

CHAPTER 1
OVERVIEW OF MOBILE AD HOC NETWORKS
(MANETs)

1.1 Introduction

This chapter presents an overview of MANETs covering the characteristics, applications, mobility models, and a reference model of MANETs. The most significant issue in MANETs is reviewed which include routing, especially the working of Ad hoc On-demand Distance Vector routing protocol (AODV) which is the general scope of this research.

1.2 Ad Hoc Network

An ad hoc network [13] is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration [1]. They are infrastructureless networks formed on-the-fly (anytime, anywhere, for virtually any application) with limited life of existence. Ad hoc networks can be established as a stand-alone group of mobile terminals, which communicate autonomously in a self-organized manner or are connected to a pre-existing infrastructure and use it to communicate with outside networks [2]. Ad hoc terminals (i.e., nodes) communicate wirelessly and share the same media (radio, infrared, etc.) and are free to move while communicating with other nodes as shown in Figure 1.1. [3].

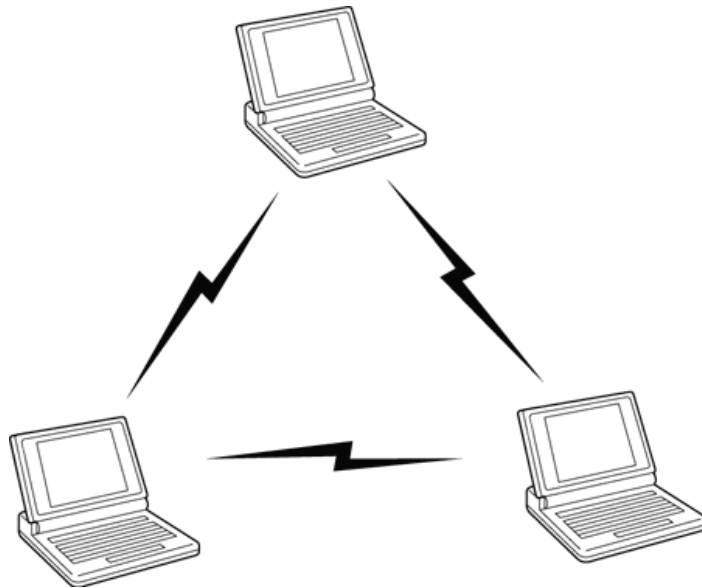


Figure 1.1 Mobile Ad Hoc Network

1.3 Characteristics of Ad Hoc Networks

The MANET working group within the IETF describes the main characteristics of MANETs which differs from the characteristics of traditional wireless local area networks such as WLANs due to the dynamic and the infrastructureless natures of MANETs. The most significant characteristics of a MANET are summarized as follows [4]:

- A collection of autonomous terminals means that each mobile node in a MANET functions as both a host and a router.
- A peer-to-peer and multi-hop wireless network means that no central routing in MANET.
- It has a dynamic topology means that it contains a set of nodes that are continuously moving leading to random change in the network topology rapidly at unpredictable times.
- It has a distributed operation which means that the control and management of the network is distributed among the nodes due to the absence of any type of infrastructure that usually supports the central control of the network operations. The nodes involved in a MANET should collaborate amongst each other, and each node acts as a host and router at the same time to implement network functions such as security and routing.
- It can be rapidly deployed.
- It does not rely on pre-existing infrastructure.
- A bandwidth-constrained network with variable capacity links.
- Self-adapts to the connectivity and propagation patterns.
- Adapts to traffic and mobility patterns.
- It has a limited physical security, especially in the absence of any centralized authentication or encryption. Existing link security techniques are often applied within wired networks and WLANs to reduce security threats however, MANETs are generally more prone to physical security threats than are wired networks or WLANS.
- It has an energy-constrained operation so that energy conservation of batteries in mobile nodes may be considered one of the most significant design criteria for optimization in MANETs.

1.4 Services and Applications of ad hoc networks

Table 1.1 below gives an overview of existing applications and examples of services they provide [3].

Applications	Descriptions/Services
Tactical networks	Military communication, operations Automated Battlefields
Emergency services	Search-and-rescue operations Disaster recovery, e.g, early retrieval and transmission of patient data (record, status, diagnosis) from/to the hospital Replacement of a fixed infrastructure in case of earthquakes, hurricanes, fire, etc.
Commercial environments	E-Commerce, e.g, electronic payments from anywhere (i.e., in a taxi). Business: – dynamic access to customer files stored in a central location on the fly provide consistent databases for all agents – mobile office Vehicular Services: – transmission of news, road conditions, weather, music – local ad hoc network with nearby vehicles for road/accident guidance – Unmanned Aerial Vehicles (UAV) — remotely piloted or self-piloted aircrafts that can carry cameras, sensors, communications equipment or other payloads
Home and enterprise networking	Home/office wireless networking (WLAN), e.g, shared whiteboard application, use PDA to print anywhere, trade shows Personal Area Network (PAN)
Educational applications	Set up virtual classrooms or conference rooms Set up ad hoc communication during conferences, meetings or lectures
Sensor networks	Home security and tracing Indoor/outdoor environmental monitoring Disaster prevention Health and wellness monitoring Power monitoring Location awareness Factory and process automation Military applications
Hybrid networks	Enhancements of cell coverage and connectivity of holes

Table 1.1 Applications of Wireless Ad Hoc Networks.

1.5 Mobility Models for Mobile Ad Hoc Networks

An ad hoc wireless network [10] is a multi-hop wireless configuration without a fixed infrastructure or central administration. It consists of mobile nodes, which create a highly dynamic environment that poses some of the major challenges in network design and performance analysis. *Mobility modelling* [5] that specifies the dynamic characteristics of nodes movement, is a crucial mechanism in evaluation and study of such networks [3].

For some mobility models [12], the movement of a mobile node is likely to be affected by its movement history. We refer to this type of mobility model as a “*mobility model with temporal dependency*.” In some mobility scenarios, the mobile nodes tend to travel in a correlated manner. We refer to such models as “*mobility models with spatial dependency*.” Another class is the mobility model with geographic restriction, where the movement of nodes is bounded by streets, freeways, or obstacles [1]. The categorization of mobility models is shown in Figure 1.2.

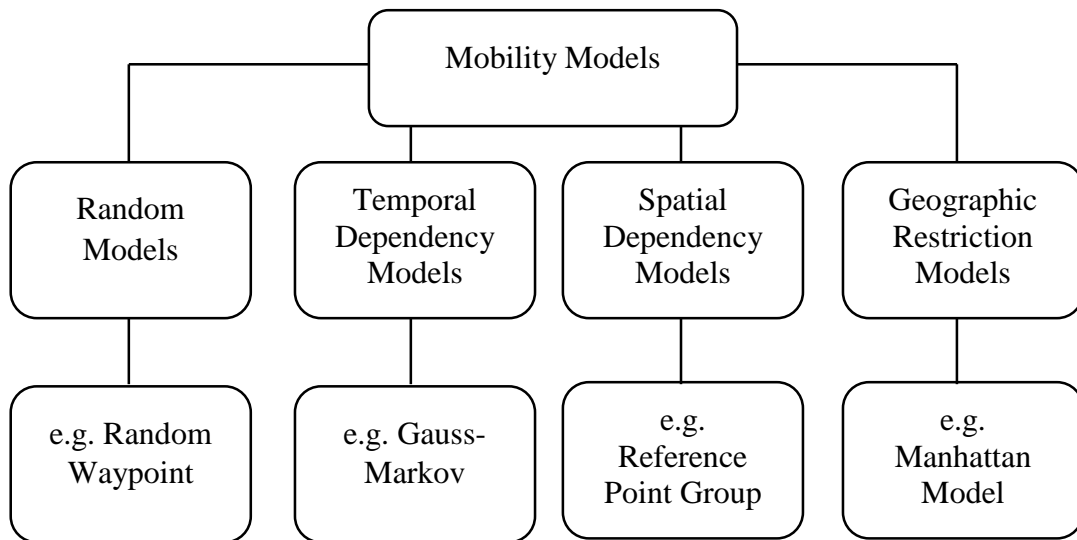


Figure 1.2 Classification of Mobility Models

1.6 Routing in Mobile Ad hoc Networks

The routing in mobile ad hoc networks [8, 9] is very challenging due to the frequent updates for changes in topologies, and active routes may be disconnected as mobile nodes move from one place to another. Routing schemes in mobile ad hoc networks [11] must include mechanisms that cope with difficulties incurred by node mobility and topology changes along with lower consumption of energy, communications bandwidth, and computing resources. The traditional **link-state** and **distance vector** algorithms that are used for routing in non-MANET networks are not suitable for MANETs because of large routes updates traffic. The excessive overhead traffic caused route updates may lead to the consumption of a

significant part of the available resources including the channel bandwidth, especially in a large MANET. Many routing protocols have been proposed for MANETs to overcome these problems [5].

1.7 On Demand Routing Protocols

On-demand routing protocols [1] do not maintain the network topology information continuously. They perform a path discovery process and exchange routing information only when it is needed. In order to start the packet transmission, the source node checks if the requested route toward the destination node exists. If such route does not exist, it performs a path discovery procedure. Two nodes that have not communicated before do not maintain a route between each other. The route discovery often consists of flooding of request messages through the network [3].

A reactive protocol [8] manages the path through path discovery, path maintenance and path deletion (which is optional). Data forwarding is accomplished according to two main techniques: source routing and hop-by-hop. Path discovery is triggered asynchronously on demand. Network nodes update the routing state through path discovery process, storing the information about discovered paths to the destination. Routing state information can be maintained with different techniques such as route caches, temporary routing tables, and logical structures [3].

1.8 Ad Hoc On-Demand Distance Vector Protocol (AODV)

AODV [6] is a reactive routing protocol designed for ad hoc networks. Each mobile host operates as a specialized router, and routes are obtained as needed (i.e., on demand with little or no reliance on periodic advertisements). The AODV routing algorithm is quite suitable for a dynamic self-starting network as required by users wishing to utilize ad hoc networks[1].

AODV uses symmetric links between neighboring nodes. It does not attempt to follow paths between nodes when one of the nodes cannot hear the other one. Nodes do not lie on active paths; they neither maintain any routing information nor participate in any periodic routing table exchanges [1].

One distinguishing feature of AODV is its use of a destination sequence number for each route entry [7]. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes [6].

1.9 Working of AODV

Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV [6-9]. These message types are received via UDP, and normal IP header processing applies. So, for instance, the requesting node is expected to use its IP address as the Originator IP address for the messages. For broadcast messages, the IP limited broadcast address (255.255.255.255) is used. This means that such messages are not blindly forwarded. However, AODV operation does require certain messages (e.g., RREQ) to be disseminated widely, perhaps throughout the ad hoc network. The range of dissemination of such RREQs is indicated by the TTL (Time To Live) in the IP header. Fragmentation is typically not required [6].

As long as the endpoints of a communication connection have valid routes to each other, AODV does not play any role. When a route to a new destination is needed, the node broadcasts a RREQ to find a route to the destination. A route can be determined when the RREQ reaches either the destination itself, or an intermediate node with a 'fresh enough' route to the destination. A 'fresh enough' route is a valid route entry for the destination whose associated sequence number is at least as great as that contained in the RREQ. The route is made available by unicasting a RREP back to the origination of the RREQ. Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator, or likewise from any intermediate node that is able to satisfy the request [6].

Nodes monitor the link status of next hops in active routes. When a link break in an active route is detected, a RERR message is used to notify other nodes that the loss of that link has occurred (the Figure 1.11 illustrate the three circumstances under which a Node would broadcast a RERR to its neighbors). The RERR message [7] indicates those destinations (possibly subnets) which are no longer reachable by way of the broken link. In order to enable this reporting mechanism, each node keeps a "precursor list", containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination. The information in the precursor lists is most easily acquired during the processing for generation of a RREP message, which by definition has to be sent to a node in a precursor list. If the RREP has a nonzero prefix length, then the originator of the RREQ which solicited the RREP information is included among the precursors for the subnet route (not specifically for the particular destination) [6].

A RREQ [6-8], may also be received for a multicast IP address. In this document, full processing for such messages is not specified. For example, the originator of such a RREQ for a multicast IP address may have to follow special rules. However, it is important to enable correct multicast operation by intermediate nodes that are not enabled as originating or destination nodes for IP multicast addresses, and likewise are not equipped for any special multicast protocol processing. For such multicast-unaware nodes, processing for a multicast IP address as a destination IP address **MUST** be carried out in the same way as for any other destination IP address [6].

AODV is a routing protocol [6], and it deals with route table management. Route table information must be kept even for short-lived routes, such as are created to temporarily store reverse paths towards nodes originating RREQs. AODV uses the following fields with each route table entry [6]:

- Destination IP Address
- Destination Sequence Number
- Valid Destination Sequence Number flag
- Other state and routing flags (e.g., valid, invalid, repairable, being repaired)
- Network Interface
- Hop Count (number of hops needed to reach destination)
- Next Hop
- List of Precursors
- Lifetime (expiration or deletion time of the route)

Managing the sequence number is crucial to avoiding routing loops. A destination node increments its own sequence number in two circumstances [6], immediately before a node originates a route discovery, it **MUST** increment its own sequence number. This prevents conflicts with previously established reverse routes towards the originator of a RREQ, or immediately before a destination node originates a RREP in response to a RREQ, it **MUST** update its own sequence number to the maximum of its current sequence number and the destination sequence number in the RREQ packet. The Figure 1.10. Shows what was explained about the sequence numbers.

A node may change the sequence number in the routing table entry of a destination only if [6]:

- 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.

An example of propagation and reverse path set-up in AODV is presented in Figure 1.3.

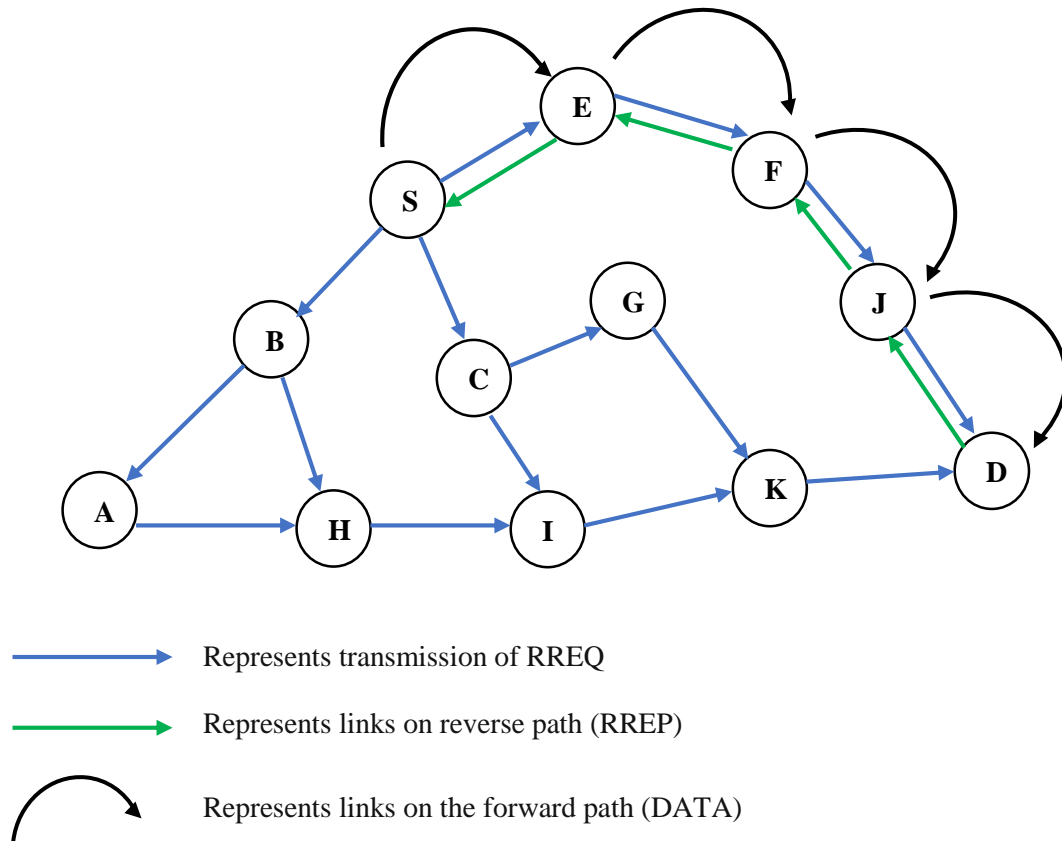


Figure 1.3 Propagation and Path Set-Up in AODV

1.10 Message Formats

1.10.1 Route Request (RREQ) Message Format

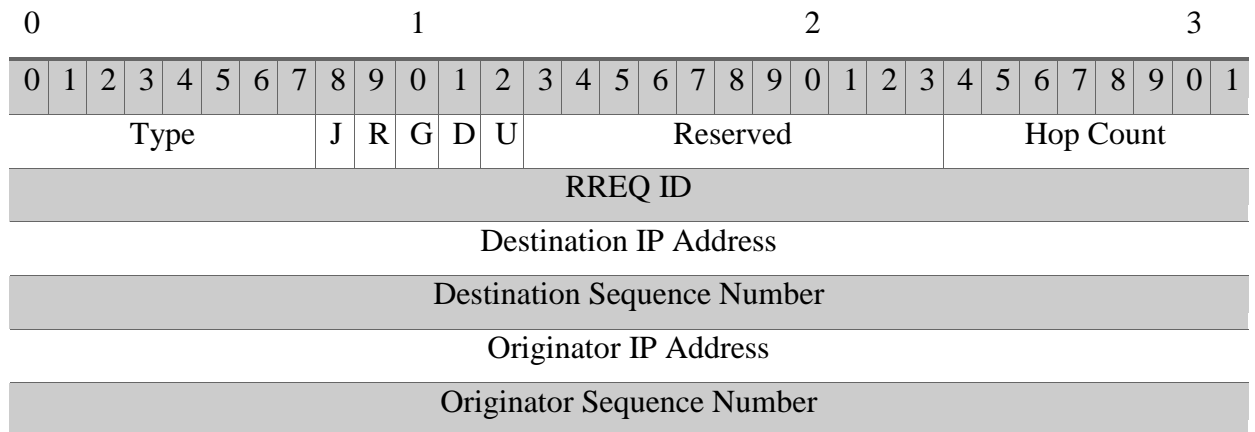


Figure 1.4 RREQ Packet Format of AODV Protocol

The format of the Route Request message [6], is illustrated above, and contains the following fields:

Fields	Descriptions
Type	1
J	Join flag; reserved for multicast.
R	Repair flag; reserved for multicast.
G	Gratuitous RREP flag; indicates whether a gratuitous RREP should be unicast to the node specified in the Destination IP Address field.
D	Destination only flag; indicates only the destination may respond to this RREQ.
U	Unknown sequence number; indicates the destination Sequence number is unknown.
Reserved	Sent as 0; ignored on reception.
Hop Count	The number of hops from the Originator IP Address to the node handling the request.
RREQ ID	A sequence number uniquely identifying the particular RREQ when taken in conjunction with the originating node's IP address.
Destination IP Address	The IP address of the destination for which a route is desired.
Destination Sequence Number	The latest sequence number received in the past by the originator for any route towards the destination.
Originator IP Address	The IP address of the node which originated the Route Request.
Originator Sequence Number	The current sequence number to be used in the route entry pointing towards the originator of the route request.

Table 1.2 Fields Description of RREQ Packet

1.10.2 Route Reply (RREP) Message Format

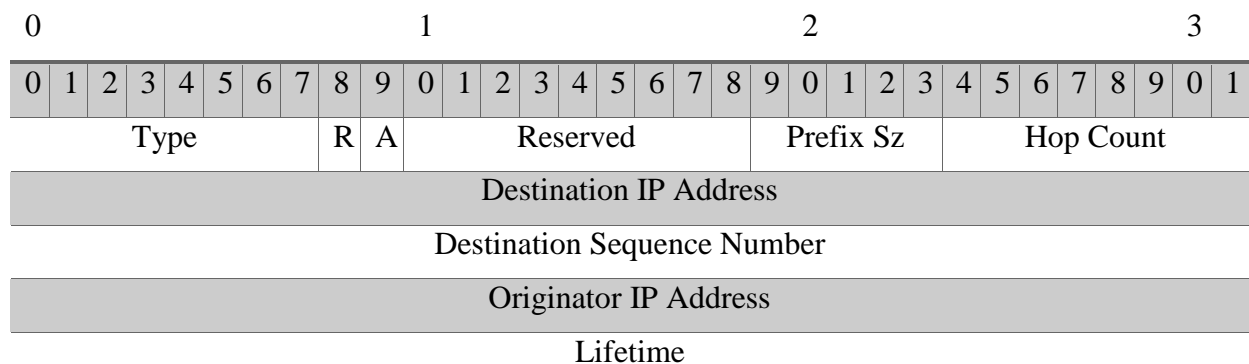


Figure 1.5 RREP Packet Format of AODV Protocol

The format of the Route Reply message is illustrated above, and contains the following fields [6]:

Fields	Descriptions
Type	2
R	Repair flag; used for multicast.
A	Acknowledgment required.
Reserved	Sent as 0; ignored on reception.
Prefix Size	If nonzero, the 5-bit Prefix Size specifies that the indicated next hop may be used for any nodes with the same routing prefix (as defined by the Prefix Size) as the requested destination.
Hop Count	The number of hops from the Originator IP Address to the Destination IP Address. For multicast route requests this indicates the number of hops to the multicast tree member sending the RREP.
Destination IP Address	The IP address of the destination for which a route is supplied.
Destination Sequence Number	The destination sequence number associated to the route.
Originator IP Address	The IP address of the node which originated the RREQ for which the route is supplied.
Lifetime	The time in milliseconds for which nodes receiving the RREP consider the route to be valid.

Table 1.3 Fields Description of RREP Packet

1.10.3 Route Error (RERR) Message Format

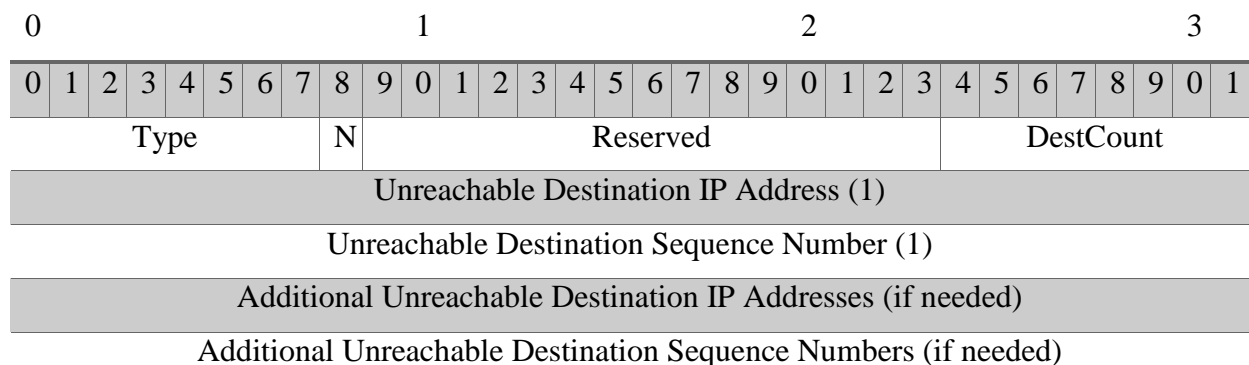


Figure 1.6 RERR Packet Format of AODV Protocol

The format of the Route Error message is illustrated above, and contains the following fields [6]:

Fields	Descriptions
Type	3
N	No delete flag; set when a node has performed a local repair of a link, and upstream nodes should not delete the route.
Reserved	Sent as 0; ignored on reception.
DestCount	The number of unreachable destinations included in the message; MUST be at least 1.
Unreachable Destination IP Address	The IP address of the destination that has become unreachable due to a link break.
Unreachable Destination Sequence Number	The sequence number in the route table entry for the destination listed in the previous Unreachable Destination IP Address field.

Table 1.4 Fields Description of RERR Packet

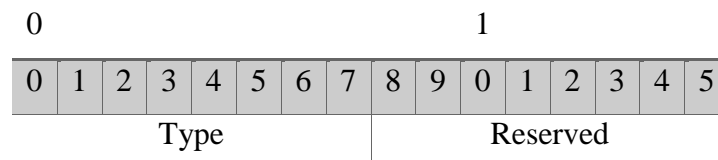
A node initiates processing for a RERR message in three situations [6] :

- 1) If it detects a link break for the next hop of an active route in its routing table while transmitting data (and route repair, if attempted, was unsuccessful), or
- 2) If it gets a data packet destined to a node for which it does not have an active route and is not repairing (if using local repair), or
- 3) If it receives a RERR from a neighbor for one or more active routes.

The Figure 1.11 below illustrate the three circumstances under which a Node would broadcast a RERR to its neighbors.

1.10.4 Route Reply Acknowledgment (RREP-ACK) Message Format

The Route Reply Acknowledgment (RREP-ACK) message [6, 7]. MUST be sent in response to a RREP message with the 'A' bit set. This is typically done when there is danger of unidirectional links preventing the completion of a Route Discovery cycle [6].

**Figure 1.7** RREP-ACK Packet Format of AODV Protocol

Type 4, Reserved Sent as 0; ignored on reception.

In the Figure 1.8, Node 1 wishes to send a message to Node 3. Node 1's Neighbors are Nodes 2 & 4. Since Node 1 cannot directly communicate with Node 3, Node 1 sends out a RREQ. The RREQ is heard by Node 4 and Node 2.

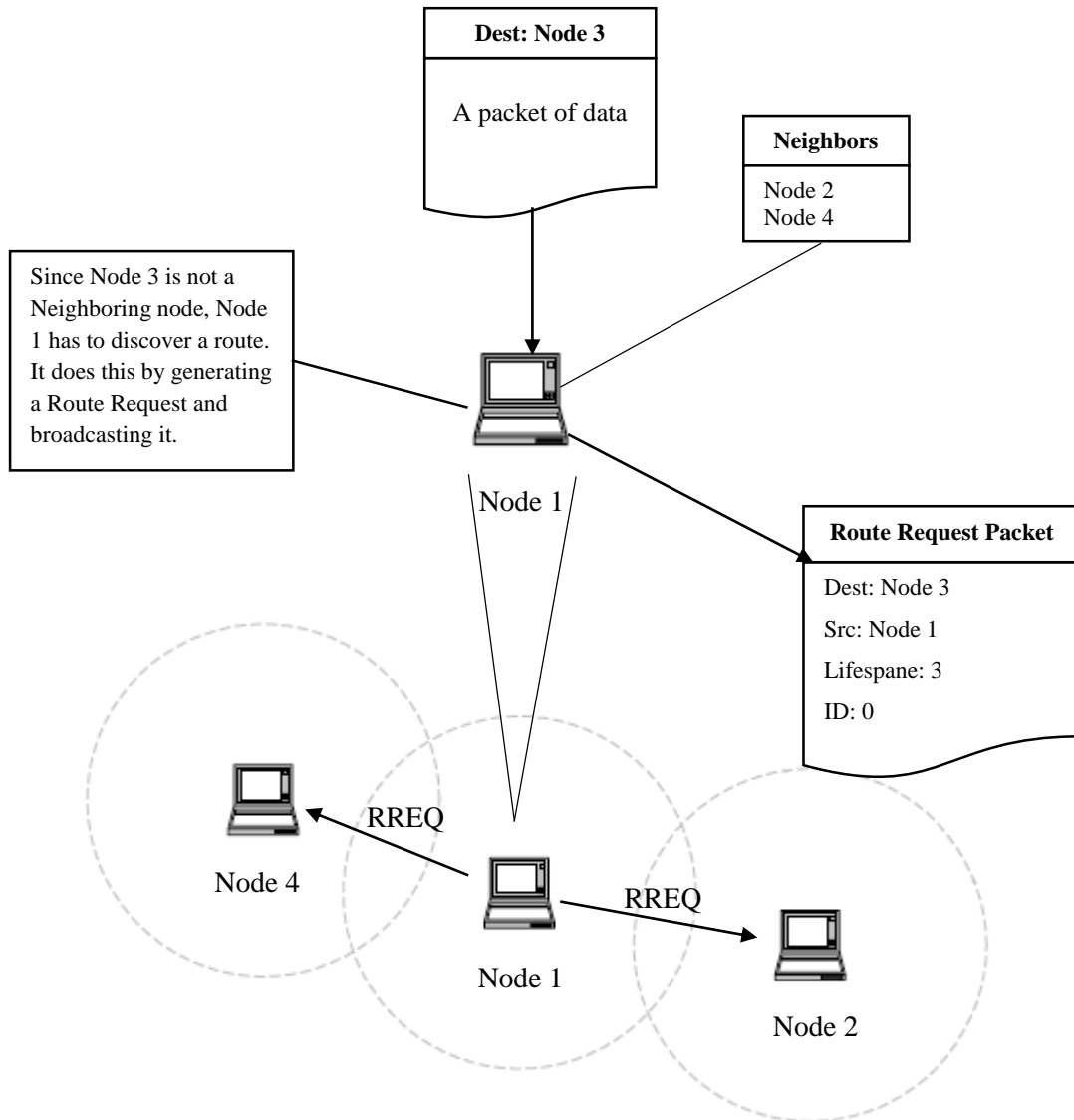


Figure 1.8 Working Mechanism of RREQ Messages

After a node receives a RREQ and responds with a RREP, it discards the RREQ. If the RREQ has the 'G' flag set, and the intermediate node returns a RREP to the originating node, it MUST also unicast a gratuitous RREP to the destination node. The Figure 1.9 summarizes what was explained about RREP messages.

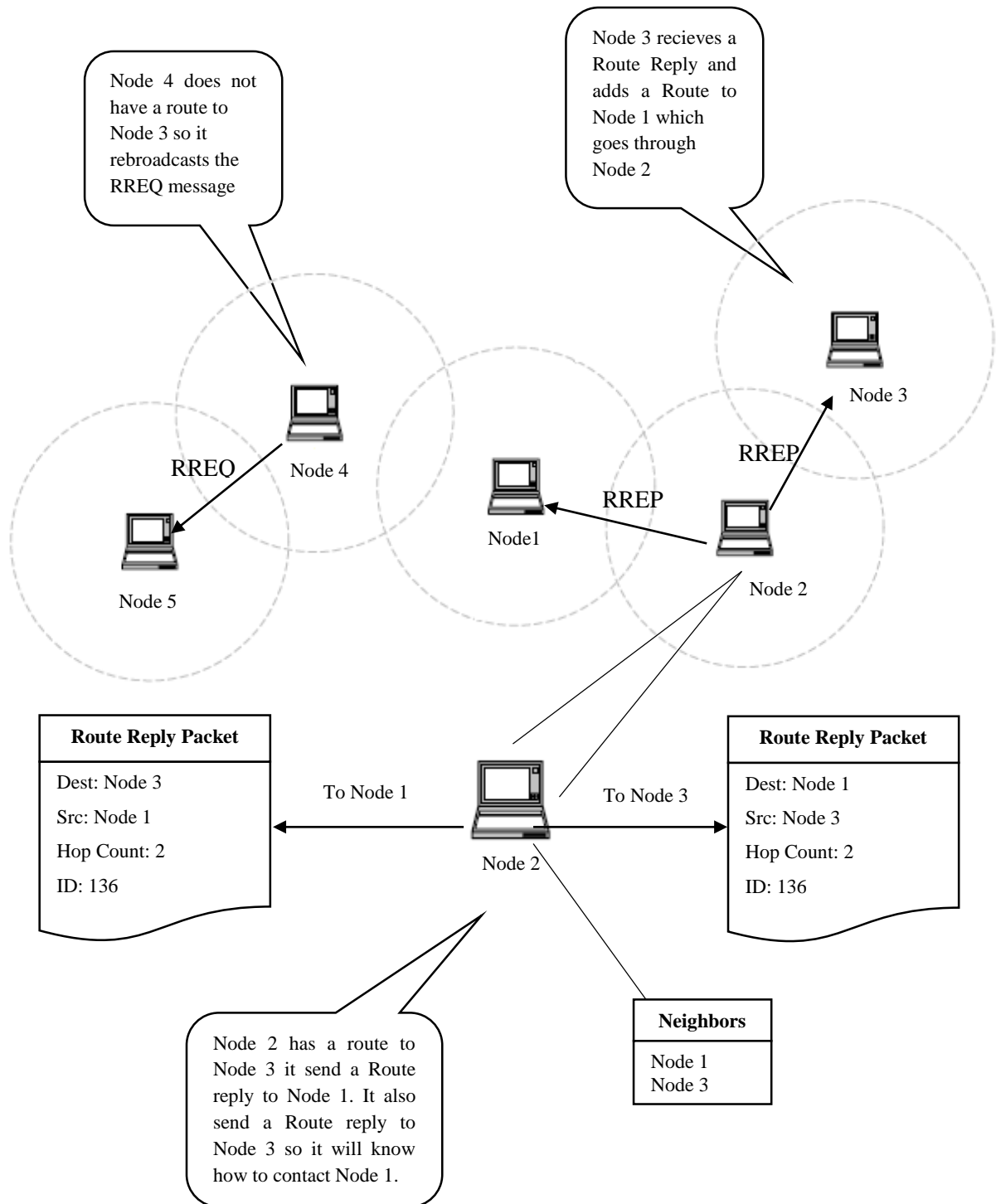
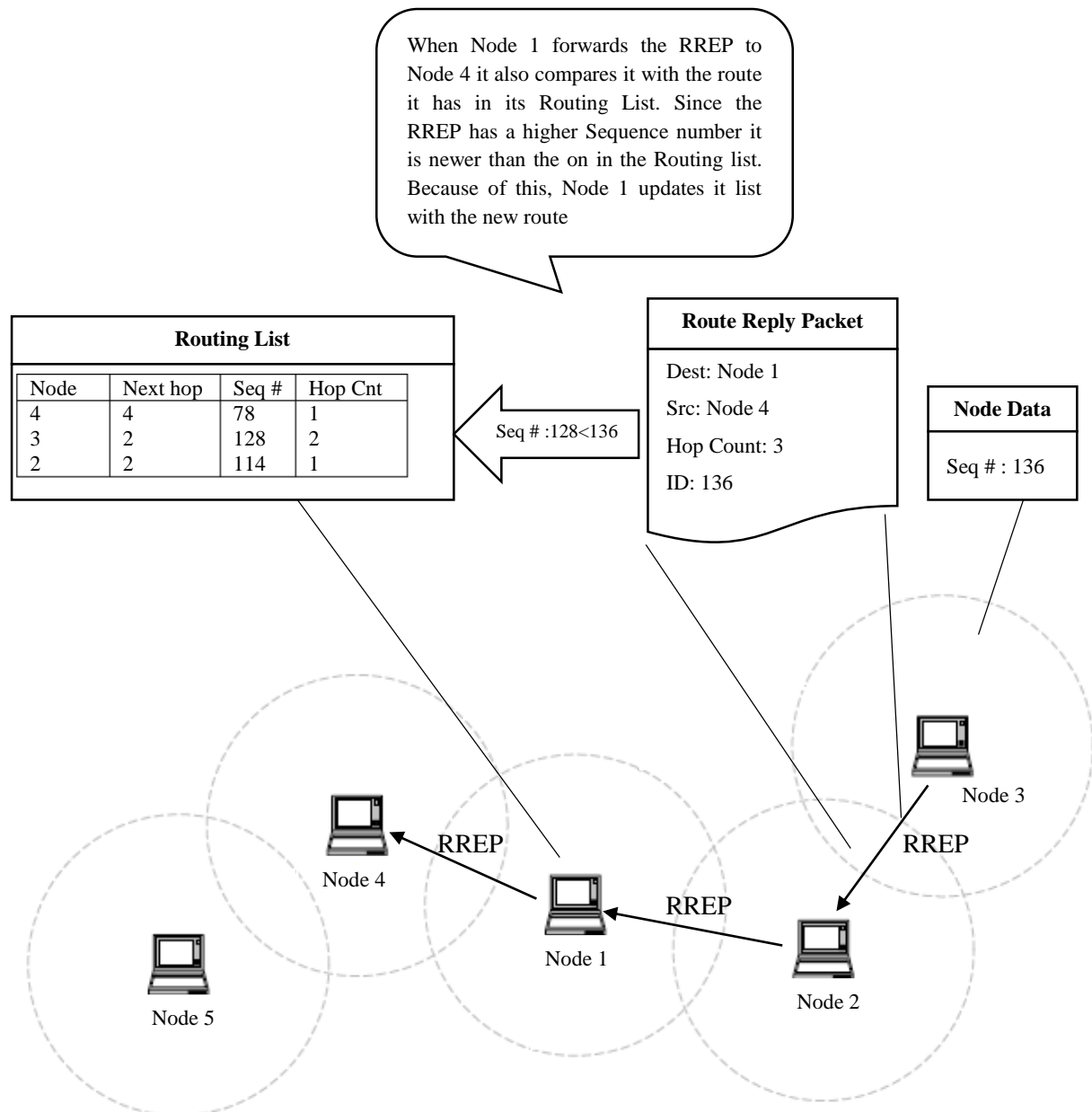


Figure 1.9 Generating Route Replies Messages

**Figure 1.10** Maintaining Sequence Numbers

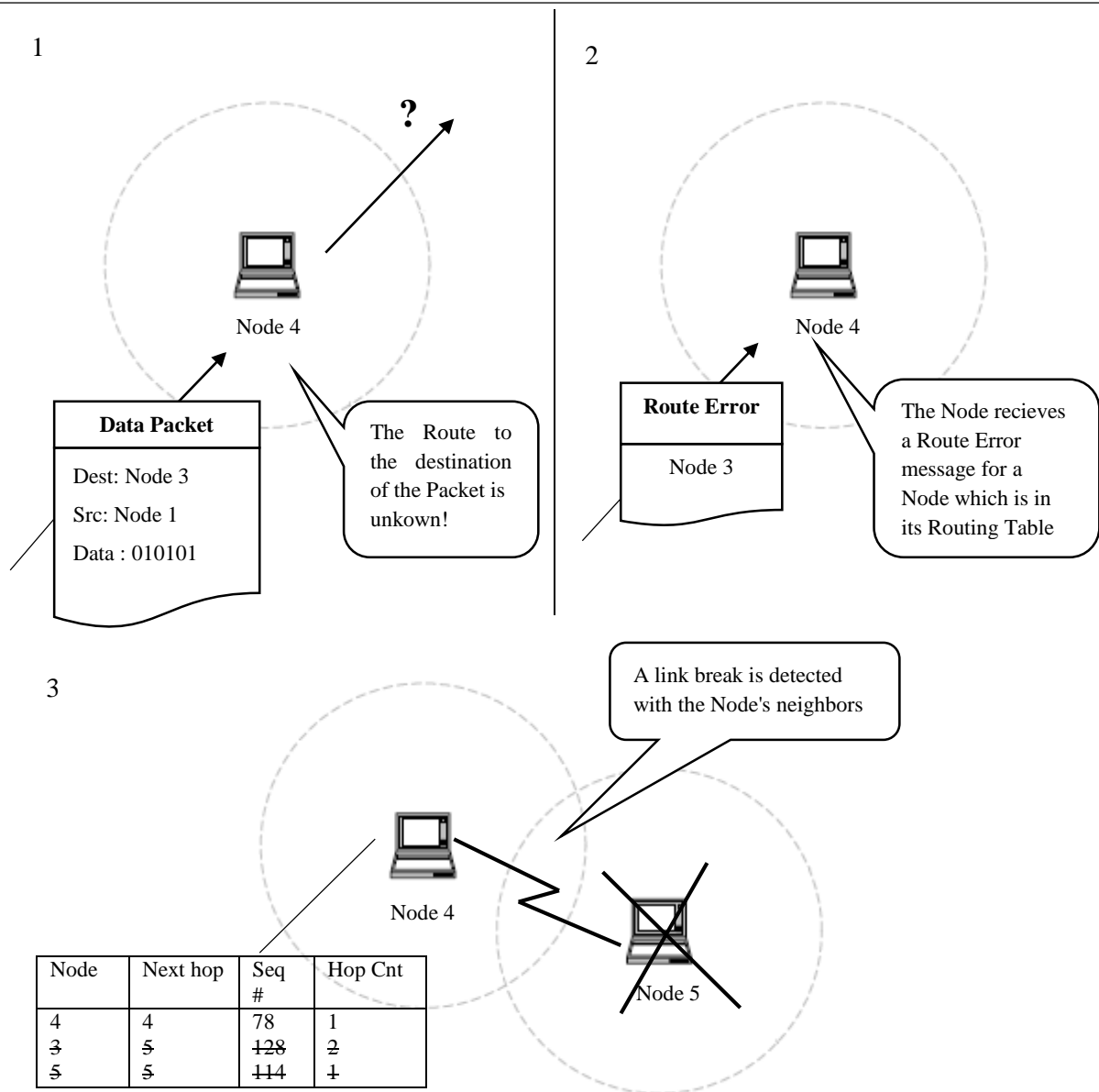


Figure 1.11 Situations of Broadcast the RERR Messages

1.11 Conclusion

This chapter gave an overview of Mobile Ad-Hoc Networks and the main objectives were to outline the fundamentals of mobile ad hoc networks technology by highlighting the principle characteristics, applications, and Routing in MANET. Then the working of aodv protocol was explained. One the most important points when designing a routing protocol is to define an efficient route failure recovery strategy. AODV routing protocol uses an innovative mechanism to deal with route failures. It uses a local route repair approach when the upstream node is close to the destination rather than the source node. Otherwise, it simply apply a new route discovery phase as described above. The following chapter has a strong relationship with link breakage, “The Link failure Prediction”, it’s the core of explanation and discussion in the next chapter.