for the maintenance of the Signal Stability Table (SST) and Routing Table (RT). The SST records the signal strength (strong or weak channel) of neighboring nodes (obtained by periodic beacons from the link layer of each neighboring node). All transmissions are received by and processed in the DRP. After updating table entries, the DRP passes a received packet to the SRP.
  - **SRP** processes packets by passing the packet up the stack if it is the intended receiver or looking up the destination in the RT and then forwarding the packet if it is not. If no entry is found in the RT for the destination, a ***route-search*** process is initiated to find a route. Route requests are propagated throughout the network, but are only forwarded to the next hop if they are received over strong channels and have not been previously processed. The destination chooses the first arriving route-search packet to send back because it is most probable that the packet arrived over the shortest and/or least congested path. The DRP then reverses the selected route and sends a route-reply message back to the initiator. The DRP of the nodes along the path update their RTs accordingly. Route-search packets arriving at the destination have necessarily chosen the path of strongest signal stability, since the packets are dropped at a node if they have arrived over a weak channel. If there is no route-reply message received at the source within a specific timeout period, the source changes the PREF field in the header to indicate that weak channels are acceptable, since these may be the only links over which the packet can be propagated.
- When a failed link is detected within the network, the intermediate nodes send an error message to the source indicating which channel has failed. The source then initiates another route-search process to find a new path to the destination. The source also sends an erase message to notify all nodes of the broken link.

Comparisons: Table-Driven Protocols

Parameters	DSDV	CGSR	WRP
Time complexity (link addition / failure)	O(d)	O(d)	O(h)
Communication complexity (link addition / failure)	O(x=N)	O(x=N)	O(x=N)
Routing philosophy	Flat	Hierarchical	Flat*
Loop-free	Yes	Yes	Yes, but not instantaneous
Multicast capability	No	No**	No
Number of required tables	Two	Two	Four
Frequency of update transmissions	Periodically and as needed	Periodically	Periodically and as needed
Updates transmitted to	Neighbors	Neighbors and cluster head	Neighbors
Utilizes sequence numbers	Yes	Yes	Yes
Utilizes hello messages	Yes	No	Yes
Critical nodes	No	Yes (cluster head)	No
Routing metric	Shortest Path	Shortest Path	Shortest Path

N= Number of nodes in the network, d= Network diameter, h= Height of routing tree, x= Number of nodes affected by a topological change

* While WRP uses flat addressing, it can be used hierarchically.

** The protocol itself currently does not support multicast; however, there is a separate protocol which runs on top of CGSR and provides multicast capability.

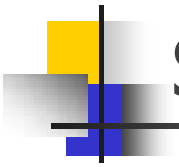
Comparisons: Source-Initiated On-Demand Routing Protocols

Performance Parameters	AODV	DSR	TORA	ABR	SSR
Time complexity (initialization)	O(2d)	O(2d)	O(2d)	O(d+z)	O(d+z)
Time complexity (postfailure)	O(2d)	O(2d) or 0*	O(2d)	O(l+z)	O(l+z)
Communication complexity (initialization)	O(2N)	O(2N)	O(2N)	O(N+y)	O(N+y)
Communication complexity (postfailure)	O(2N)	O(2N)	O(2x)	O(x+y)	O(x+y)
Routing philosophy	Flat	Flat	Flat	Flat	Flat
Loop-free	Yes	Yes	Yes	Yes	Yes
Multicast capability	Yes	No	No**	No	No
Beaconing requirements	No	No	No	Yes	Yes
Multiple route possibilites	No	Yes	Yes	No	No
Routes maintained in	Route table	Route cache	Route table	Route table	Route table
Utilizes route cache/table expiration timers	Yes	No	No	No	No
Route reconfiguration methodology	Erase route; notify source	Erase route; notify source	Link reversal; route repair	Localized broadcast query	Erase route; notify source
Routing metric	Freshest and shortest path	Shortest path	Shortest path	Associativity and shortest path and others***	Associativity and stability

l= Diameter of the affected network segment
y= Total number of nodes forming the directed path where the REPLY packets transits
z= Diameter of the directed path where the REPLY packet transits
* Cache hit
** Like CGSR, TORA also does not support multicast; however, there is a separate protocol LAM which runs on top of ORA and provides multicast capability
*** ABR also uses the route relaying load and cumulative forwarding delay as routing metrics

Comparisons: Table-Driven vs. On-Demand Routing

Parameters	On-Demand	Table-Driven
Availability of routing information	Available when needed	Always available regardless of need
Routing philosophy	Flat	Mostly flat, except for CGSR
Periodic route updates	Not required	Required
Coping with mobility	Use localized route discovery as in ABR and SSR	Inform other nodes to achieve a consistent routing table
Signaling traffic generated	Grows with increasing mobility of active routes (as in ABR)	Greater than that of on-demand routing
Quality of service support	Few can support QoS, although most support shortest path	Mainly shortest path as the QoS metric

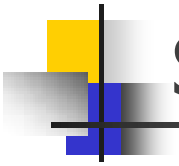


Security

Mobile ad hoc network (MANET) is dependent on maintaining appropriate routing information. No security is considered in currently proposed routing protocols, which makes the routing protocol an easy target for attackers. The existing security solutions for wired networks cannot be applied directly in wireless MANETs. Wireless MANET presents a larger security problem than conventional wired and wireless networks:

- all signals go through bandwidth-constrained wireless links in a MANET, which makes it more prone to physical security threats than fixed landline networks.
- mobile nodes are roaming independently and are able to move in any direction. Therefore, any security solution with a static configuration would not be adequate for the dynamically changing topology.
- decentralized decision making in the MANET relies on the cooperative participation of all nodes. The malicious node could simply block or modify the traffic traversing it by refusing cooperation to break the cooperative algorithms.
- some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. An attacker could create a new type of DoS attack by forcing a node to replay packets to exhaust its energy.

⇨ **the wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, absence of central authorities, distributed cooperation, and constrained capability**

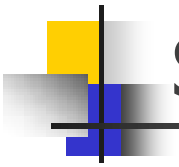


Security

Three main routing protocols for a MANET: DSDV, AODV, DSR.

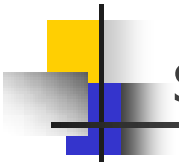
Types of attacks that can easily be performed against a MANET:

- A **passive attack** does not disrupt the operation of a routing protocol, but only attempts to discover valuable information by listening to routing traffic, which makes it very difficult to detect.
- An **active attack** is an attempt to improperly modify data, gain authentication, or procure authorization by inserting false packets into the data stream or modifying packets transition through the network.
  - An ***external attack*** is one caused by nodes that do not belong to the network.
  - An ***internal attack*** is one from compromised or hijacked nodes that belong to the network.



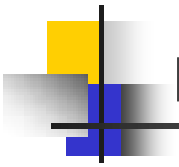
Security

Types of active attacks against a MANET in the network layer:
Black hole: In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept.
Denial of service: The DoS attack results when the network bandwidth is hijacked by a malicious node. It has many forms: the classic way is to flood any centralized resource so that the network no longer operates correctly or crashes. For instance, a route request is generated whenever a node has to send data to a particular destination. A malicious node might generate frequent unnecessary route requests to make the network resources unavailable to other nodes.
Routing table overflow: The attacker attempts to create routes to nonexistent nodes. The goal is to have enough routes so that creation of new routes is prevented or the implementation of routing protocol is overwhelmed.
Impersonation: A malicious node may impersonate another node while sending the control packets to create an anomaly update in the routing table.
Energy consummation: Energy is a critical parameter in the MANET. Battery-powered devices try to conserve energy by transmitting only when absolutely necessary. An attacker can attempt to consume batteries by requesting routes or forwarding unnecessary packets to a node.
Information disclosure: The malicious node may leak confidential information to unauthorized users in the network, such as routing or location information. In the end, the attacker knows which nodes are situated on the target route.



SUMMARY

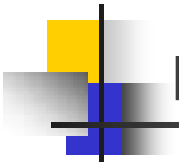
- Commercial scenarios for ad hoc wireless networks include: Conferences/meetings/lectures, Emergency services, Law enforcement
- While it is not clear that any particular algorithm or class of algorithm is the best for all scenarios, each protocol has definite advantages and disadvantages, and is well suited for certain situations.
- Current ad hoc routing approaches have introduced several new paradigms, such as exploiting user demand, and the use of location, power, and association parameters. Adaptivity and self-configuration are key features of these approaches. However, flexibility is also important. A flexible ad hoc routing protocol could responsively invoke table-driven and/or on-demand approaches based on situations and communication requirements. The "toggle" between these two approaches may not be trivial since concerned nodes must be "in sync" with the toggling. Coexistence of both approaches may also exist in spatially clustered ad hoc groups, with intracluster employing the table-driven approach and intercluster employing the demand-driven approach or vice versa. Further work is necessary to investigate the feasibility and performance of *hybrid ad hoc* routing approaches.
- Further research in the areas of media access control, security, service discovery, and Internet protocol operability is required before the potential of ad hoc mobile networking can be realized. A wireless MANET presents a greater security problem than conventional wired and wireless networks due to its fundamental characteristics of open medium, dynamic topology, absence of central authorities, distributed cooperation, and constrained capability. Routing security plays an important role in the security of the entire network. In general, routing security in wireless networks appears to be a nontrivial problem that cannot easily be solved. It is impossible to find a general idea that can work efficiently against all kinds of attacks, since every attack has its own distinct characteristics.
- Other current challenges for ad hoc wireless networks include: Multicast, QoS support, Power-aware routing, Location-aided routing
- The field of ad hoc mobile networks is rapidly growing and changing, and while there are still many challenges that need to be met, it is likely that such networks will see widespread use within the next few years.



References

A review of current routing protocols for ad hoc mobile wireless networks
Royer, E.M.; Chai-Keong Toh; Personal Communications, IEEE , Volume: 6 , Issue: 2 , April 1999 Pages:46 - 55. [1]

Routing security in wireless ad hoc networks
Hongmei Deng; Wei Li; Agrawal, D.P.; Communications Magazine, IEEE , Volume: 40 , Issue: 10 , Oct. 2002 Pages:70 – 75. [2]



Homework

Describe the Black Hole Problem in the AODV protocol and present a feasible solution to the problem
(see reference [2]).