MAC Protocol for Ad hoc Wireless Networks

Aim of MAC:

- provide fair access to shared broadcast radio channel.

Issues to deal with:

- Bandwidth efficiency: – must be maximized.

The radio spectrum is limited, the bandwidth available for communication is also very limited. The MAC protocol must be designed in such a way that the scarce bandwidth is utilized in an efficient manner. The control overhead involved must be kept as minimal as possible.

Bandwidth efficiency=ratio of the bandwidth used/ Total Bandwidth

- Real-time traffic support: – should be provided.

- QoS support to data sessions in such networks is very difficult. Bandwidth reservation made at one point of time may become invalid once the node moves out of the region where the reservation was made.
- QoS support is essential for supporting time-critical traffic sessions such as in military communications.
- The MAC protocol for ad hoc wireless networks that are to be used in such real-time applications must have some kind of a resource reservation mechanism

- Synchronization: – sometimes needed, e.g. TDMA.
  - Exchange of control packets may be required for achieving time synchronization among nodes. Very important for bandwidth (time slot) reservations by nodes.

- Shared broadcast medium: – collisions must be avoided/minimized.
  - A node should get access to the shared medium only when its transmissions do not affect any ongoing session.
  - Since multiple nodes may contend for the channel simultaneously, the possibility of packet collisions is quite high in wireless networks.
  - A MAC protocol should grant channel access to nodes in such a manner that collisions are minimized

- Lack of central coordination: – fully distributed MAC design.
  - Nodes must be scheduled in a distributed fashion for gaining access to the channel.
  - The MAC protocol must make sure that the additional overhead, in terms of bandwidth consumption, incurred due to this control information exchange is not very high.

MAC Protocol for Ad hoc Wireless Networks

- Mobility of nodes: – loss of connectivity; – network partitioning; – bit errors.
- The protocol design must take this mobility factor into consideration so that the performance of the system is not significantly affected due to node mobility.

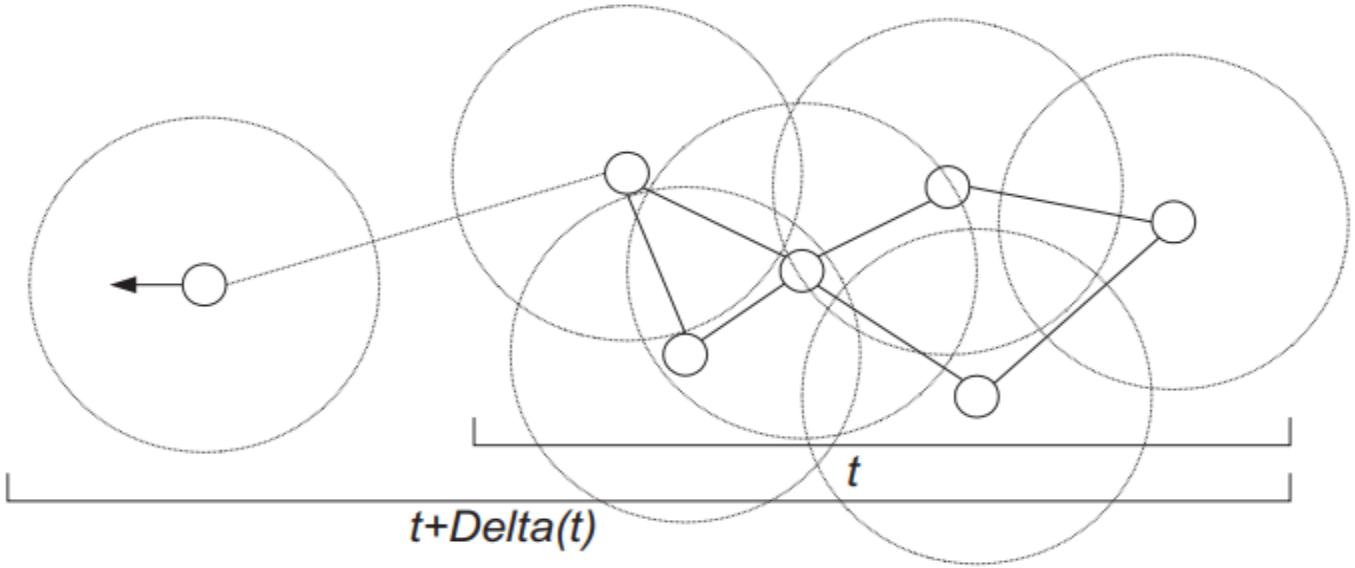


Figure 3: Network partitioning is one of the biggest problem to deal with at MAC sublayer.

MAC Protocol for Ad hoc Wireless Networks

- Hidden terminal problem: – collisions → inefficient bandwidth utilization.

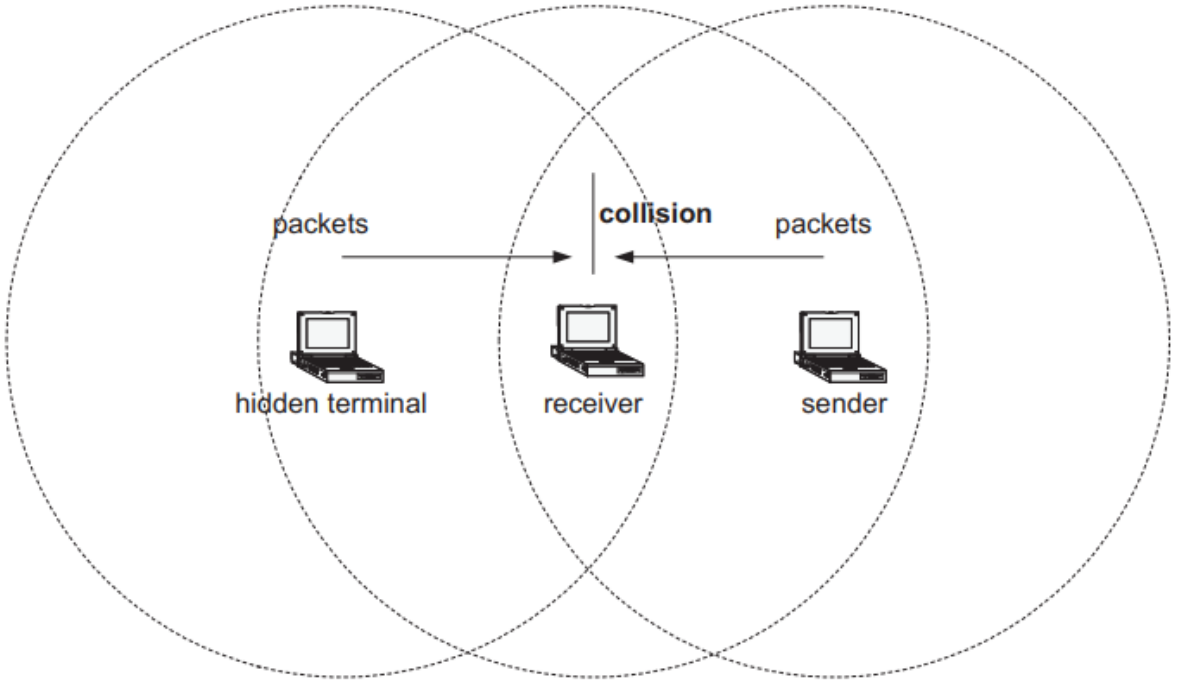


Figure 1: Illustration of the hidden terminal problems.

MAC Protocol for Ad hoc Wireless Networks

- Exposed terminal problem: – inability to transmit → inefficient bandwidth utilization.

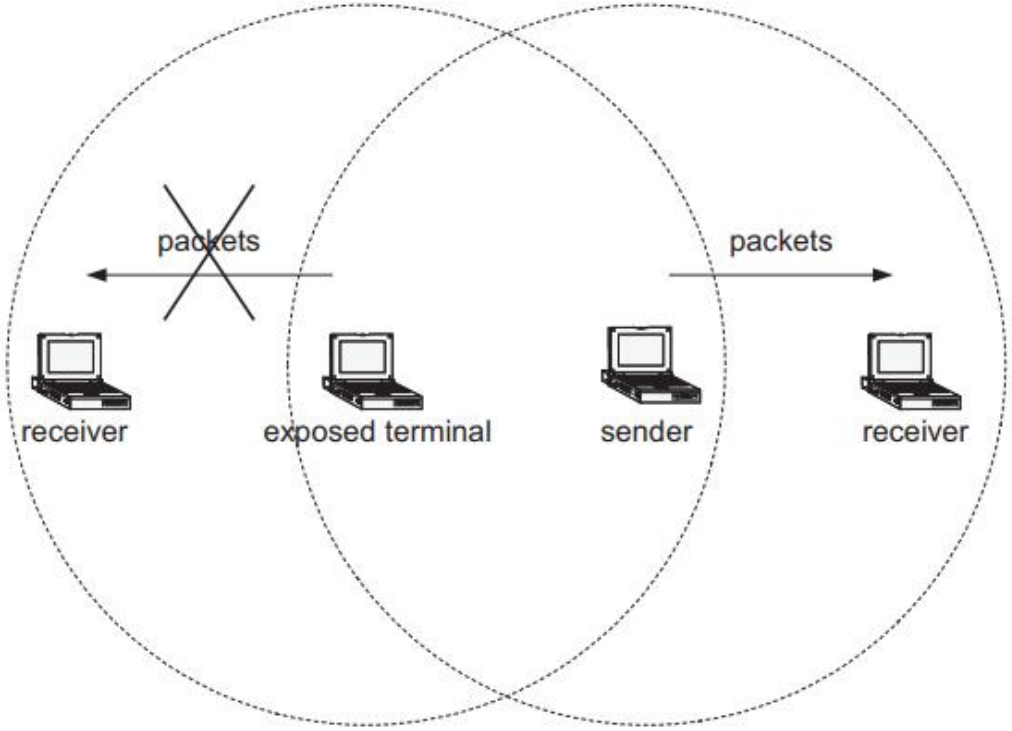


Figure 2: Illustration of the exposed terminal problem.

MAC Protocol for Ad hoc Wireless Networks

Design goals-What we want from MAC protocol?

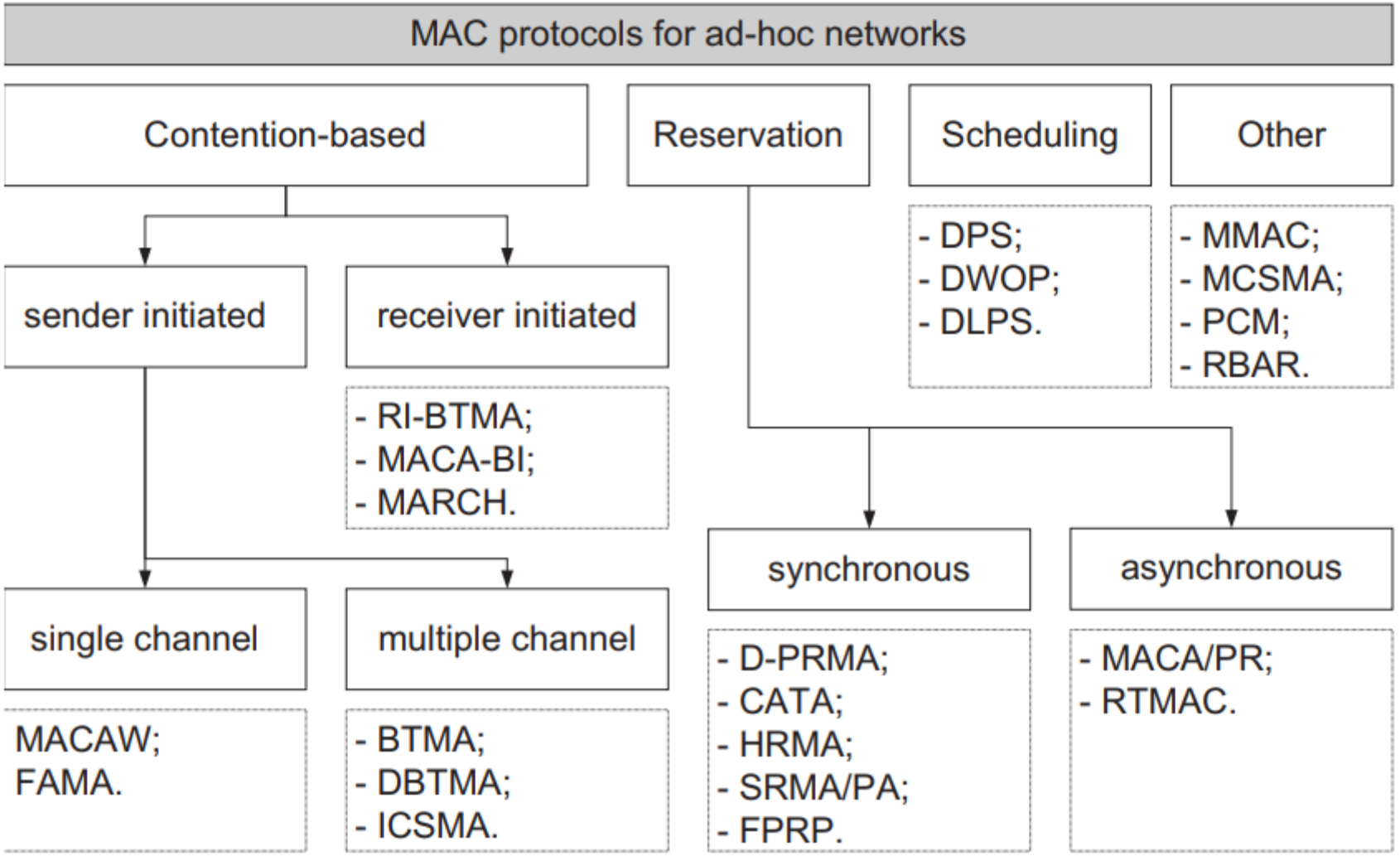
- allow fair access to the shared radio medium;
- operation of the protocol should be distributed;
- should support real-time traffic;
- the access delay must be minimized;
- available bandwidth must be utilized efficiently;
- fair bandwidth allocation to competing nodes;
- control overhead must be minimized;
- the effects of hidden/exposed terminals must be minimized;
- must be scalable;
- should minimize power consumption;
- should provide synchronization between nodes.

MAC Protocol for Ad hoc Wireless Networks

Classification of MAC protocols

- Contention-based protocols without reservation/scheduling:
  - no reservation of the bandwidth is made;
  - guarantees are not possible.
- Contention-based protocols with reservation mechanisms:
  - bandwidth for transmission is reserved in advance.
  - guarantees are possible.
- Contention-based protocols with scheduling mechanisms:
  - distributed scheduling between nodes is used.
  - guarantees are possible.
- Protocols that do not fall to any of these categories:
  - implement several features of different protocol groups or
  - use completely different approach

MAC Protocol for Ad hoc Wireless Networks



MACA

- Contention based protocols w/o reservation/scheduling
  - The basic idea: contention for the resource, winning node transmits.
- **Multiple access collision avoidance (MACA) protocol (Extension of CSMA):**
- **CSMA operates as follows:**
  - the sender sense the channel for the carrier signal;
  - if the carrier is present it retries to sense the channel after some time (exp. back-off);
  - if not, the sender transmits a packet.
- The following shortcomings are inherent to CSMA/CA:
  - hidden terminal problem leading to frequent collisions;
  - exposed terminal problem leading to worse bandwidth utilization.
- To avoid it:
  - virtual carrier sensing;
  - RTS-CTS handshake before transmission.

MACA

- MACA does not make use of carrier-sensing for channel access.
- Two additional signaling packets: the request-to-send (RTS) packet and the clear-to-send (CTS) packet are used.
- When a node has data to transmit, it first transmits an RTS packet.
- The receiver node, on receiving the RTS packet, if it is ready to receive the data packet, transmits a CTS packet.
- Once the sender receives the CTS packet without any error, it starts transmitting the data packet.

MACA

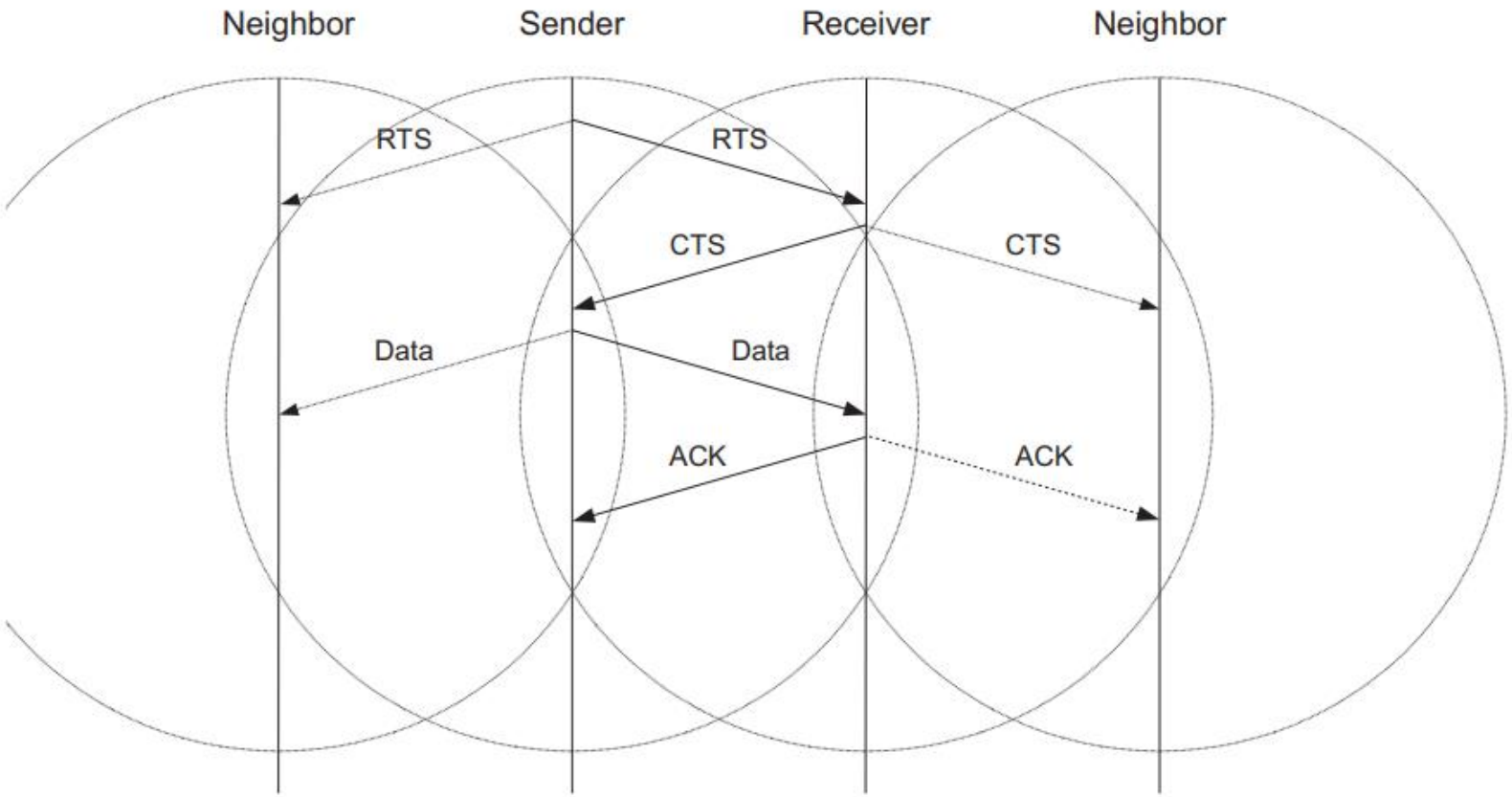


Figure 4: Packet transmission in MACA.

MACA

- If the transmission fails in MACA:
- The node uses the binary exponential back-off (BEB) algorithm
- In the binary exponential backoff mechanism, each time a collision is detected, the node doubles its maximum back-off window.
  - contention window: CW×2;
  - retransmission of RTS.

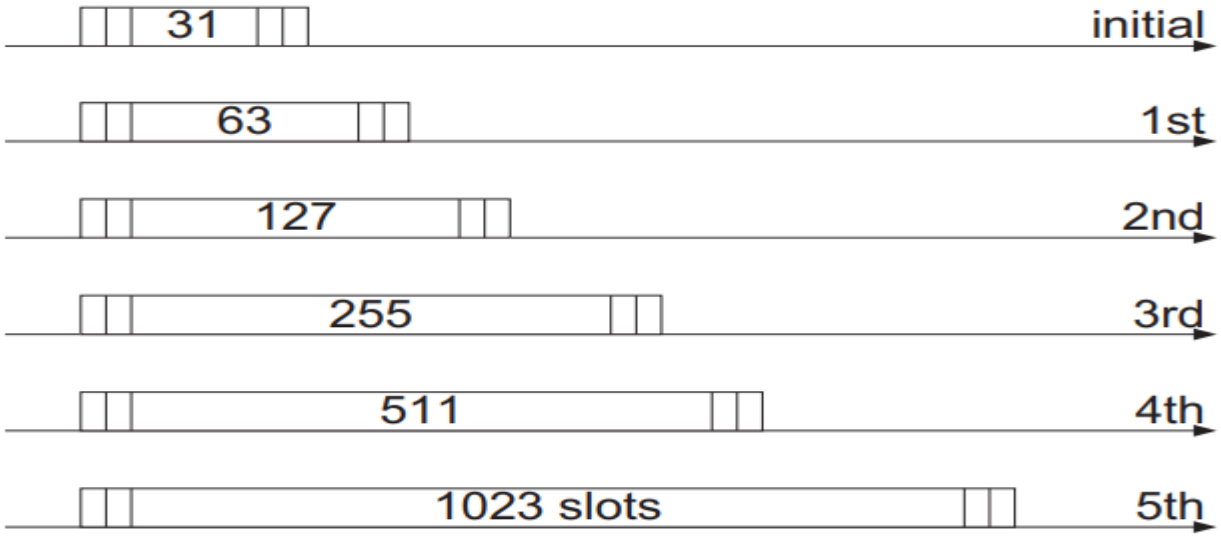


Figure 6: Evolution of the contention window with increasing of transmission attempts.

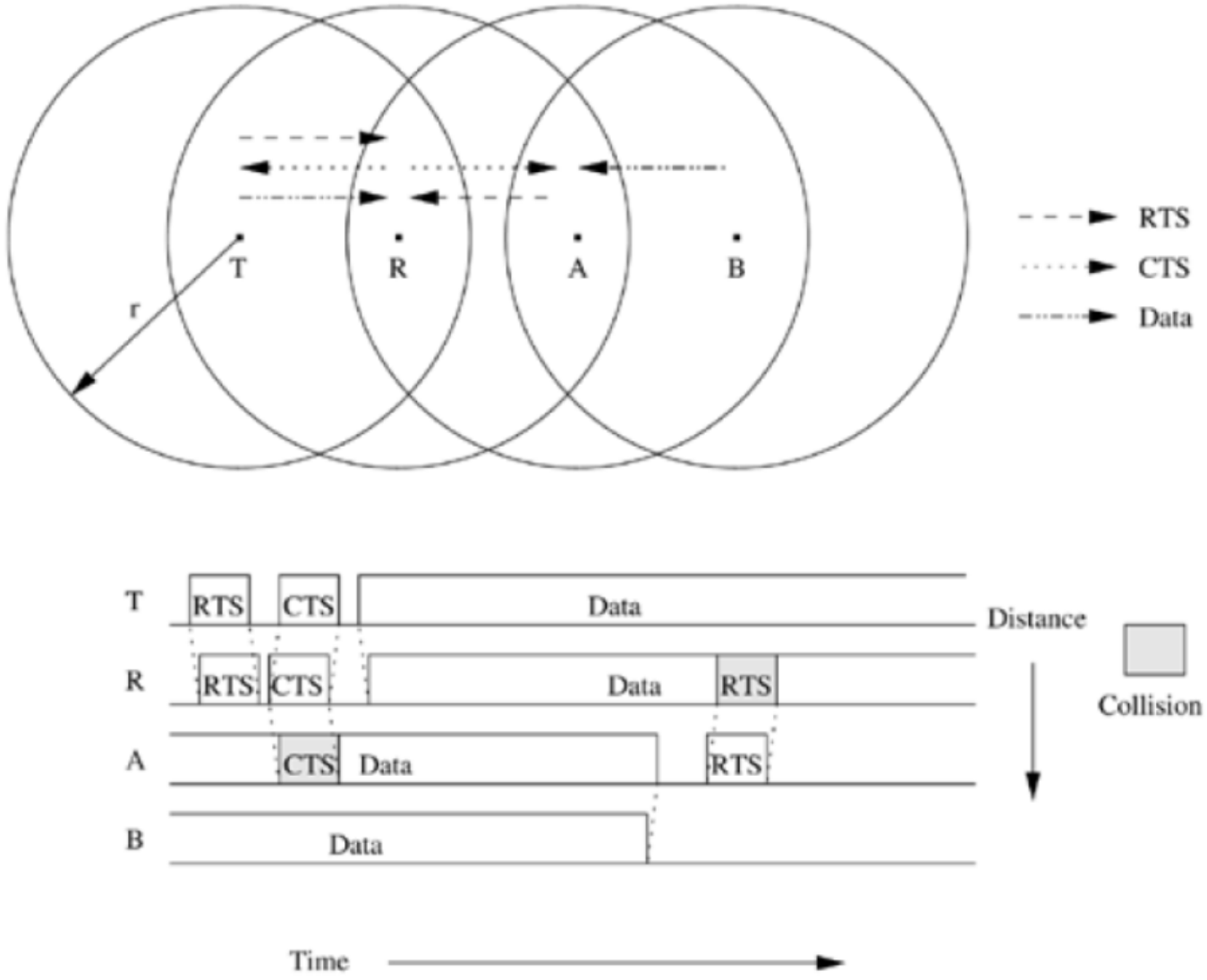
Solving Hidden and Exposed Terminal

- Both the RTS and the CTS packets carry the expected duration of the data packet transmission.
- Neighbor nodes near the sender that hear the RTS packet do not transmit for a long enough period of time so that the sender could receive the CTS packet.
- A node near the receiver, upon hearing the CTS packet, defers its transmission till the receiver receives the data packet. **Thus, MACA overcomes the hidden node**
- Similarly, a node receiving an RTS defers only for a short period of time till the sender could receive the CTS. If no CTS is heard by the node during its waiting period, it is free to transmit packets once the waiting interval is over.
- Thus, a node that hears only the RTS packet is free to transmit simultaneously when the sender of the RTS is transmitting data packets. Hence,
- Thus, the **exposed terminal problem is also overcome in MACA.**
- But MACA still has certain problems, which was why MACAW, described below, was proposed.

Hidden Terminal Problem with RTS-CTS

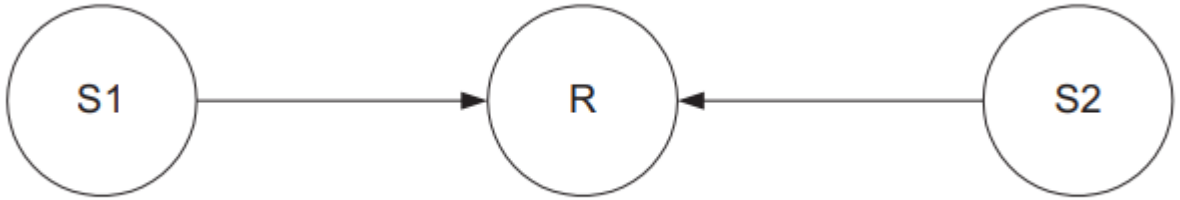
- The RTS-CTS control packet exchange cannot ensure collision-free data transmission that has no interference from hidden terminals.
- One very important assumption made is that every node in the capture area of the receiver (transmitter) receives the CTS (RTS) cleanly.
- Nodes that do not hear either of these clearly can disrupt the successful transmission of the Data or the ACK packet.

Hidden Terminal Problem with RTS-CTS



MACAW (MACA for Wireless)

- There are still some problems in MACA which are resolved by MACAW: an extension of MACA
- **Problem 1 of MACA: starvation of flows:**
  - •both S1 and S2 have the high volume of traffic, S1 seizes the channel first;
  - • packets transmitted by S2 get collided and it doubles CW (CW = 2CW);
  - • the probability that the node S2 seizes the channel is decreasing.



Starvation of the flow from S2.

Solution:

- • the packet header contains the field set to the current back-off value of the transmitting node;
- • a node receiving this packet copies this value to its back-off counter (fairness);

MACAW

- **Problem 2 of MACA: fast adjustment of CW:**
  - when a node successfully transmits a packet;
  - when a collisions is detected by a node.

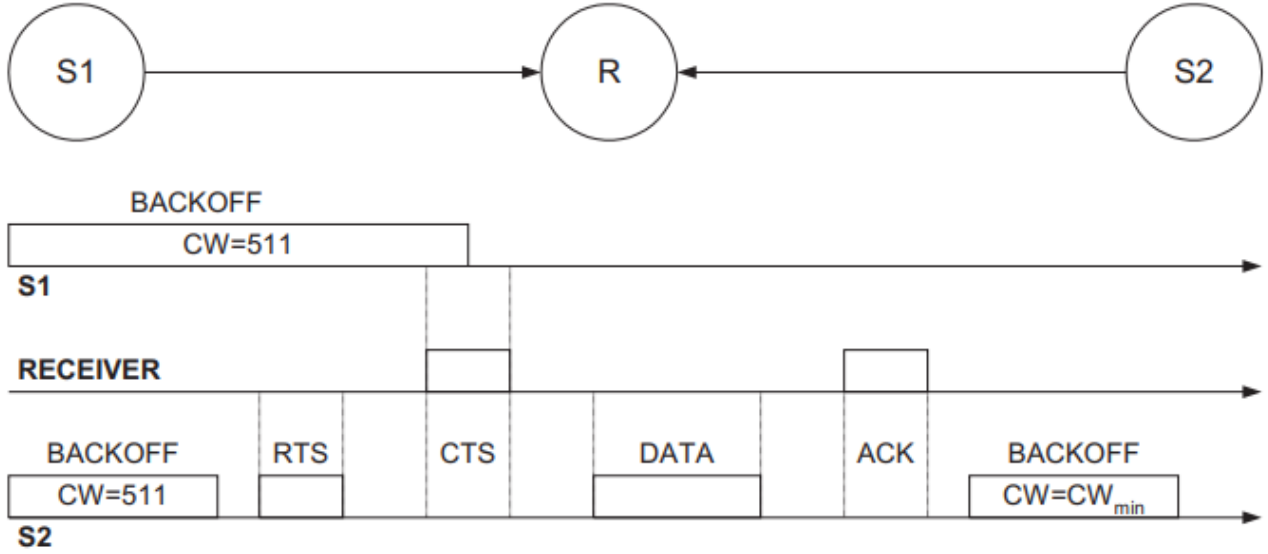


Figure 8: Rapid adjustments of the CW.

Solution: multiplicative increase when collision, linear decrease when success.

BEB in MACAW

- Multiplicative increase, linear decrease (MILD)
- MACAW sender:
  - CW0 = 2 and CWM = 64
  - Upon failed RTS/CTS

    $CW = \min[1.5CW, CWM]$
  - Upon successful RTS/CTS but failed ACK, no change
  - Upon successful RTS/CTS/DATA/ACK

    $CW = CW - 1$

- Another modification related to the back-off mechanism is that the MACAW implements per flow fairness as opposed to the per node fairness in MACA.
- This is done by maintaining multiple queues at every node, one each for each data stream, and running the backoff algorithm independently for each queue.
- A node that is ready to transmit packets first determines how long it needs to wait before it could transmit an RTS packet to each of the destination nodes.
- It then selects the packet for which the waiting time is minimal.

ACK in MACAW

- In MACA, the responsibility of recovering from transmission errors lies with the transport layer. As many TCP implementations have a minimum timeout period of about 0.5 sec, significant delay is involved while recovering from errors. Decreases the network throughput.
- But in MACAW, the error recovery responsibility is given to the data link layer (DLL).
- In MACAW, after successful reception of each data packet, the receiver node transmits an ACK packet.
- If the sender does not receive the ACK packet, it reschedules the same data packet for transmission.
- The sender would retry by transmitting an RTS for the same packet.
- But now the receiver, instead of sending back a CTS, sends an ACK for the packet received, and the sender moves on to transmit the next data packet.

MACAW

- **Problem 3 of MACA: an exposed node is free to transmit.**
  - node S2 hears RTS but not CTS (exposed node);
  - S2 initiates transfer to R2;
  - DATA from S1 and CTS from R2 may collide, CW unnecessary increases at S2.

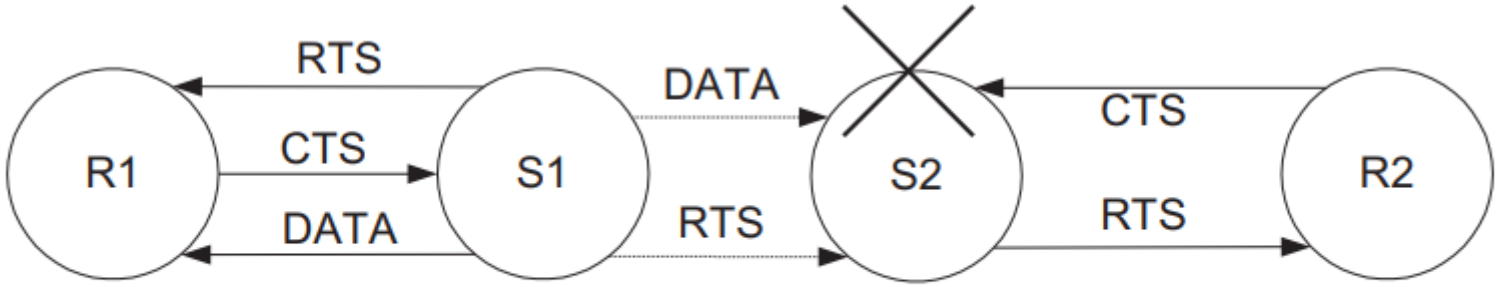


Figure 9: Problems with exposed node.

We conclude from this line of reasoning that S2 should defer transmission while S1 is transmitting data. Note that because S2 has only heard the RTS and not the CTS, station S2 cannot tell if the RTS-CTS exchange between S1 and R1 was a success and so does not know. So to confirm its successfulness a DS packet is used.

Solution: use of small data sending packet (DS) to update information.

MACAW

- **Problem 4 of MACA: neighbour receivers problem:**

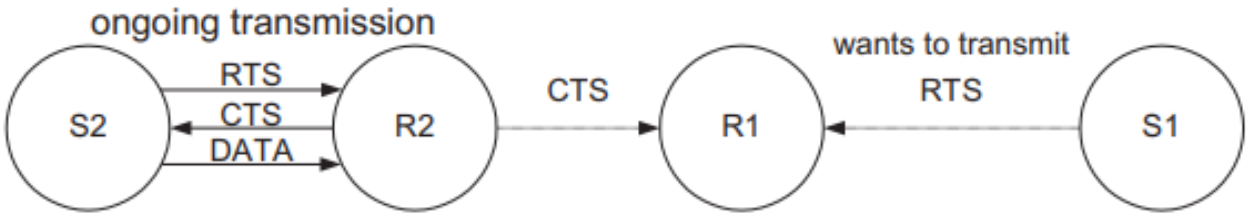


Figure 10: Illustration of the neighbor receivers problem.

- **Solution**: usage of request-for-request (RRTS) to send packets:
  - if R1 had received RTS (S1) and did not respond due to R2-S2 it backs off sends RRTS;
  - R2 hears RRTS waits for successive RTS-CTS between S1 and R1;
  - S1 hears the RRTS, transmits regular RTS and RTS-CTS-DATA-ACK takes place

Figure 11: Solution of the neighbor receivers problem.

MACAW

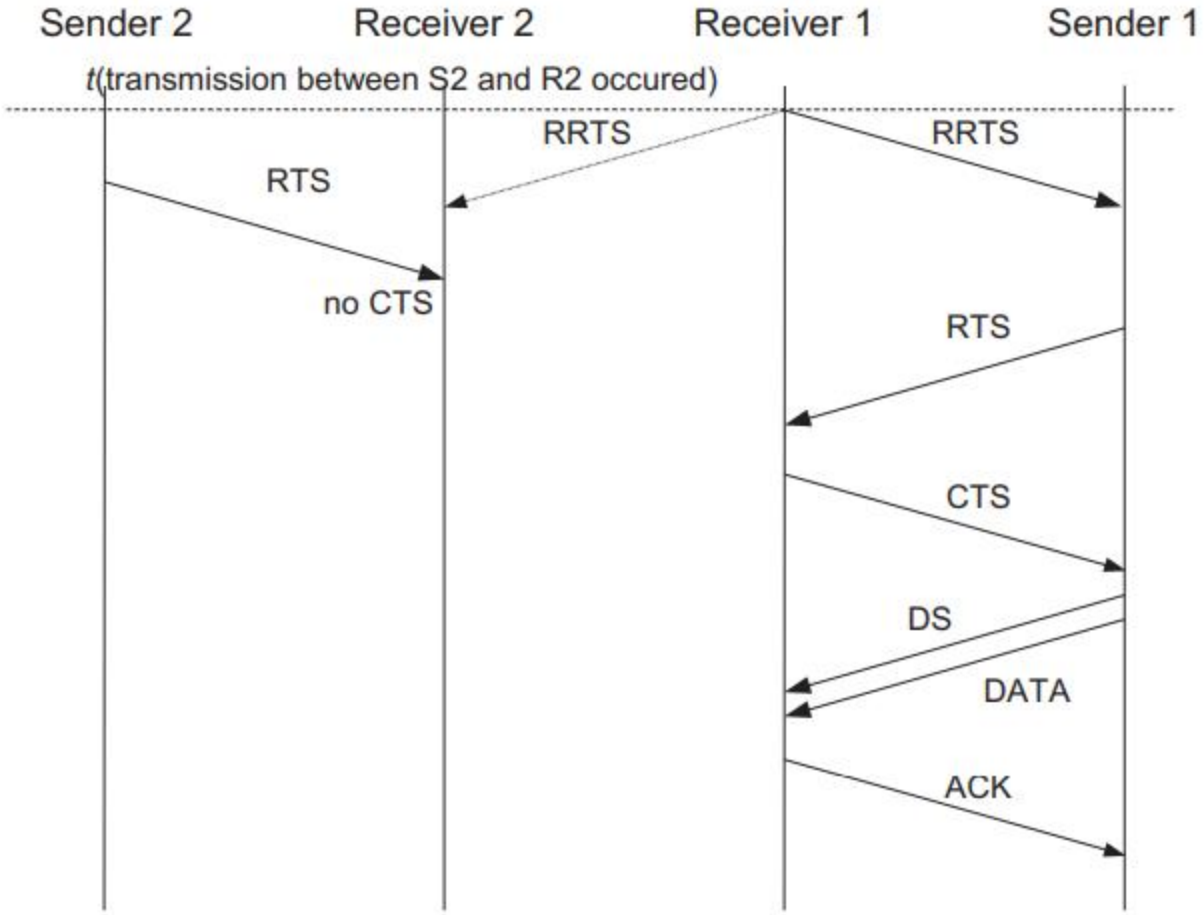


Figure 12: Packets exchange in neighbor receivers problem.

Routing in Ad hoc Wireless Networks

Introduction

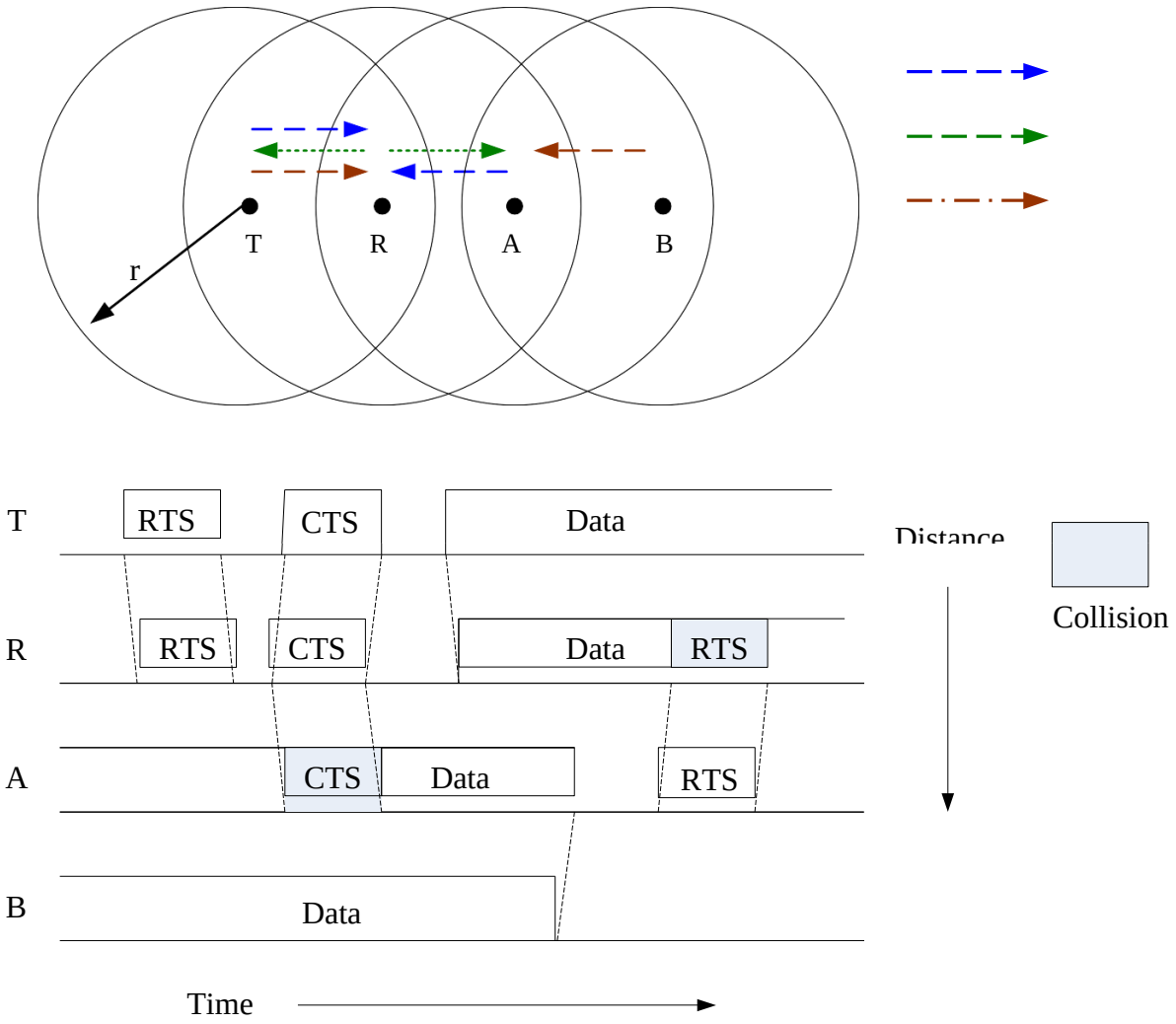
- Routing protocols used in wired networks cannot be directly applied to ad hoc wireless networks
  - Highly dynamic topology
  - No infrastructure for centralized administration
  - Bandwidth constrained
  - Energy constrained
- For the above reasons, we need to design new routing protocols for ad hoc networks

Issues in Designing a Routing Protocol

- Mobility:
  - Ad hoc is highly dynamic due to the movement of nodes
  - Node movement causes frequent path breaks
  - The path repair in wired network has slow convergence
- Bandwidth Constraint:
  - Wireless has less bandwidth due to the limited radio band: Less data rate and difficult to maintain topology information
  - Frequent change of topology causes more overhead of topology maintenance
  - Target: Bandwidth optimization and design topology update mechanism with less overhead

Issues in Designing a Routing Protocol

- Error-prone shared broadcast radio channel:
  - Wireless links have time varying characteristics in terms of link capacity and link-error probability
  - Target: Interact with MAC layer to find better-quality link
  - Hidden terminal problem causes packet collision
  - Target: Find routes through better quality links and find path with less congestion
- Hidden and exposed terminal problems
  - RTS-CTS control packet cannot ensure collision free, see Fig. 7.2
- Resource Constraints:
  - Limited battery life and limited processing power
  - Target: optimally manage these resources



Hidden terminal problem with RTS-CTS-Data-ACK scheme.

Characteristics of an Ideal Routing Protocol for Ad Hoc

- Fully distributed
- Adaptive to frequent topology changes
- Minimum connection setup time is desired
- Localized

– global maintenance involves a huge state propagation control overhead

- Loop free and free from stale routes
- Packet collision must seldom happen

Characteristics of an Ideal Routing Protocol for Ad Hoc (cont.)

- Converge to optimal route quickly
- Optimally use scarce resource

– Bandwidth, computing power, memory, and battery

- Remote parts of the network must not cause updates in the topology information maintained by this node
- Provide quality of service and support for time-sensitive traffic

Classifications of Routing Protocols

- Routing protocol can be broadly classified into four categories :
  - Routing information update mechanism
  - Use of temporal information for routing
  - Routing topology
  - Utilization of specific resource
- These classification is not mutually exclusive

Based on the Routing Information Update Mechanism

- Proactive or table-driven routing protocols
  - Maintain routing information in the routing table
  - Routing information is flooded in the whole network
  - Runs path-finding algorithm with the routing table
- Reactive or on-demand routing protocols
  - Obtain the necessary path while required
- Hybrid routing protocols
  - In the zone of given node : use table-driven
  - Out of the zone of given node : use on-demand

Based on the Use of Temporal Information for Routing

- Using past temporal information
  - Past status of the links or
  - the status of links at the time of routing to make routing decision
- Using future temporal information
  - Expected future status of the links to make decision
  - Node lifetime is also included
    - Ex: remaining battery charge, prediction of location, and link availability

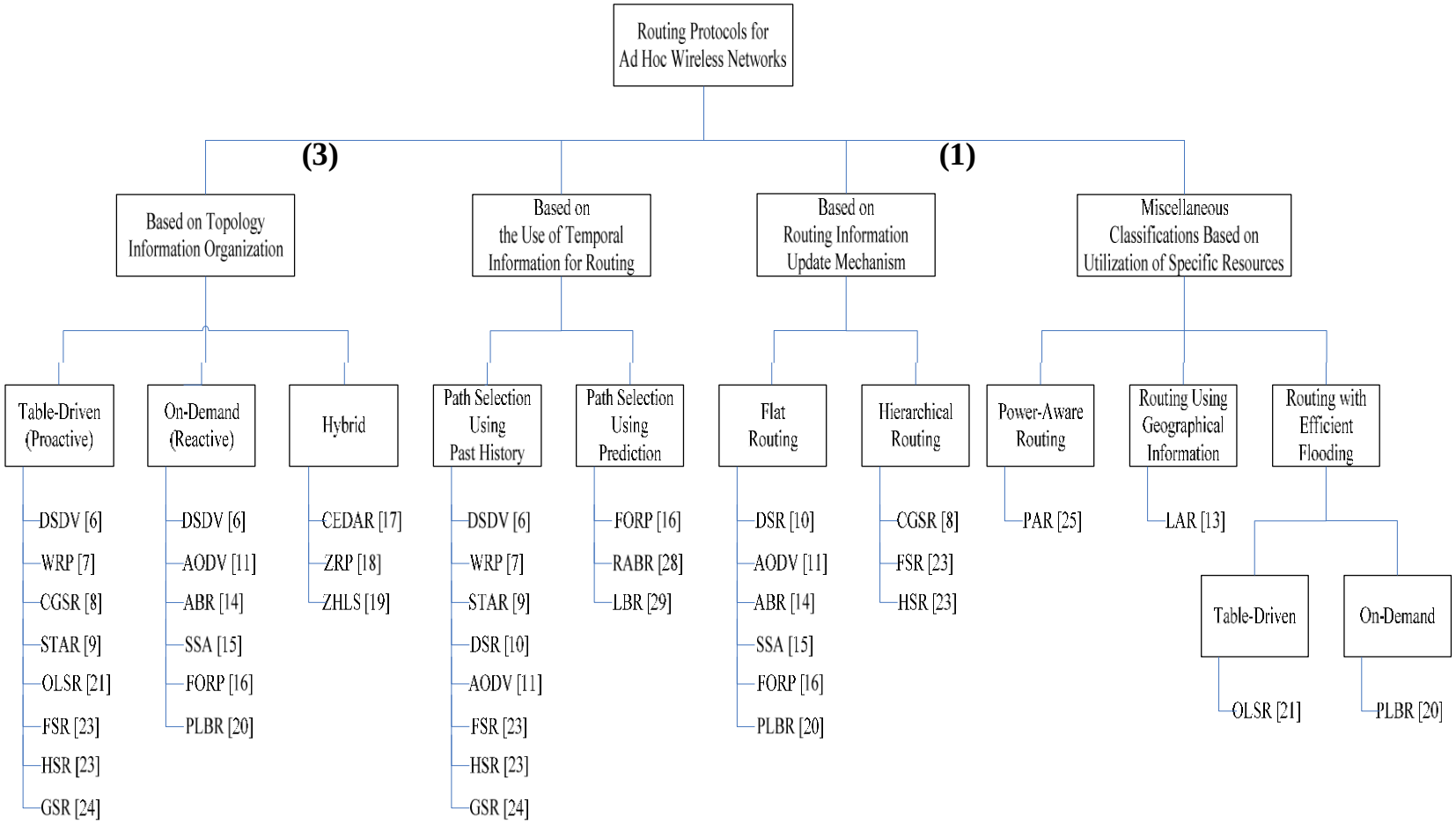
Based on the Routing Topology

- Flat topology routing protocols
  - Flat addressing scheme similar to IEEE 802.3 LANs
  - Globally unique addressing mechanism for nodes
- Hierarchical topology routing protocols
  - Logical hierarchy
  - Associated addressing scheme
  - May based on geographical information or hop distance

Based on the Utilization of Specific Resource

- Power-aware routing
  - Minimize consumption of resource
    - Ex: Battery power
- Geographical information assisted routing
  - Improve the routing performance
  - Reduce control overhead

Classifications of Routing Protocol:



- Table-Driven Routing Protocols
- On-Demand Routing Protocols
- Hybrid Routing Protocols
- Routing Protocol With Efficient Flooding Mechanisms
- Hierarchical Routing Protocols
- Power-Aware Routing Protocols

Table-Driven Routing Protocols

- We introduce these routing protocols:
  - Destination Sequenced Distance-Vector Routing Protocol (DSDV)
  - Wireless Routing Protocol (WRP)
  - Cluster-Head Gateway Switch Routing Protocol (CGSR)
  - Source-Tree Adaptive Routing Protocol (STAR)

Destination Sequenced Distance-Vector Routing Protocol (DSDV)

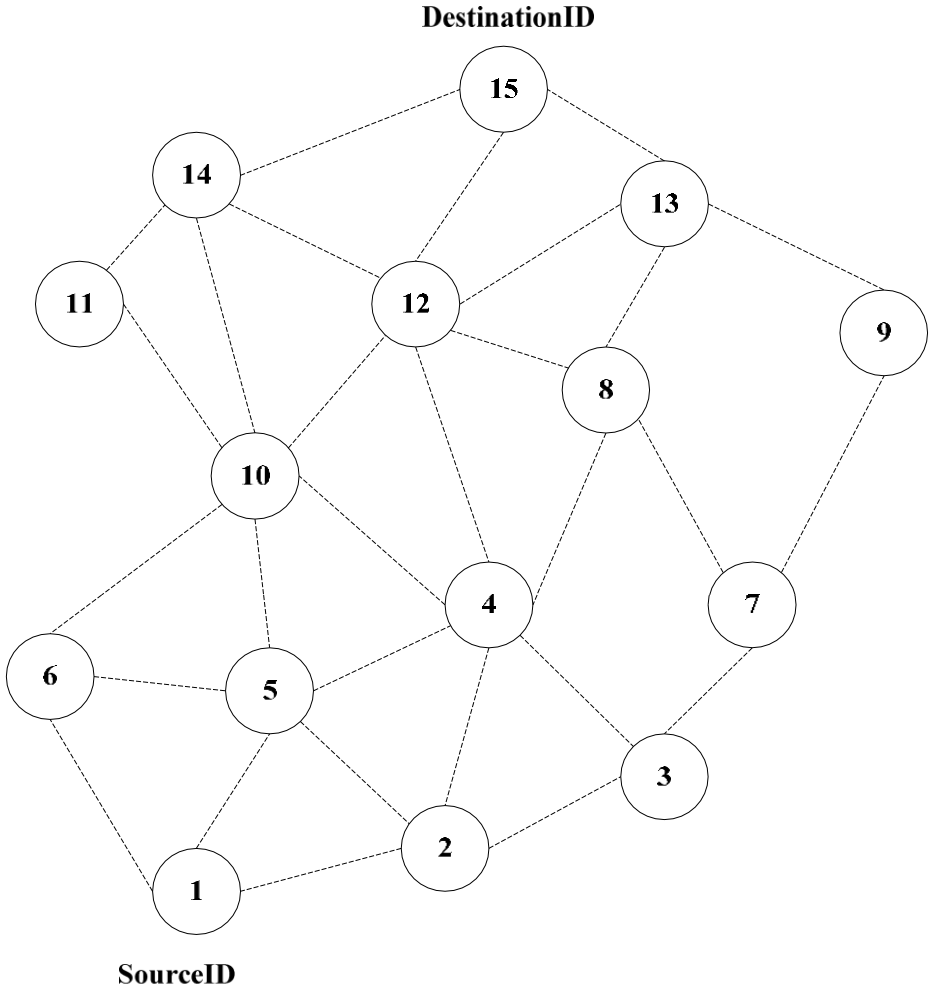
- Enhanced from distributed Bellman-Ford algorithm
- Obtain a table that contains shortest path from this node to every node
- Incorporate table updates with increasing sequence number tags
  - Prevent loops
  - Counter the count-to-infinity problem
  - Faster convergence

DSDV (Cont.)

- Exchange table between neighbors at regular time interval
- Two types of table updates
  - Incremental update
    - Takes a single network data packet unit (NDPU)
      - When no significant change in the local topology
  - Full dumps update
    - Takes multiple NDPUs:
      - When local topology changes significantly
      - Or incremental updates require more than a NDPU

DSDV
(Cont.)

- Table updates are initiated by the destination with the new sequence number which is always greater than the previous one
- Single link break cause propagation of table update information to the whole network
  - With odd sequence
- The changed node informs neighbors about new shortest path while receiving the table update message
  - With even sequence

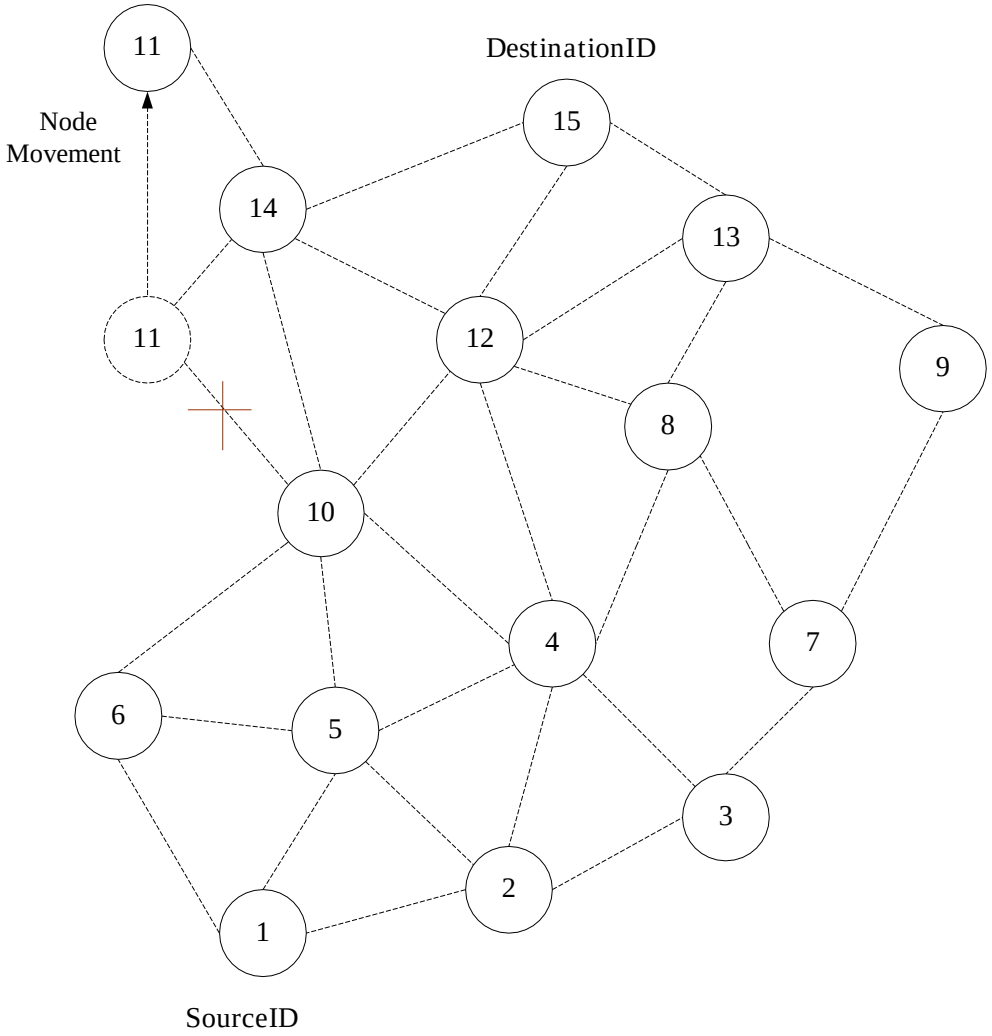


(a) Topology graph of the network

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

(b) Routing table for Node 1

Figure 7.5. Route establishment in DSDV



Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	5	4	180
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

Figure 7.6. Route maintenance in DSDV

DSDV (Cont.)

- Advantages:
  - Route setup process is very fast
  - Make the existing wired network protocol apply to ad hoc network with fewer modifications
- Disadvantages:
  - Excessive control overhead during high mobility
  - Node must wait for a table update message initiated by the destination node
    - Cause stale routing information at nodes

Cluster-Head Gateway Switch Routing Protocol (CGSR)

- Hierarchical topology based on cluster
- Cluster-head is elected by a Least Cluster Change (LCC)algorithm
- Clustering uses CDMA to allocate bandwidth between different clusters

– Every cluster has its own spreading code

- Cluster-head coordinate channel access based on token-based polling protocol
- Cluster-head can reach all member nodes within a single hop

Cluster-Head Gateway Switch Routing Protocol (CGSR)

- Communication passes through the cluster-head
- Gateway: a member in more than one clusters
  - Listens to multiple spreading codes
  - Becomes a bridge between cluster
  - Gateways are capable of simultaneously communicating over two interfaces can avoid conflict
- Performance is influenced by:
  - Token scheduling for cluster-head
  - Code scheduling for gateway

Cluster-Head Gateway Switch Routing Protocol (CGSR)

- Routing in CGSR is an extension of DSDV
- Each node maintains a routing table containing
  - Destination cluster-head for every node
  - The list of next-hop nodes for reaching destination cluster
- Route reconfiguration is necessitated by two factor:
  - Cluster-head changes
  - Stale entries in the cluster member table and routing table

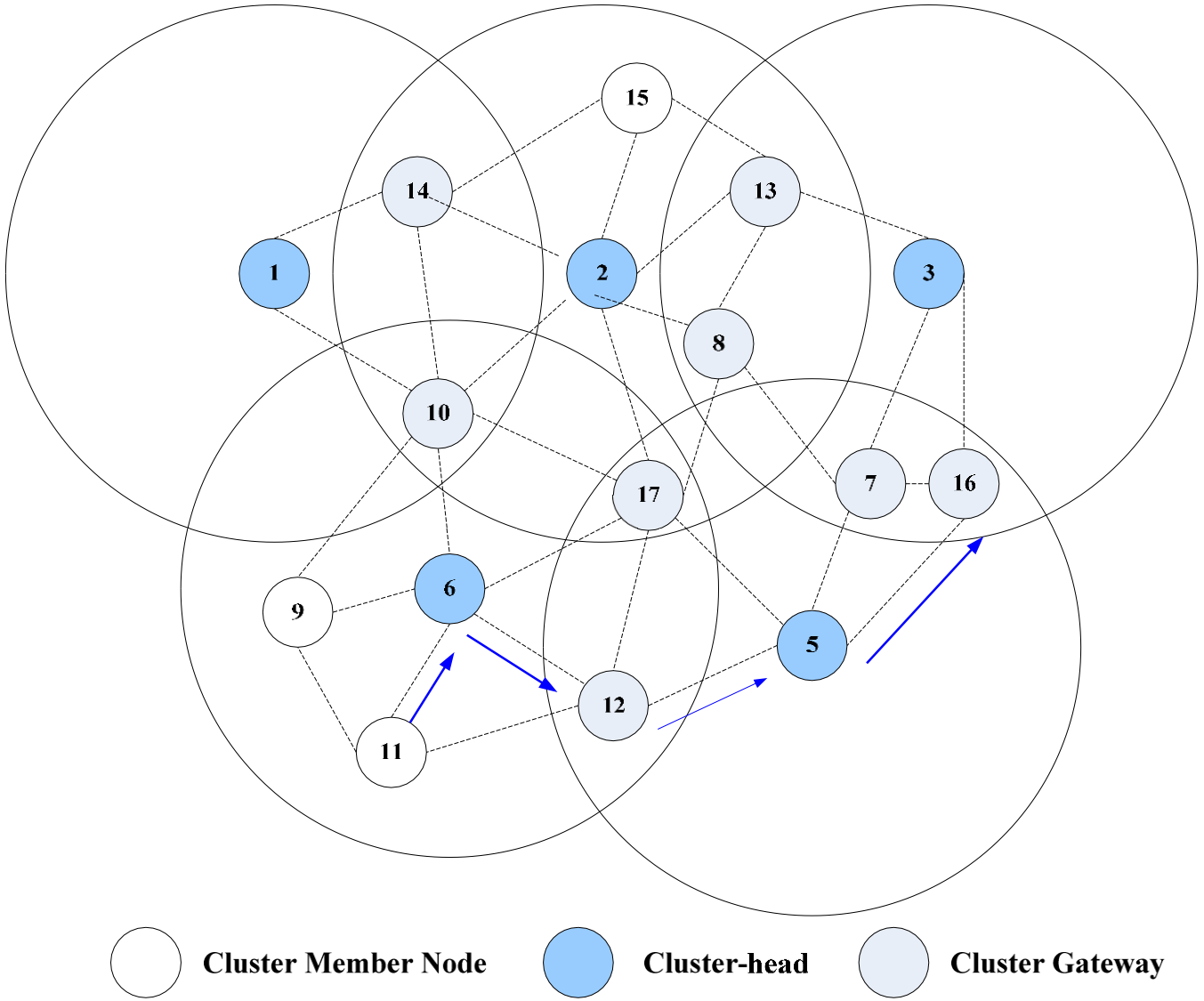


Figure 7.9. Route establishment in CGSR.

Cluster-Head Gateway Switch Routing Protocol (CGSR)

- Advantages:
  - Better bandwidth utilization
  - Easy to implement priority scheduling scheme
- Disadvantages:
  - Increase in path length
  - Instability when cluster-head are high mobility
  - Battery-draining rate at cluster-head is more than a normal node
    - Frequent changes in the cluster-head = multiple path break

- Table-Driven Routing Protocols
- On-Demand Routing Protocols
- Hybrid Routing Protocols
- Routing Protocol With Efficient Flooding Mechanisms
- Hierarchical Routing Protocols
- Power-Aware Routing Protocols
- Summery

On-demand Routing Protocol

- Unlike the table-driven routing protocols, on- demand routing protocols execute the path-finding process and exchange routing information only when a path is required by a node to communicate with a destination.

On-demand Routing Protocol

- Dynamic Source Routing Protocol (DSR)
- Ad Hoc On-demand Distance-Vector Routing Protocol (AODV)
- Temporally Ordered Algorithm (TORA)
- Location-Aided Routing (LAR)
- Associativity-Based Routing(ABR)
- Signal Stability-Based Adaptive Routing Protocol (SSA)
- Flow-Oriented Routing Protocol (FORP)

Dynamic Source Routing Protocol (DSR)

- Beacon-less: no *hello* packet
- Routing cache
- DSR contains two phases
  - Route Discovery (find a path)
    - Flooding RouteRequest with TTL from source
    - Response RouteReply by destination
  - If an forwarding node has a route to the destination in its route cache, it sends a RouteREply to the source
  - Route Maintenance (maintain a path)
    - RouteError

Routing Discovery

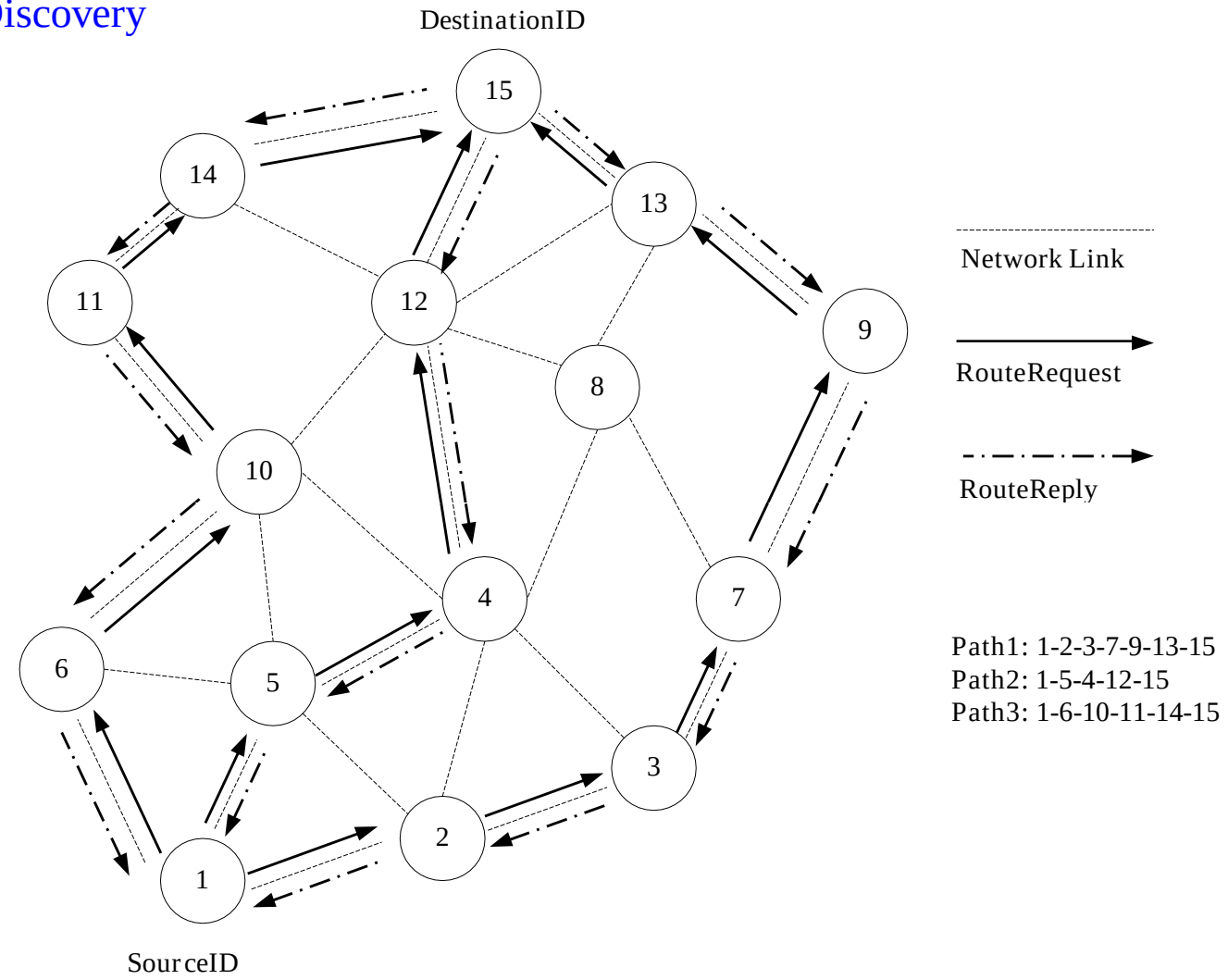


Figure 7.10. Route establishment in DSR.

Routing Maintain

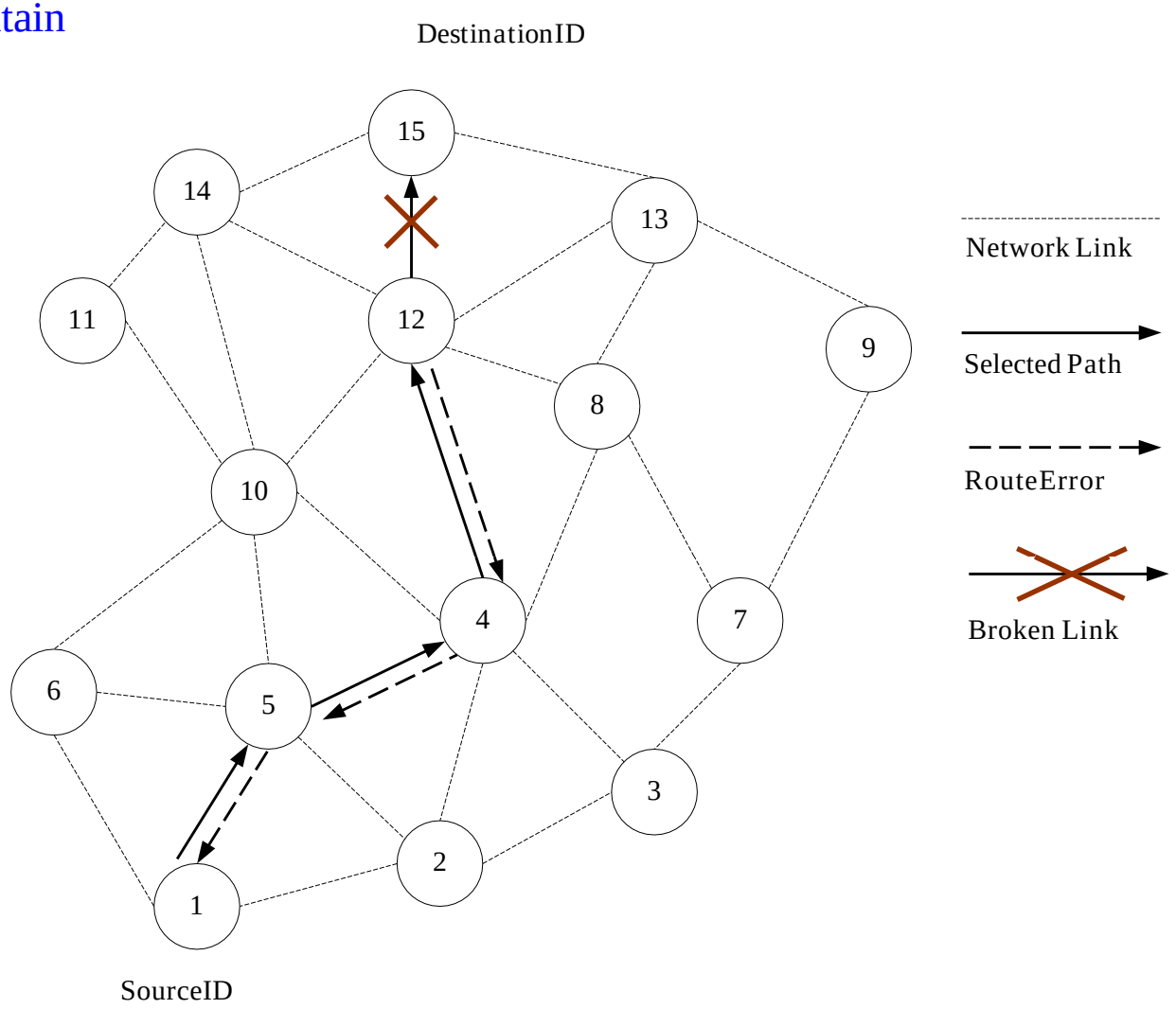


Figure 7.11. Route maintenance in DSR.

Dynamic Source Routing Protocol

- Advantage
  - No need to updating the routing tables
  - Intermediate nodes are able to utilize the Route Cache information efficiently to reduce the control overhead
  - There are no “hello” messages needed (beacon-less)
- Disadvantage
  - The Route Maintenance protocol does not locally repair a broken link
  - There is always a small time delay at the begin of a new connection

Ad Hoc On-demand Distance-Vector Routing Protocol (AODV)

- Every node has a routing table. When a node knows a route to the destination, it sends a route reply to the source node
- The major difference between DSR and AODV
  - DSR uses source routing in which a data packet carries the complete path to traversed.
  - AODV stores the next-hop information corresponding to each flow for data packet transmission.
- Message types
  - Route Requests (RREQs)
  - Route Replies (RREPs)
  - Route Errors (RERRs).

AODV

- RouteRequest packet carries:
  - SreID, DestID, DestSeqNum, BcastID, and TTL
  - DestSeqNum indicates the freshness of the route is accepted
  - An intermediate node receives a RouteRequest packet. It either forwards it or prepares a RouteReply if it has a valid route to the destination
- RouteReply packet:
  - A node receives RouteReply packet will record the information as the next hop toward the destination
- AODV does not repair a broken path locally

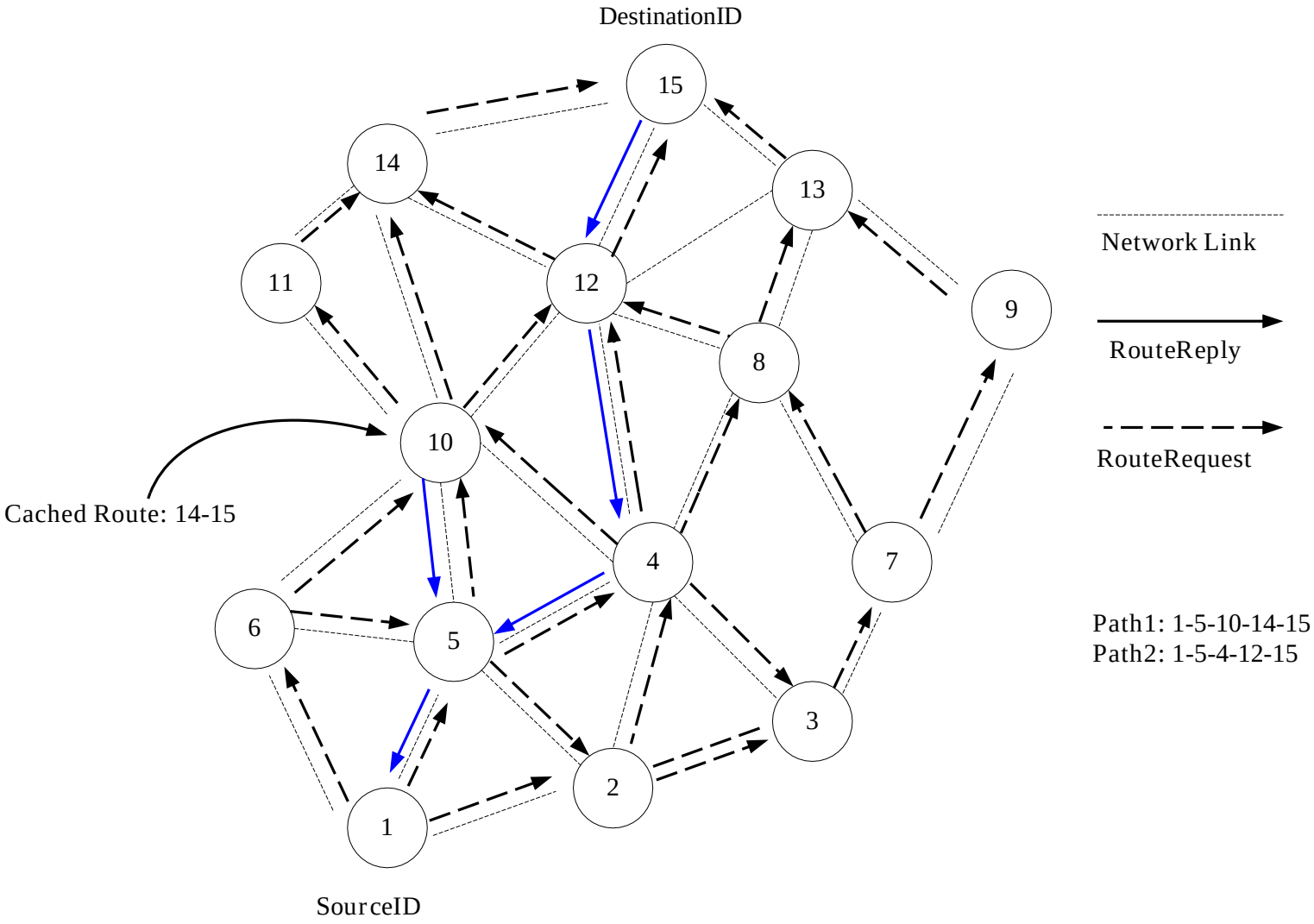


Figure 7.12. Route establishment in AODV.

Route Maintenance

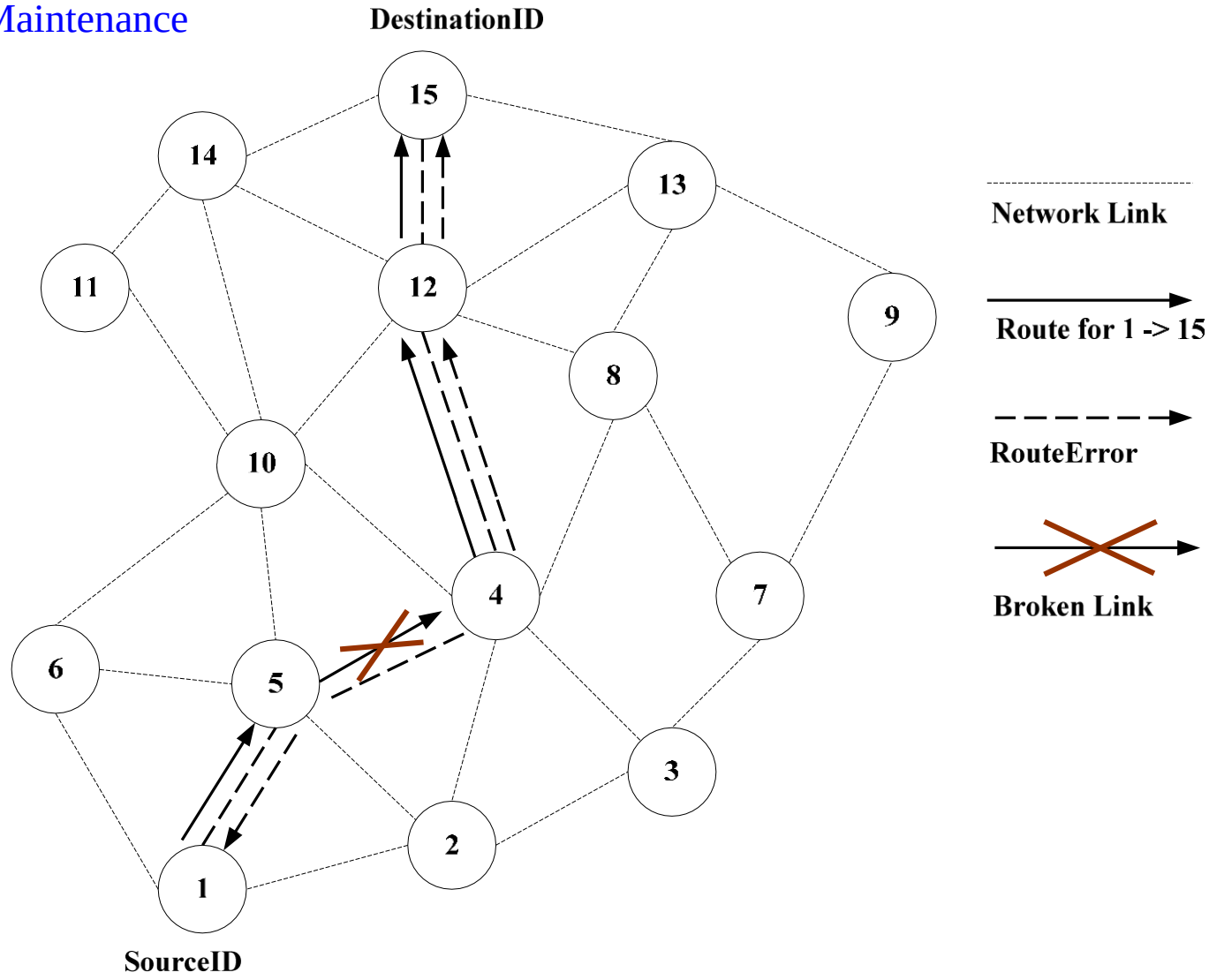


Figure 7.13. Route maintenance in AODV.

AODV

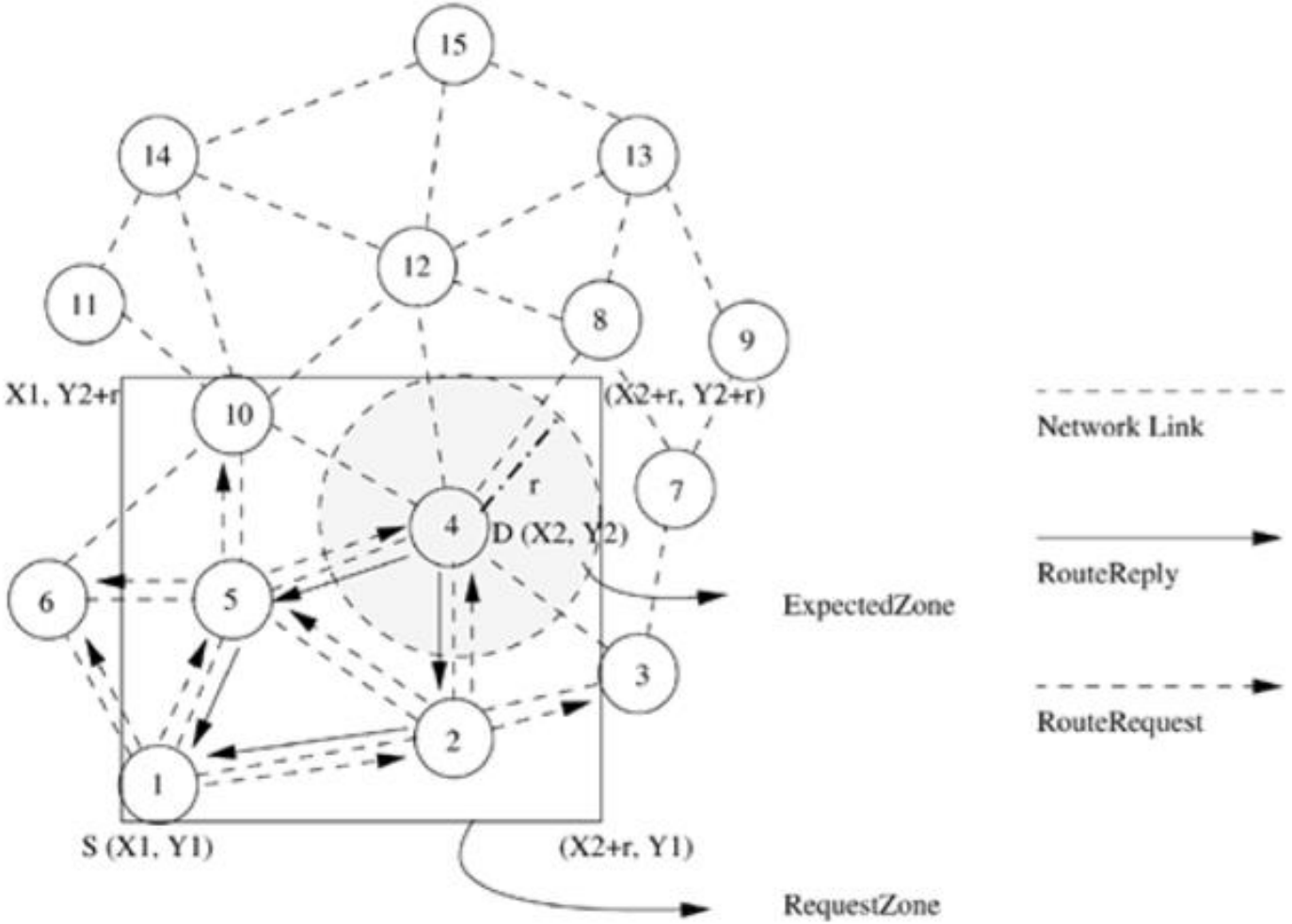
- Advantage
  - Establish on demand
  - Destination sequences are used to find the latest path to destination
  - The connection setup delay is less
- Disadvantage
  - Intermediate node can lead to inconsistent route
  - Beacon-base
  - Heavy control overhead

Location Aided Routing (LAR)

- Utilizes the location information (by GPS) for improving the efficiency of routing by reducing the control overhead.
- Designates two geographical regions for selective forwarding of control packets.
- **ExpectedZone:** is the region in which the destination node is expected to be present.
- **RequestZone** is a geographical region within which the path-finding control packets are permitted to be propagated.
- This area is determined by the sender of a data transfer session.
- The control packets used for path-finding are forwarded by nodes which are present in the RequestZone and are discarded by nodes outside the zone.
- When the requested nodes are not present in the RequestZone, additional area is included for forwarding the packets.
- This is done, when the first attempt for obtaining a path to a destination using the initial RequestZone fails to yield a path within a sufficiently long waiting time.
- The nodes decide to forward or discard the control packets based on two algorithms, namely, LAR1 and LAR2.

LAR1

- RequestedZone and ExpectedZone in LAR1



LAR2

- Source node S (node 5) includes the distance between itself and the destination node D along with the (X, Y) coordinates of the destination node D in theRouteRequest.
- Intermediate node computes the distance to the node D.
- If this distance is less than the distance from S to node D + δ, then the RouteRequest packet is forwarded. Otherwise, discarded
- Where δ is a parameter of the algorithm decided based on the error in location estimation and mobility