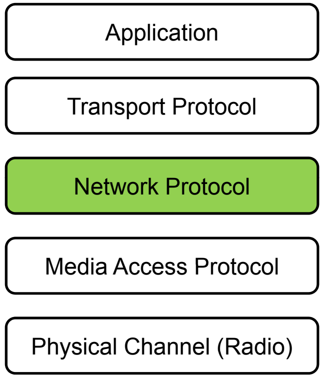
TELEMATICS GROUP

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

Wireless Ad Hoc & Sensor Networks

Routing Protocols



WS 2009/2010

Prof. Dr. Dieter Hogrefe/Prof. Dr. Xiaoming Fu
Dr. Omar Alfandi

TELEMATICS GROUP

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

Outline

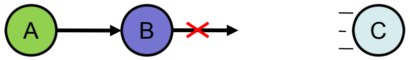
- Issues in Designing Routing Protocols
- Classification of Routing Protocols
  - Proactive Routing Protocols
  - Reactive Routing Protocols
  - Hybrid Routing Protocols
- Summary

TELEMATICS GROUP

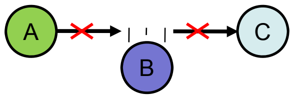
GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

Mobility

- Dynamic network topology
- Session disruption by Movement
  - End node movement



  - Intermediate nodes in path movement



- Classic wired protocols do not consider node mobility

TELEMATICS GROUP

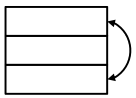
GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

Bandwidth Constraint

- Wired: Fiber + WDM → abundant bandwidth
- Wireless: Limited radio band → low bandwidth
- Keeping routing overhead low, is key.
- Complete topology information not suitable for AdHoc wireless.

Error-Prone Shared Broadcast Radio Channel

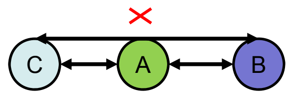
- Link capacity varies
- Link-error probability varies
- MAC layer interaction necessary (Cross Layer)
  - Using better-quality links for route determination



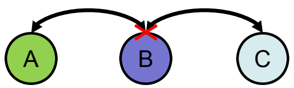
- **Broadcast nature is a challenge**
  - Packet collision → Terminal Problems

Repetition: Problems with CSMA/CA

- Want to know state of channel at receiver, not transmitter
- But wireless is not transitive!
  - A hears B
  - A hears C
  - B and C may not hear each other
  - B and C can only sense their channel, but need to know if A's channel is clear



Repetition: Hidden Terminal Problem



- A and C can't hear each other, B can hear both
- A and C sense a clear channel, transmit, and collide at B
- A is a *hidden terminal* to C, and C is *a hidden terminal* to A

Repetition: Exposed Terminal Problem

- A transmits to B
- C hears the transmission, backs off, even if it wants to transmit to D
- C is an exposed terminal to A's transmission

Resource Constraints

- **Limitations for mobile nodes**
  - Battery life (1500 mAh mobile; 35 Ah portable)
  - Processing power (2 MIPS RISC mobile; 20MIPS CISC portable)
  - Weight constraints (150g mobile; 2500g portable)
  - Size constraints (100 cm^3 mobile; 2000 cm^3 portable)
- **Routing protocol needs to adress**
  - Energy effcienct route detection
  - Processing effort minimization

TELEMATICS GROUP
GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

Ideal AdHoc Routing Protocol

- 1. Fully distributed, no central control node
  - Lower control overhead, increased scalability
- 2. Adaptive to frequent topology changes (mobility)
- 3. Route computation: Minimal node involvement
  - Quick access to routes for each node
  - Minimum connection set up time
- 4. Localization of route discovery/maintenance
  - No global state maintenance -> high control overhead

TELEMATICS GROUP
GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

Ideal AdHoc Routing Protocol (2)

- 5. Loop free/stale route free routes
- 6. Minimal packet collisions
  - Reduced broadcasts by each node
- 7. Convergence to optimal routes
  - In case topology becomes stable
  - Quick convergence
- 8. Low resource comsumption
  - Bandwidth, cpu/ram, energy
- 9. Local topology updates only
- 10. QoS support as demanded by applications

TELEMATICS GROUP
GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

Outline

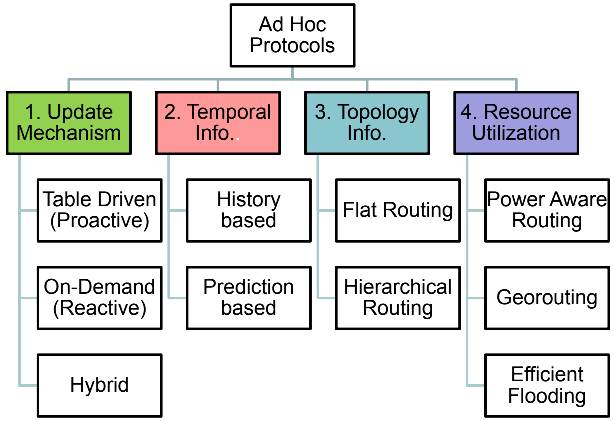
- Issues in Designing Routing Protocols
- Classification of Routing Protocols
  - Proactive Routing Protocols
  - Reactive Routing Protocols
  - Hybrid Routing Protocols
- Summary

Classification

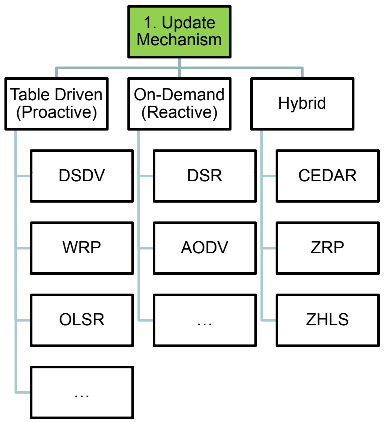
- 4 categories based on
  1. Update mechanism (routing table)
  2. Temporal information
  3. Topology information
  4. Resource utilization

- Path finding processes and routing metrics deviate from traditional wired protocols
- Some protocols fall in more than one class

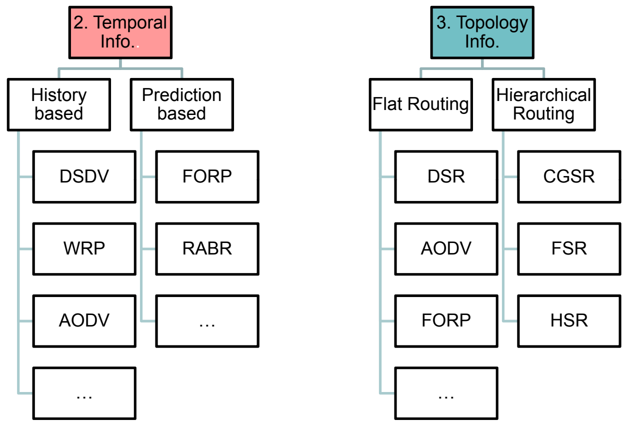
Classification



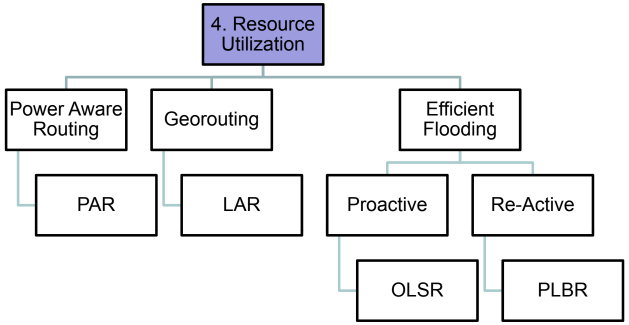
Classification



Classification



Classification

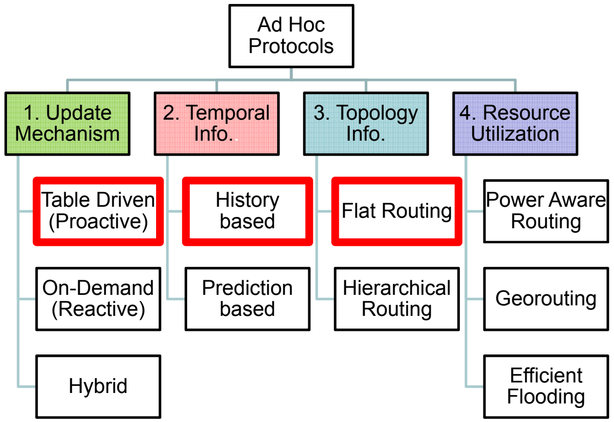


Outline

- Issues in Designing Routing Protocols
- Classification of Routing Protocols
  - Proactive Routing Protocols
  - Reactive Routing Protocols
  - Hybrid Routing Protocols
- Summary

Proactive routing protocols: DSDV

Destination **S**ecuenced **D**istance **V**ector Routing



DSDV: Routing Updates

- Routes to all destinations are readily available at every node's routing table at all times
- Each routing table entry at every given node maintains:

  <dest-addr, dest-seq#, next-hop, hop-count>
- Seq#s (created by destinations) are used to distinguish stale routes and avoid formation of route loops.
- The tables are exchanged between neighbours at regular intervals to keep an up-to-date view of the network topology (can happen time-based and event-based)

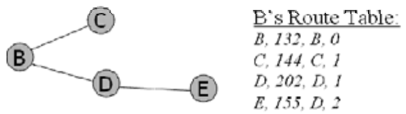
DSDV: Routing Updates

- Each node sends a periodic update to its neighbors
  - The update contains its own dest-seq# and other routing information for the destination
    < dest-addr, dest-seq#, hop-count >
- Also each node sends routing table updates caused by important changes in the local topology (e.g. link failure)
- When a node receives two routes to the same destination from two neighbors it would:
  - Choose the route with the largest sequence number
  - If the same: Choose the smalest hop-count

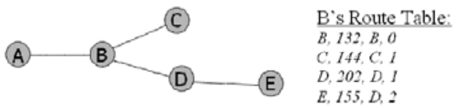
DSDV: Full/Incremental Updates

- Full updates
  - The full routing table is included inside the update
  - Relatively are rare
- Incremental updates
  - Contain only those entries with metrics that have been changed scince the last update was sent
  - Usually fits in one packet, otherwise a full update would be sent

DSDV: Adding a link

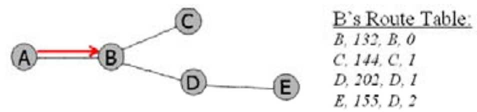


1. An ad hoc network

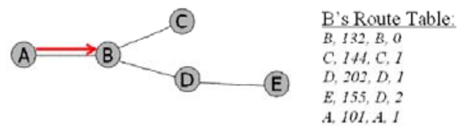


2. Node A is added to the network

DSDV: Adding a link

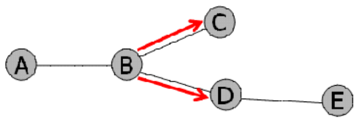


3. Node A sends its routing table to its neighbors
<A, 101, 0>



4. Node B receives the information and adds
<A, 101, 1> to its own routing table

DSDV: Adding a link

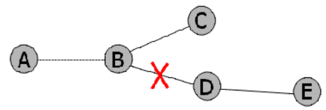


B's Route Table:
B, 132, B, 0
C, 144, C, 1
D, 202, D, 1
E, 155, D, 2
A, 101, A, 1

5. Node B propagates the new routing information to its neighbors <A, 101, 1>
6. The neighbors complement their routing tables

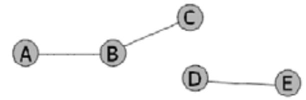
<A, 101, B, 2> and propagate their information to their neighbors

DSDV: Failure of a link



B's Route Table:
B, 132, B, 0
C, 144, C, 1
D, 202, D, 1
E, 155, D, 2
A, 101, A, 1

1. A link between B and D fails

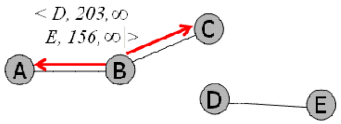


B's Route Table:
B, 132, B, 0
C, 144, C, 1
D, 203, D, ∞
E, 156, D, ∞
A, 101, A, 1

2. Node B notices the failure:

- Sets hop-counts for D and E on ∞
- increment seq# for D and E

DSDV: Failure of a link



B's Route Table:
B, 132, B, 0
C, 144, C, 1
D, 203, D, ∞
E, 156, D, ∞
A, 101, A, 1

3. Node B sends new routing information to its neighbors

DSDV Advantages:

- The availability of routes to all destinations at all times implies that much less delay is involved in the route setup process.

DSDV Disadvantages:

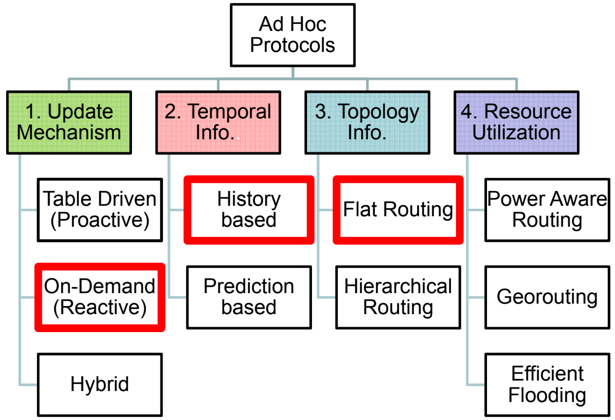
- The updates due to broken links lead to a heavy control overhead during high mobility. Proactive protocols work best in networks with low or moderate mobility and a few nodes
- in order to obtain information about a particular destination node, a node has to wait for a table update message initiated by the same destination node

Outline

- Issues in Designing Routing Protocols
- Classification of Routing Protocols
  - Proactive Routing Protocols
  - Reactive Routing Protocols
  - Hybrid Routing Protocols
- Summary

Reactive routing protocols: AODV

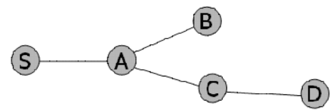
Ad Hoc **O**n demand **D**istance **V**ector routing



AODV

- Managing only active routes
- Every node maintains two counters: node seq#, node broadcast-ID
- It employs destination seq#s to identify the most recent path
- Nodes keep track of their neighbors listening to HELLO messages that each node broadcasts at set intervals.
- All intermediate nodes having valid routes to the destination, or the destination node itself, are allowed to send *RouteReply packets to the* source.

AODV: Route Discovery



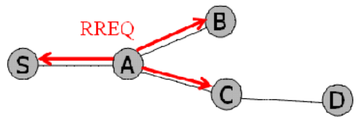
1. Node S needs to find a route to D
2. S initiates a Route Request (RREQ) message

<D‘s-IP-addr., D‘s-Seq#, S‘s-IP-addr., S‘s-Seq#, hop-count(=0)>

The pair <S‘s-IP-addr., S‘s-Seq#> is the RREQ unique identifier helping the nodes droping duplicate RREQs.

3. S sends the RREQ message to its neighbors

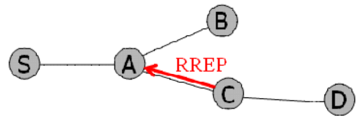
AODV: Route Discovery



4. Node A receives RREQ
- makes route reverse entry for
  Des=S, nexthop=S, hopcount=1
- A has no direct route to D, So sends RREQ to its neighbors

5. Node C receives the RREQ
- makes route reverse entry for S
  Des=S, nexthop=A, hopcount=2
- C has a direct route to D, and the seq# for route to D is S's seq# in RREQ

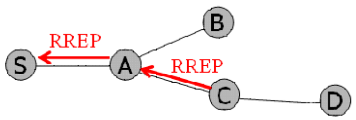
AODV: Route Discovery



6. Node C receives RREQ
- C initiates a route reply (RREP)

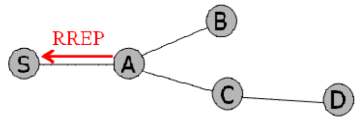
RREP=<D's_IP_addr, D's-seq#, S's_IP_addr, hopcount_to_D(=1)>
- C sends the RREP to A

AODV: Route Discovery



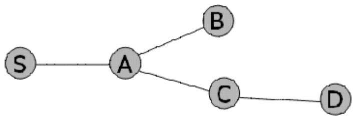
7. Node A receives RREP
- A makes a route forward entry for D
  Dest=D, nexthop=C, hopcount=2
- A sends RREP to S

AODV: Route Discovery



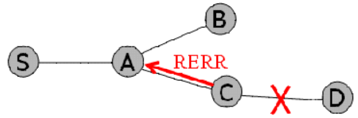
8. Node S receives RREP
- S makes a route forward entry for D
  Dest=D, nexthop=A, hopcount=3

AODV: Route Discovery



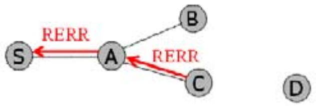
9. Node S receives RREP
- S makes a forward entry route for D
  Dest=D, nexthop=A, hopcount=3
- S sends the data packets on the new route to D

AODV: Route Management

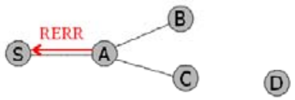


1. The route between C and D fails
2. Node C invalidates the route to D in its routing table
3. Node C generates Route Error message (RERR)
- Lists all of the destinations which are not accessible now
- Sends RERR to the upstream neighbor

AODV: Route Management



4. Node A receives RERR message
- Checks whether C is the next hop on the route to D
- Deletes the route to D
- RERR broadcast continues to S



5. Node S receives RERR message
- Examines if A is the next hop on the route to D
- Deletes the route to D
- Finds a new route to D if necessary

AODV Advantages:

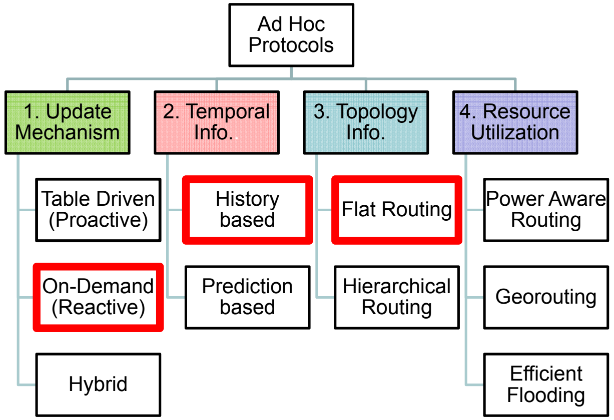
- routes are established on demand and destination sequence numbers are used to find the latest route to the destination

AODV Disadvantages:

- multiple RouteReply packets in response to a single RouteRequest packet can lead to heavy control overhead
- the periodic *beaconing* leads to unnecessary bandwidth consumption

Reactive routing protocols: DSR

Dynamic Source Routing

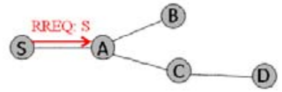


DSR: Route Discovery

DSR Route Discovery:

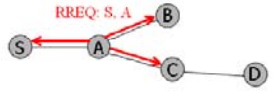
Node S needs a route to D

1. S sends RREQ message



2. A receives the message, but it has no route to D

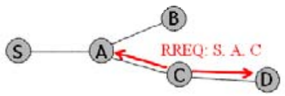
- A adds its own address and sends the message to its neighbors



3. C receives RREQ message, but has no route to D

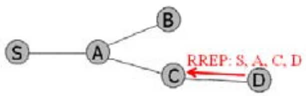
- adds its own address and sends the packet to its neighbors

DSR: Route Discovery



4. Node C receives RREQ message, but has no route to D

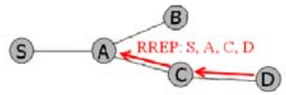
- adds its own address and sends the packet to its neighbors



5. Node D receives RREQ and sends a RREP back to C

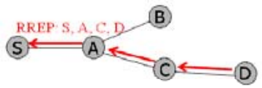
- The RREP contains the route from S to D

DSR: Route Discovery



6. Node C receives RREP

- RREP is broadcasted continuesly to A



7. Node A receives the RREP message

- sends RREP to S

8. Node S receives the RREP message

- S will use the discovered route to forward data

- DSR nodes may learn more than one route during route discovery

DSR Advantages:

- A route is established only when it is required
- The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead.

DSR Disadvantages:

- The route maintenance mechanism does not locally repair a broken link.
- The connection setup delay is higher than in table-driven protocols.
- Considerable routing overhead is involved due to the source-routing mechanism. This routing overhead is directly proportional to the path length.

AODV and DSR differences:

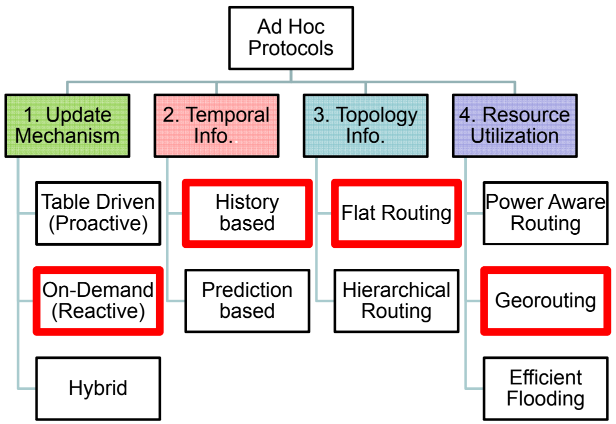
- DSR uses sourse routing in which a data packet carries the complete path to be traversed, but AODV uses next hop record in which the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission.
- DSR route uses cashe, AODV uses routing table
- DSR route cash entries have no lifetimes

  AODV routing table entries have lifetimes
- DSR has alternate route available when one breaks

  AODV nodes do not alternate route when one breaks

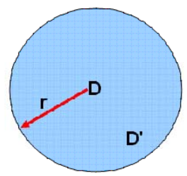
Reactive routing protocols: LAR

Location **A**ided **R**outing



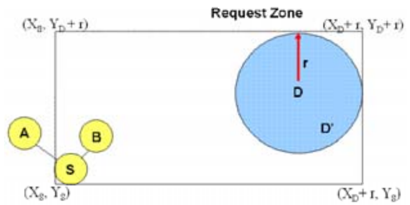
LAR

- A location based reactive routing protocol
  - Location information of the nodes is used (e.g. Obtained from GPS)
  - All nodes should know their current location
- **Expected Zone:** The area that probably contains the desired destination
  - EZ is estimated based on any previous location information and the destination‘s velocity
- D= last known location of node D at time t0
- D‘= location of node D at present time t1
  - D‘ is unknown to the sender
- r=(t1- t0)*Vd
- Vd= estimated speed of D



LAR: Request Zone

- Request Zone contains the expected zone and the location of the sender and the RREQ is limited in that
  - Only nodes within the request zone forward the RREQ
- Request zone explicitly is specified in RREQ
- Each node must know its location to determine whether it is within the request zone or not



LAR: Request Zone

- If route discovery with the smallest request zone fails, the sender would try to discover the route with a larger request zone (after a time out)
  - The larger zone can cover the entire network
- The rest of the route discovery is similar to DSR

LAR: Advantages and Disadvantages

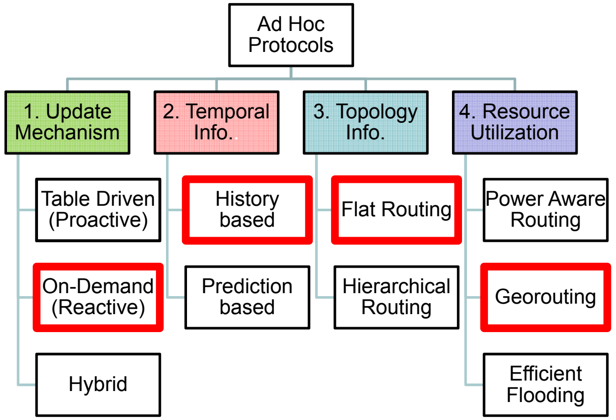
- **Advantages**
  - reduced RREQ flood (only in the request zone)
  - reduced route discovery overhead
- **Disadvantages**
  - Nodes need to know their locations
  - The possible existence of obstructions for radio transmissions is not taken into account

Outline

- Issues in Designing Routing Protocols
- Classification of Routing Protocols
  - Proactive Routing Protocols
  - Reactive Routing Protocols
  - Hybrid Routing Protocols
- Summary

Hybrid routing protocols: ZRP

Zone **R**outing **P**rotocol



TELEMATICS GROUP
GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

ZRP: Zone Routing Protocol

- Combining the advantages of both reactive and proactive approaches
- Each node maintains an up-to-date map of a zone centered at every node (r-hops)
- Within a zone the routes are immidiately available (*intra-zone routing protocol)*
- For destinations out of the zone a reactive route discovery protocol is used (*inter-zone routing protocol*)
- In MANETs it can be assumed that the most traffic is directed to nearby nodes, so ZRP reduces the proactive scope to a limited zone

TELEMATICS GROUP
GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

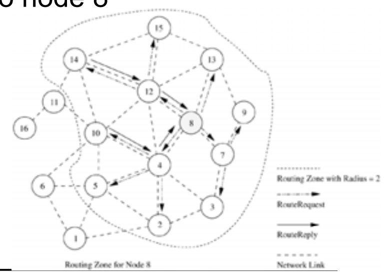
ZRP: Route Discovery

- The larger the routing zone, the higher the update control traffic
- When a node s needs a route to a destination d, it checks whether node d is within its zone
- If so, it delivers the packet directly. Otherwise, node s directly routes the RREQ to the border nodes to its peripheral nodes
- If any peripheral node finds node d to be located within its routing zone, it sends a RREP back to s; otherwise, the node rebordercasts the RREQ packet to the peripheral nodes.
- This process continues until node d is located.

TELEMATICS GROUP
GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

ZRP: Route Discovery

- In the figure node 8 needs a route to node 16 node
- node 8 bordercasts RouteRequests to nodes 2, 3, 5, 7, 9, 10, 13, 14 and 15
- Nodes 10 and 14 find the information about node 16 to be available in their intrazone routing tables, and hence they originate RouteReply packets back to node 8
- During RouteRequest propagation, every node that forwards the RREQ appends its address to it.
- This information is used for delivering the RREP packet back to the source.



ZRP: Route Discovery

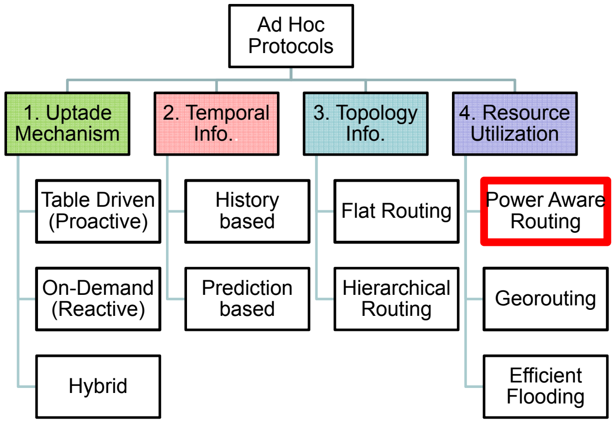
- When an intermediate node in an active path detects a broken link in the path, it performs
- A local path reconfiguration in which the broken link is bypassed by means of a short alternate path connecting the ends of the broken link.
- A path update message is then sent to the sender node to inform it about the change in path.

ZRP: Advantages and Disadvantages

- ZRP reduces the control overhead compared to the RREQ flooding mechanism employed in on demand approaches and the periodic flooding of routing information packets in table driven approaches.
- But in the absence of a query control, ZRP tends to produce higher control overhead than the aforementioned schemes. This can happen due to the large overlapping of nodes' routing zones. The query control must ensure that redundant or duplicate RREQs are not forwarded. Also, the decision on the zone radius has a significant impact on the performance of the protocol.

Power Aware Routing Protocols

Coming Lecture



Outline

- Issues in Designing Routing Protocols
- Classification of Routing Protocols
  - Proactive Routing Protocols
  - Reactive Routing Protocols
  - Hybrid Routing Protocols
- Summary

Summary

- Major Issues in Designing of Ad Hoc Routing Protocol
  - Mobility of nodes
  - Rapid topology changes
  - Limited bandwidth
  - Hidden/exposed terminal problem
  - Limited battery capacity
  - Time-varying channel properties
  - Location dependent contention

Summary

- Classification of protocols
  - Topology maintenance approach
  - Routing topology used
  - Use of temporal information
  - Consideration of Resource utilization