Chapter 4
Routing in Mobile Ad Hoc Networks

Al-Sakib Khan Pathan and Choong Seon Hong

Abstract A Mobile Ad Hoc Network (MANET) is built on the fly where a number of wireless mobile nodes work in cooperation without the engagement of any centralized access point or any fixed infrastructure. Two nodes in such a network can communicate in a bidirectional manner if and only if the distance between them is at most the minimum of their transmission ranges. When a node wants to communicate with a node outside its transmission range, a multihop routing strategy is used which involves some intermediate nodes. Because of the movements of nodes, there is a constant possibility of topology change in MANET. Considering this unique aspect of MANET, a number of routing protocols have been proposed so far. This chapter gives an overview of the past, current, and future research areas for routing in MANET. In this chapter we will learn about the following things:

- The preliminaries of mobile ad hoc network
- The challenges for routing in MANET
- Expected properties of a MANET routing protocol
- Categories of routing protocols for MANET
- Major routing protocols for MANET
- Criteria for performance comparison of the routing protocols for MANET
- Achievements and future research directions
- Expectations and reality

4.1 Introduction

With the staggering growth of wireless handheld devices and plummeting costs of mobile telecommunications, mobile ad hoc network has emerged as a major area of research for both the academic and the industrial sectors. A mobile ad

A.-S.K. Pathan (✉)
Department of Computer Engineering, Kyung Hee University, 1 Seocheon, Giheung, Yongin, Gyeonggi 449701, Korea
e-mail: spathan@networking.khu.ac.kr, pathan_sakib@yahoo.com

S. Misra et al. (eds.), *Guide to Wireless Ad Hoc Networks*,
Computer Communications and Networks, DOI 10.1007/978-1-84800-328-6_4,

hoc network (MANET) is built on the fly where a number of mobile nodes work in cooperation without the engagement of any centralized access point or any fixed infrastructure. MANETs are self-organizing, self-configuring, and dynamic topology networks, which form a particular class of multi-hop networks. Minimal configuration, absence of infrastructure, and quick deployment make them convenient for combat, medical, and other emergency situations. All nodes in a MANET are capable of movement and can be interconnected in an arbitrary manner.

The issue of routing in MANET is somewhat challenging and non-trivial. Due to the mobility of the nodes, connectivity between any two nodes in the network is considered intermittent and often it is very difficult, if not impossible to use traditional wired network's routing mechanisms. Basically, the major challenges for routing in MANET are imposed by the resource constraints and mobility of the nodes participating in the network. As there is no fixed infrastructure in such a network, we consider each node as a host and a router at the same time. Hence, during routing of data packets within the network, at each hop, each host also has to perform the tasks of a router. In fact, these special aspects of mobile ad hoc networks have attracted many researchers to work on solving the routing issues in MANET. A sample model of mobile ad hoc network is presented here in Fig. 4.1, which consists of some mobile devices with wireless communication facilities.

So far, a significant number of proposals for routing in MANET have seen the daylight. However, it is apparent that there could not be a single solution for routing in MANETs. Different deployment scenarios and application-dependent requirements need the employment of different types of routing mechanisms. In this chapter, we will learn about the routing protocols for MANET, their features, advantages, drawbacks, and future expectations.

Let us start this chapter with a brief background of MANET. We will know about how the practitioners, researchers, scientists, and industrialists have tried

Fig. 4.1. An Example of Mobile Ad Hoc Network (MANET)

to solve this challenging issue for MANET. We will know various types of routing schemes those are already proposed or those could be applied for these types of networks. Considering the practical scenarios, we will also discuss how the reality might betray the expectations.

4.2 Background

From the advent of packet radio network up to today's MANET, the whole life cycle of ad hoc networks can be categorized mainly into three parts: first generation, second generation, and third generation. Today's ad hoc networks are considered as the third-generation networks.

The first generation goes back to 1972. At that time, they were called PRNET (Packet Radio Networks). In 1973, the Defense Advanced Research Projects Agency (DARPA) initiated research on the feasibility of using packet-switched radio communications to provide reliable computer communications [1, 2]. This development was motivated by the need to provide computer network access to mobile hosts and terminals, and to provide computer communications in a mobile environment.

The second generation of ad hoc networks emerged in 1980s, when the ad hoc network systems were further enhanced and implemented as a part of the SURAN (Survivable Adaptive Radio Networks) program [3]. This provided a packet-switched network to the mobile battlefield in an environment without infrastructure. This program proved to be beneficial in improving the radio performance by making them smaller, cheaper, and resilient to electronic attacks.

In the 1990s, the concept of commercial ad hoc networks arrived with handheld computers and other small portable communication equipments. At the same time, the idea of a collection of mobile nodes was proposed at several research conferences. From then up to today, research works have been going on for solving various issues of mobile ad hoc networks.

We mentioned the formal definition of a mobile ad hoc network earlier. Let us investigate how the unique characteristics of MANET make the task of routing complicated. So far we have learnt that the major features of this type of network are each node is considered both as a host and as a router; the nodes in the network are allowed to move while participating in the network; for their connectivity they use wireless communications; there is no centralized entity in the network; and the nodes are mainly battery-powered. Now, let us consider the following network structure for starting our discussion on routing in MANET.

Example 4.1 In Fig. 4.2, a sample model of MANET is presented where there are three nodes; A, B, and C. The radio transmission ranges of the nodes are shown as circles.

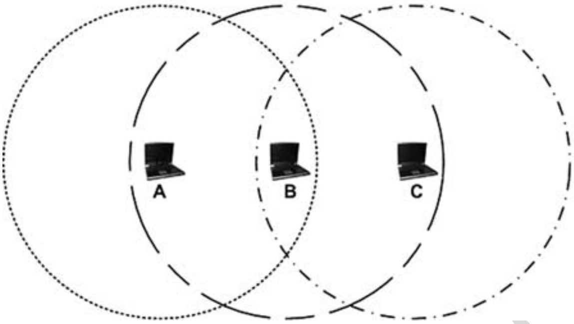


Fig. 4. 2 A MANET with three nodes

In the figure, node A and node B are within the transmission ranges of each other. We call any of these nodes as a neighbor of the other. Likewise, B and C are neighbors. But, A and C are not neighbors as none of their transmission ranges covers other node. In this setting, the neighbors can communicate directly and no routing is required. But, if node A and C want to communicate with each other, they must seek help from node B, who can help them by forwarding their data packets. Here, we can reach this decision that it is quite natural. Yes, it could be done as node A knows about B and C knows about B, so both A and C can use B as an intermediate node for their communications! Simple neighbor information could be used in such a case.

Example 4.2 Now, the task of routing data packets becomes more complicated if we consider a model like that presented in Fig. 4.3.

With the addition of node D, we have several options to exchange data between A and C. For example, a packet from A can take the path, A-B-C or A-D-C or A-D-B-C or A-B-D-C. This is where we need to employ efficient mechanism or logic for routing the packet in the best possible way. The whole

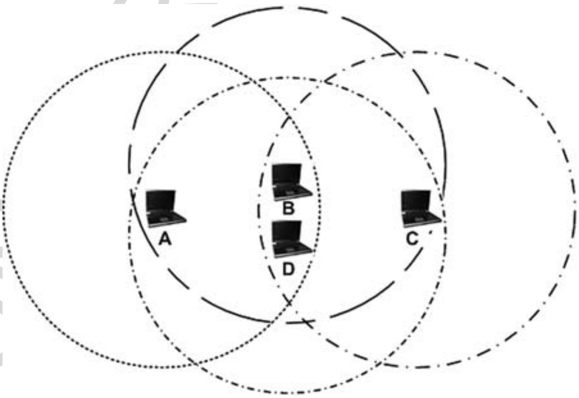


Fig. 4. 3 A MANET with four nodes

scenario gets even more complicated with the increase of the number of nodes in the network. If two nodes are far from each other and if they must have to communicate using a path involving multiple intermediate nodes, in that case, neighbor information might not be enough to solve the problem. Even if neighbor information is used, it is not possible or inefficient for a MANET to provide the full topological information to each node in the network. Because of the mobility of nodes within the network, the scenario becomes more and more complex. Hence, to allow a MANET to operate successfully maintaining all the properties of ad hoc networks, different routing protocols were developed by the practitioners. Sometimes, choosing a single routing protocol does not provide the complete solution, rather the system and environment settings require different approaches of routing. As we have seen in Figs. 4.2 and 4.3, based on the situation we can apply different routing mechanisms. While only neighbor information is enough for solving the routing problem in Fig. 4.2, some extra mechanism is necessary for efficient routing in case of Fig. 4.3.

4.3 Routing Protocols

From the very beginning of the concept of mobile ad hoc network, the researchers took the issue of routing as a major challenge. With the course of time, many routing protocols have been proposed. In this section, we will learn about various routing protocols for MANET, their major aspects, and their relative pros and cons.

4.3.1 Expected Properties of MANET Routing Protocols

Considering the special properties of MANET, when thinking about any routing protocol, we generally expect the following properties, though all of these might not be possible to incorporate in a single solution:

- A routing protocol for MANET should be distributed in manner in order to increase its reliability. Where all nodes are mobile, it is unacceptable to have a routing protocol that requires a centralized entity. Each node should be intelligent enough to make routing decisions using other collaborating nodes. A distributed but virtually centralized protocol might be a good idea.
- The routing protocol should assume routes as unidirectional links. Wireless medium may cause a wireless link to be opened in unidirection only due to physical factors. It may not be possible to communicate bidirectionally. Thus a routing protocol must be designed considering unidirectional links.
- The routing protocol should be power-efficient. It should consider every possible measure to save power, as power is very important for small battery-powered devices. To save power, the routing-related loads could be distributed among the participating nodes.

- The routing protocol should consider its security. MANET routing protocols in many cases lack proper security. Generally, a wireless medium is highly vulnerable and susceptible to various sorts of threats and attacks. Because of the use of wireless technology in MANETs, the methods of attacks against such networks are larger in scale than those of their wired counterparts [4, 5]. At physical layer, denial of service attacks may be avoided using coded or frequency hopping spread spectrum; however, at routing level, we need authentication for communicating nodes, non-repudiation, and encryption for private networking to shun hostile entities.
- Hybrid protocols, which combine the benefits of different routing protocols can be preferred in most of the cases. A protocol should be much more reactive (which reacts on demand) than proactive (which uses periodic refreshment of information) to avoid protocol overhead.
- A routing protocol should be aware of Quality of Service (QoS). It should know about the delay and throughput for the route of a source–destination pair, and must be able to verify its longevity so that a real-time application may rely on it.

4.3.2 Categorizing the Routing Protocols for MANET

One of the most interesting aspects for routing in MANET, which many research works have tried to solve is, whether or not the nodes in the network should keep track of routes to all possible destinations, or instead keep track of only those destinations of immediate interest. Generally, a node in MANET does not need a route to a destination until the node is necessarily be the recipient of packets, either as the final destination or as an intermediate node along the path from the source to the destination. As this is still a controversial issue, we can assume that the mechanism should not be fixed for all types of settings, instead based on the situation and application at hand, any of the methods could be chosen.

Though there is no common consensus about the method of keeping the information about routes in the network, many routing protocols have been proposed by this time on the basis of all the available methods. The routing protocols for MANET could be broadly classified into two major categories:

- Proactive Routing Protocols
- Reactive Routing Protocols

4.3.2.1 Proactive Routing Protocols

Proactive protocols continuously learn the topology of the network by exchanging topological information among the network nodes. Thus, when there is a need for a route to a destination, such route information is available immediately. The main concern regarding using a proactive routing protocol is: if the network topology changes too frequently, the cost of maintaining the network might be very high. Moreover, if the network activity is low, the information about the actual topology might even not be used and, in such a case, the investment with such limited transmission ranges and energies is lost, which might result in a shorter lifetime of the network than that is expected. Proactive protocols are sometimes called as table-driven routing protocols.

4.3.2.2 Reactive Routing Protocols

The reactive routing protocols, on the other hand, are based on some sort of *query-reply* dialog. Reactive protocols proceed for establishing route(s) to the destination only when the need arises or on demand basis. They do not need periodic transmission of topological information of the network; hence, they primarily seem to be resource-conserving protocols. Reactive protocols are also known as on-demand routing protocols.

4.3.2.3 Hybrid Routing Protocols

Often reactive or proactive feature of a particular routing protocol might not be enough; instead a mixture might yield better solution. Hence, in the recent days, several hybrid protocols are also proposed. The hybrid protocols include some of the characteristics of proactive protocols and some of the characteristics of reactive protocols.

Based on the method of delivery of data packets from the source to destination, classification of the MANET routing protocols could be done as follows:

- *Unicast Routing Protocols*: The routing protocols that consider sending information packets to a single destination from a single source.
- *Multicast Routing Protocols*: Multicast is the delivery of information to a group of destinations simultaneously, using the most efficient strategy to deliver the messages over each link of the network only once, creating copies only when the links to the destinations split. Multicast routing protocols for MANET use both multicast and unicast for data transmission.

Multicast routing protocols for MANET can be classified again into two categories:

- Tree-based multicast protocol
- Mesh-based multicast protocol

Mesh-based routing protocols use several routes to reach a destination while the tree-based protocols maintain only one path. Tree-based protocols ensure less end-to-end delay in comparison with the mesh-based protocols. Besides all of these categories, recently some geocast [6] routing protocols are also proposed, which aim to send messages to some or all of the wireless nodes within a particular geographic region. Often the nodes know their exact physical positions in a network, and these protocols use that information for transmitting packets from the source to the destination(s).

4.3.3 Proposed Routing Protocols: Major Features

In this section, we will investigate the major routing protocols for MANET. We will explore their distinctive features with easily understandable examples wherever necessary.

4.3.3.1 Proactive Routing Protocols

Dynamic Destination-Sequenced Distance-Vector Routing Protocol

Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV) [7] is developed on the basis of Bellman–Ford routing [8] algorithm with some modifications. In this routing protocol, each mobile node in the network keeps a routing table. Each of the routing table contains the list of all available destinations and the number of hops to each. Each table entry is tagged with a sequence number, which is originated by the destination node. Periodic transmissions of updates of the routing tables help maintaining the topology information of the network. If there is any new significant change for the routing information, the updates are transmitted immediately. So, the routing information updates might either be periodic or event-driven. DSDV protocol requires each mobile node in the network to advertise its own routing table to its current neighbors. The advertisement is done either by broadcasting or by multicasting. By the advertisements, the neighboring nodes can know about any change that has occurred in the network due to the movements of nodes.

The routing updates could be sent in two ways: one is called a "*full dump*" and another is "*incremental*." In case of *full dump*, the entire routing table is sent to the neighbors, whereas in case of *incremental* update, only the entries that require changes are sent. Full dump is transmitted relatively infrequently when no movement of nodes occur. The incremental updates could be more appropriate when the network is relatively stable so that extra traffic could be avoided. But, when the movements of nodes become frequent, the sizes of the incremental updates become large and approach the network protocol data unit (NPDU). Hence, in such a case, full dump could be used. Each of the route update packets also has a sequence number assigned by the transmitter. For updating the routing information in a node, the update packet with the highest sequence number is used, as the highest number means the most recent update packet. Each node waits up to certain time interval to transmit the advertisement message to its neighbors so that the latest information with better route to a destination could be informed to the neighbors. Let us explain DSDV routing protocol with an example.

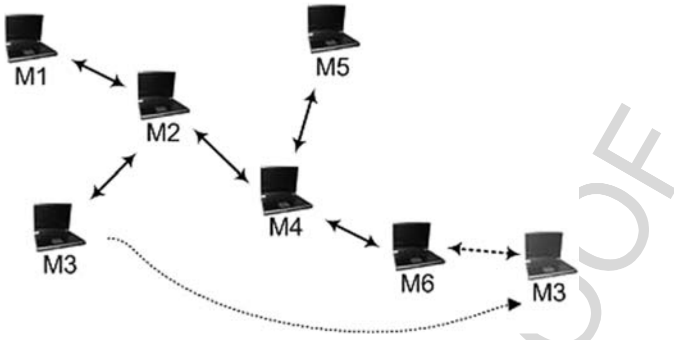


Fig. 4.4 A sample MANET using DSDV

Example 4.3 Figure 4.4 shows a sample network consisting of six mobile nodes. Table 1.1 shows a sample structure of the forwarding table maintained in node M2. The *Install* time field helps determine when to delete a stale route. As in DSDV, any change in the routing path is immediately propagated throughout the network, it is very rare that deletion of stale routes occur. The *Stable_data* field contains the pointers that are needed to be stored when there is a competition with other possible routes to any particular destination. Table 1.2 shows a sample advertisement table of node M2 using DSDV.

Now, in Fig. 4.4, if a node, say M3, moves close to M6, only the entry for M3 needs to be changed. After some time M2 will get the information of M3 from M4, as M4 will get the information about M3 from M6, and accordingly M2 can adjust the entry for M3 in its own routing (forwarding) table. If M3 quits the network after some time interval, its entry will be deleted from M2's routing table.

Wireless Routing Protocol

Wireless Routing Protocol (WRP) [9] belongs to the general class of path-finding algorithms [8, 10, 11], defined as the set of distributed shortest-path algorithms that calculate the paths using information regarding the length and second-to-last hop of the shortest path to each destination. WRP reduces the number of cases in

Table 1.1 Structure of node M2's forwarding table

Destination	Next Hop	Metric	Sequence Number	Install	Flags	Stable_data
M1	M1	1	S593_M1	T001_M2	–	Ptrl_M1
M2	M2	0	S983_M2	T001_M2	–	Ptrl_M2
M3	M3	1	S193_M3	T002_M2	–	Ptrl_M3
M4	M4	1	S233_M4	T001_M2	–	Ptrl_M4
M5	M4	2	S243_M5	T001_M2	–	Ptrl_M5
M6	M4	2	S053_M6	T002_M2	–	Ptrl_M6

Table 1.2 Route table advertised by node M2

Destination	Metric	Sequence Number
M1	1	S593_M1
M2	0	S983_M2
M3	1	S193_M3
M4	1	S233_M4
M5	2	S243_M5
M6	2	S053_M6

which a temporary routing loop can occur. For the purpose of routing, each node maintains four things:

1. A distance table
2. A routing table
3. A link-cost table
4. A message retransmission list (MRL)

The distance table of node *x* contains the distance of each destination node *y* via each neighbor *z* of *x* and the predecessor node reported by *z*. The routing table of node *x* is a vector with an entry for each known destination *y*, which specifies:

- The identifier of the destination *y*
- The distance to the destination *y*
- The predecessor of the chosen shortest path to *y*
- The successor of the chosen shortest path to *y*
- A tag to identify whether the entry is a simple path, a loop, or invalid
- Storing predecessor and successor in the table is beneficial to detect loops and to avoid count-to-infinity problems.

The link-cost table of node *x* lists the cost of relaying information through each neighbor *z*, and the number of periodic update periods that have elapsed since node *x* received any error-free message from *z*. The message retransmission list (MRL) contains information to let a node know which of its neighbors has not acknowledged its update message and to retransmit the update message to that neighbor.

WRP uses periodic update message transmissions to the neighbors of a node. The nodes in the response list of update message (which is formed using MRL) should send acknowledgments. If there is no change from the last update, the nodes in the response list should send an *idle Hello* message to ensure connectivity. A node can decide whether to update its routing table after receiving an update message from a neighbor and always it looks for a better path using the new information. If a node gets a better path, it relays back that information to the original nodes so that they can update their tables. After receiving the acknowledgment, the original node updates its MRL. Thus, each time the consistency of the routing information is checked by each node in this protocol, which helps to eliminate routing loops and always tries to find out the best solution for routing in the network.

Cluster Gateway Switch Routing Protocol

Cluster Gateway Switch Routing Protocol (CGSR) [12] considers a clustered mobile wireless network instead of a "*flat*" network. For structuring the network into separate but interrelated groups, cluster heads are elected using a cluster head selection algorithm. By forming several clusters, this protocol achieves a distributed processing mechanism in the network. However, one drawback of this protocol is that, frequent change or selection of cluster heads might be resource hungry and it might affect the routing performance. CGSR uses DSDV protocol as the underlying routing scheme and, hence, it has the same overhead as DSDV. However, it modifies DSDV by using a hierarchical cluster-head-to-gateway routing approach to route traffic from source to destination. Gateway nodes are nodes that are within the communication ranges of two or more cluster heads. A packet sent by a node is first sent to its cluster head, and then the packet is sent from the cluster head to a gateway to another cluster head, and so on until the cluster head of the destination node is reached. The packet is then transmitted to the destination from its own cluster head.

Example 4.4 Figure 4.5 shows two clusters C1 and C2 each of which has a cluster head. A gateway is the common node between two clusters. Any source node passes the packet first to its own cluster head, which in turn passes that to the gateway.

The gateway relays the packet to another cluster head and this process continues until the destination is reached. In this method, each node must keep a "*cluster member table*" where it stores the destination cluster head for each mobile node in the network. These cluster member tables are broadcasted by each node periodically using the DSDV algorithm. Nodes update their

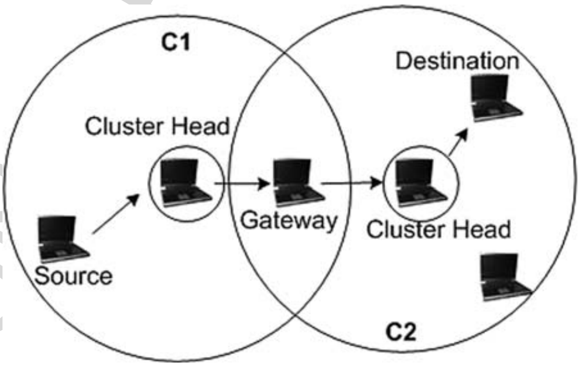


Fig. 4.5 Clustered MANET

cluster member tables on reception of such a table from a neighbor. Also each node maintains a routing table that is used to determine the next hop to reach the destination.

Global State Routing

In Global State Routing (GSR) protocol [13], nodes exchange vectors of link states among their neighbors during routing information exchange. Based on the link state vectors, nodes maintain a global knowledge of the network topology and optimize their routing decisions locally. Functionally, this protocol is similar to DSDV, but it improves DSDV in the sense that it avoids flooding of routing messages. In this protocol, each node maintains one list and three tables. They are:

- A neighbor list
- A topology table
- A next hop table
- A distance table

Neighbor list contains the set of neighboring nodes of a particular node x. Each destination y has an entry in the topology table of x. Each entry in this topology table has two parts, one is the link state information reported by destination y and the other is the timestamp indicating the time node y has generated this link state information. Next hop contains the identity of the next hop node, to which a packet is to be forwarded to reach a particular destination. The distance table contains the shortest distance between x and y.

Though the operational structure of GSR is similar to DSDV, it does not flood the link state packets. Instead, in this protocol nodes maintain link state table based on the up-to-date information received from neighboring nodes, and periodically exchange it with their local neighbors only. Information disseminated as the link state with larger sequence number replaces the one with smaller sequence number.

Fisheye State Routing

Fisheye State Routing (FSR) [14] is built on top of GSR. The novelty of FSR is that it uses a special structure of the network called the "*fisheye*." This protocol reduces the amount of traffic for transmitting the update messages. The basic idea is that each update message does not contain information about all nodes. Instead, it contains update information about the nearer nodes more frequently than that of the farther nodes. Hence, each node can have accurate and exact information about its own neighboring nodes. The following example explains the fisheye state routing protocol.

Example 4.5 In FSR, the network is viewed as a fisheye by each participating node. An example of this special structure is shown in Fig. 4.6.

Here, the *scope* of fisheye is defined as the set of nodes that can be reached within a given number of hops from a particular center node. In the figure, we

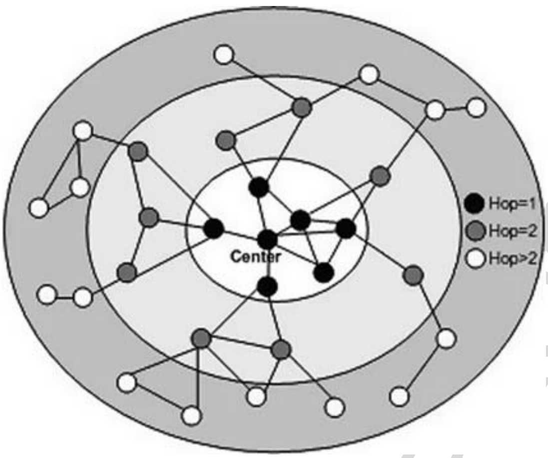


Fig. 4.6 Fisheye structure

have shown three scopes with one, two, and three hops. The center node has the most accurate information about all nodes in the white circle and so on. Each circle contains the nodes of a particular hop from a center node. The advantage of FSR is that, even if a node does not have accurate information about a destination, as the packet moves closer to the destination, more correct information about the route to the destination becomes available.

Hierarchical State Routing

Hierarchical State Routing (HSR) [14] combines dynamic, distributed multilevel hierarchical clustering technique with an efficient location management scheme. This protocol partitions the network into several clusters where each elected cluster head at the lower level in the hierarchy becomes member of the next higher level. The basic idea of HSR is that each cluster head summarizes its own cluster information and passes it to the neighboring cluster heads using gateways. After running the algorithm at any level, any node can flood the obtained information to its lower level nodes. The hierarchical structure used in this protocol is efficient enough to deliver data successfully to any part of the network.

Example 4.6 Figure 4.7 shows the clustering and hierarchy used in HSR. Here, each node has a hierarchical address by which it could be reached. A gateway can be reached from the root via more than one path; hence it can have more than one hierarchical address.

Zone-Based Hierarchical Link State Routing Protocol

In Zone-Based Hierarchical Link State Routing (ZHLS) protocol [15], the network is divided into non-overlapping zones as in cellular networks. Each node knows the node connectivity within its own zone and the zone connectivity

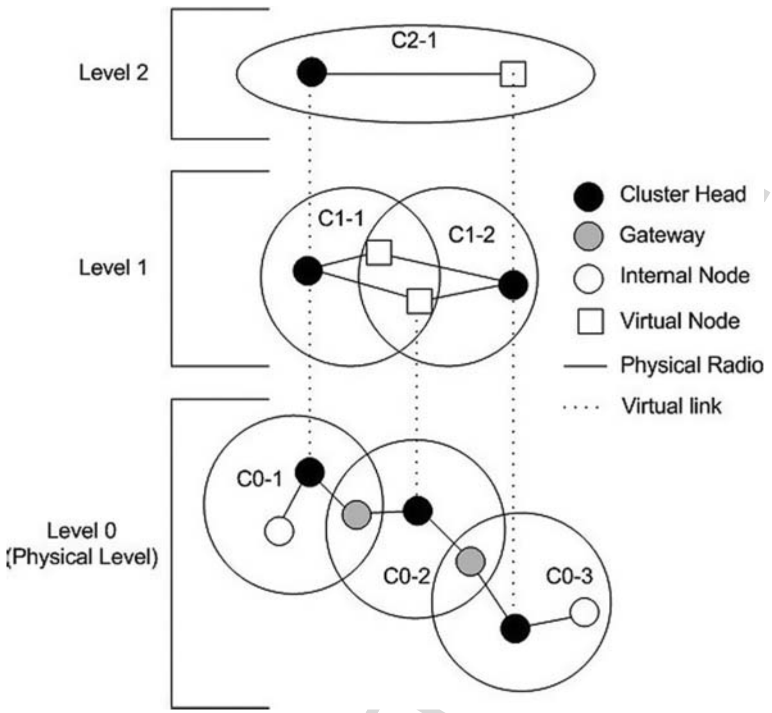


Fig. 4.7 Clustering and hierarchical structure used in HSR

information of the entire network. The link state routing is performed by employing two levels: node level and global zone level. ZHLS does not have any cluster head in the network like other hierarchical routing protocols. The zone level topological information is distributed to all nodes. Since only zone ID and node ID of a destination are needed for routing, the route from a source to a destination is adaptable to changing topology. The zone ID of the destination is found by sending one *location request* to every zone.

Landmark Ad Hoc Routing

Landmark Ad Hoc Routing (LANMAR) [16] combines the features of Fisheye State Routing (FSR) and Landmark Routing [17]. It uses the concept of *landmark* from Landmark Routing, which was originally developed for fixed wide area networks. A *landmark* is defined as a router whose neighbor routers within a certain number of hops contain routing entries for that router. Using this concept for the nodes in the MANET, LANMAR divides the network into several pre-defined logical subnets, each with a pre-selected *landmark*. All nodes in a subnet are assumed to move as a group, and they remain connected to each other via Fisheye State Routing (FSR). The routes to the landmarks, and hence the corresponding subnets, are proactively maintained by all nodes in the network through the exchange of distance-vectors. LANMAR could be regarded as an extension of FSR, which exploits group mobility by *summarizing* the routes to the group members with a single route to a *landmark*.

Optimized Link State Routing

Optimized Link State Routing (OLSR) [18] protocol inherits the stability of link state algorithm. Usually, in a pure link state protocol, all the links with neighbor nodes are declared and are flooded in the entire network. But, OLSR is an optimized version of a pure link state protocol designed for MANET. This protocol performs hop-by-hop routing; that is, each node in the network uses its most recent information to route a packet. Hence, even when a node is moving, its packets can be successfully delivered to it, if its speed is such that its movements could at least be followed in its neighborhood. The optimization in the routing is done mainly in two ways. Firstly, OLSR reduces the size of the control packets for a particular node by declaring only a subset of links with the node's neighbors who are its *multipoint relay selectors*, instead of all links in the network. Secondly, it minimizes flooding of the control traffic by using only the selected nodes, called *multipoint relays* to disseminate information in the network. As only multipoint relays of a node can retransmit its broadcast messages, this protocol significantly reduces the number of retransmissions in a flooding or broadcast procedure.

Example 4.7 Figure 4.8 shows a sample network structure used in OLSR. OLSR protocol relies on the selection of multipoint relay (MPR) nodes.

Each node calculates the routes to all known destinations through these nodes. These MPRs are selected among the one hop neighborhood of a node using the bidirectional links, and they are used to minimize the amount of broadcast traffic in the network.

4.3.3.2 Reactive Routing Protocols

All of the protocols mentioned in the previous section use periodic transmissions of routing information. In this section, we will investigate the working principles of some reactive routing protocols for mobile ad hoc networks. As stated earlier, unlike proactive protocols, reactive protocols proceed for finding a route to a destination only when a source node needs to transmit data to another node in the network.

Associativity-Based Routing

Associativity-Based Routing (ABR) [19] protocol defines a new type of routing metric for mobile ad hoc networks. This routing metric is termed as *degree of association stability*. In this routing protocol, a route is selected based on the

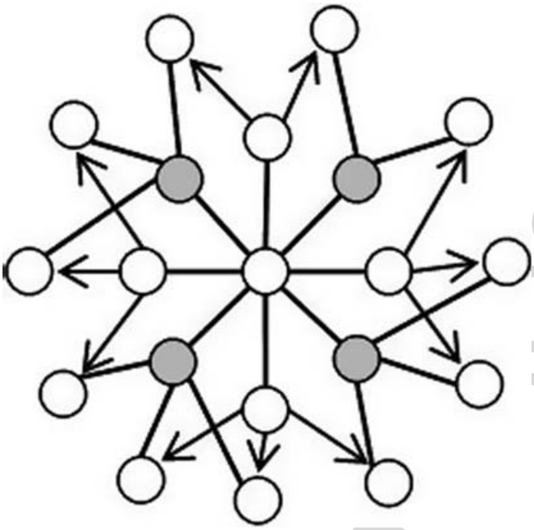


Fig. 4.8 Multipoint Relays (MPRs) are in gray color. The transmitting node is shown at the center of the sample structure

degree of association stability of mobile nodes. Each node periodically generates *beacon* to announce its existence. Upon receiving the beacon message, a neighbor node updates its own associativity table. For each beacon received, the associativity tick of the receiving node with the beaconing node is increased. A high value of associativity tick for any particular beaconing node means that the node is relatively static. Associativity tick is reset when any neighboring node moves out of the neighborhood of any other node. ABR protocol has three phases for the routing operations:

- Route discovery
- Route reconstruction
- Route deletion

The route discovery phase is done by a broadcast query and await-reply (BQ-REPLY) cycle. When a source node wants to send message to a destination, it sends the query. All other nodes receiving the query append their addresses and their associativity ticks with their neighbors along with QoS information to the query packet. A downstream node erases its immediate upstream node's associativity tick entries and retains only the entry concerned with itself and its upstream node. This process continues and eventually the packet reaches the destination. On receiving the packet with the associativity information, the destination chooses the best route and sends the REPLY packet using that path. If there are multiple paths with same overall degree of association stability, the route with the minimum number of hops is selected. Route reconstruction is needed when any path becomes invalid or broken for the mobility or failure of any intermediate node. If a source or upstream node moves, a route

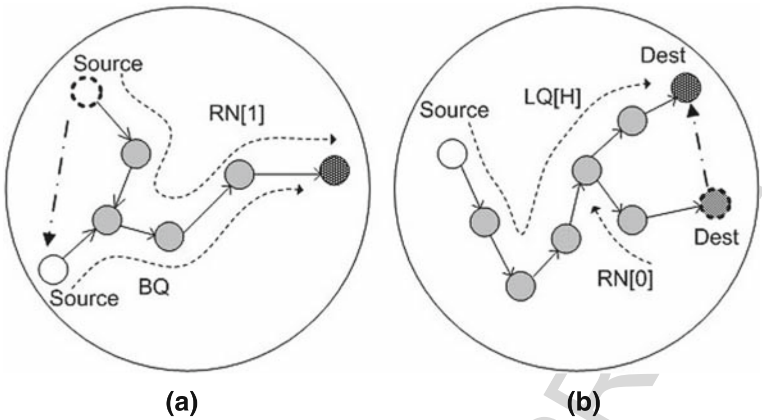


Fig. 4. 9 Route maintenance in ABR for two different scenarios

notification (RN) message is used to erase the route entries associated with downstream nodes. When the destination node moves, the destination's immediate upstream node erases its route. A localized query (LQ[H]) process, where H refers to the hop count from the upstream node to the destination, is initiated to determine whether the node is still reachable or not. Route deletion broadcast is done if any discovered route is no longer needed. Figure 4.9 shows the working principle of ABR protocol.

Example 4.8 Figure 4.9 shows two different scenarios for route maintenance where ABR is used. In Figure 4.9(a), the source moves to another place, as a result of which a new BQ request is used to find out the route to the destination. The RN [1] message is used to erase the route entries associated with the downstream nodes. In Figure 4.9(b), the destination changed its position. Hence, immediate upstream node erases its route and determines if the node is still reachable by a localized query (LQ[H]) process.

Signal Stability–Based Adaptive Routing Protocol

Signal Stability–Based Adaptive Routing (SSA) [20] protocol focuses on obtaining the most stable routes through an ad hoc network. The protocol performs on-demand route discovery based on signal strength and location stability. Based on the signal strength, SSA detects weak and strong channels in the network. SSA can be divided into two cooperative protocols: the Dynamic Routing Protocol (DRP) and the Static Routing Protocol (SRP). DRP uses two tables: Signal Stability Table (SST) and Routing Table (RT). SST stores the signal strengths of the neighboring nodes obtained by periodic beacons from the link layer of each neighboring node. These signal strengths are recorded as weak or strong. DRP receives all the transmissions and, after processing, it passes those to the SRP. SRP passes the packet to the node's upper layer stack if it is the destination. Otherwise, it looks for the destination in routing table and forwards the packet. If there is no entry in the routing table for that destination, it initiates the route-finding process. Route-request packets are forwarded to the neighbors using the strong channels. The destination, after getting the request, chooses the first arriving request packet and sends back the reply. The DRP reverses the selected route and sends a route-reply message back to the initiator of route-request. The DRPs of the nodes along the path update their routing tables accordingly. In case of a link failure, the intermediate nodes send an error message to the source indicating which channel has failed. The source in turn sends an *erase* message to inform all nodes about the broken link and initiates a new route-search process to find a new path to the destination.

Temporarily Ordered Routing Algorithm

Temporally Ordered Routing Algorithm (TORA) [21] is a reactive routing protocol with some proactive enhancements where a link between nodes is established creating a Directed Acyclic Graph (DAG) of the route from the source node to the destination. This protocol uses a "*link reversal*" model in route discovery. A route discovery query is broadcasted and propagated throughout the network until it reaches the destination or a node that has information about how to reach the destination. TORA defines a parameter, termed *height*. *Height* is a measure of the distance of the responding node's distance up to the required destination node. In the route discovery phase, this parameter is returned to the querying node. As the query response propagates back, each intermediate node updates its TORA table with the route and *height* to the destination node. The source node then uses the *height* to select the best route toward the destination. This protocol has an interesting property that it frequently chooses the most convenient route, rather than the shortest route. For all these attempts, TORA tries to minimize the routing management traffic overhead.

Cluster-Based Routing Protocol

Cluster-Based Routing Protocol (CBRP) [22] is an on-demand routing protocol, where the nodes are divided into clusters. For cluster formation, the following algorithm is employed. When a node comes up in the network, it has the *undecided* state. The first task of this node is to start a timer and to broadcast a HELLO message. When a cluster-head receives this HELLO message, it replies immediately with a triggered HELLO message. After that, when the node receives this answer, it changes its state into the *member* state. But when the node gets no message from any cluster-head, it makes itself as a cluster-head, but only when it has bidirectional link to one or more neighbor nodes. Otherwise, when it has no link to any other node, it stays in the *undecided* state and repeats the procedure with sending a HELLO message again.

Each node has a neighbor table. For each neighbor, the node keeps the status of the link and state of the neighbor in the neighbor table. A cluster head keeps information about all of its members in the same cluster. It also has a cluster adjacency table, which provides information about the neighboring clusters.

Example 4.9 The network structure shown in Fig. 4.5 could be used to explain the clustering used in CBRP. However, while CGSR is a proactive routing protocol, CBRP is a reactive or on-demand routing protocol. Though the basic clustering mechanisms are same, the difference lies in the method of routing in the network. In case of CBRP, for sending data packets a source node floods route-request packet to the neighboring cluster heads. On receiving the request, a cluster head checks whether the destination node is its own cluster or not. If it is within that cluster, it sends the request to the node, and if not, it again sends the request to the neighboring cluster head. This process continues and the destination eventually gets the route request. The reply from the destination is sent using the reverse path of the route. In case of a route failure, a local repair mechanism is used. When a node finds the next hop is unreachable, it checks whether the next hop can be reached through any of its neighbors or whether the hop after the next hop can be reached via any other neighbor. If any of these works, the packet can be routed using the repaired path.

Dynamic Source Routing

Dynamic Source Routing (DSR) [23] allows nodes in the MANET to dynamically discover a source route across multiple network hops to any destination. In this protocol, the mobile nodes are required to maintain route caches or the known routes. The route cache is updated when any new route is known for a particular entry in the route cache.

Routing in DSR is done using two phases: route discovery and route maintenance. When a source node wants to send a packet to a destination, it first consults its *route cache* to determine whether it already knows about any route to the destination or not. If already there is an entry for that destination, the source uses that to send the packet. If not, it initiates a route request broadcast. This request includes the destination address, source address, and a unique identification number. Each intermediate node checks whether it knows about the destination or not. If the intermediate node does not know about the destination, it again forwards the packet and eventually this reaches the destination. A node processes the route request packet only if it has not previously processed the packet and its address is not present in the route record of the packet. A route reply is generated by the destination or by any of the intermediate nodes when it knows about how to reach the destination. Figure 4.10 shows the operational method of the dynamic source routing protocol.

Example 4.10 In Fig. 4.10, the route discovery procedure is shown where S1 is the source node and S7 is the destination node.

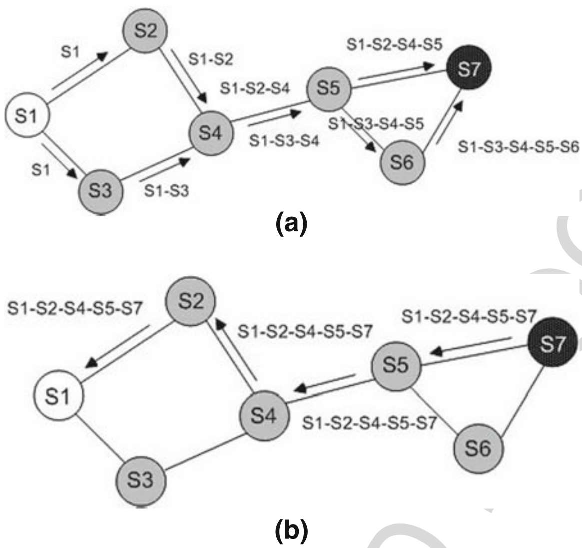


Fig. 4.10 **(a)** Route Discovery **(b)** Using route record to send the route reply

In this example, the destination gets the request through two paths. It chooses one path based on the route records in the incoming request packet and accordingly sends a reply using the reverse path to the source node. At each hop, the best route with minimum hop is stored. In this example, we have shown the route record status at each hop to reach the destination from the source node. Here, the chosen route is S1-S2-S4-S5-S7.

Ad Hoc On-Demand Distance Vector Routing

Ad Hoc On-Demand Distance Vector Routing (AODV) [24] is basically an improvement of DSDV. But, AODV is a reactive routing protocol instead of proactive. It minimizes the number of broadcasts by creating routes based on demand, which is not the case for DSDV. When any source node wants to send a packet to a destination, it broadcasts a route request (RREQ) packet. The neighboring nodes in turn broadcast the packet to their neighbors and the process continues until the packet reaches the destination. During the process of forwarding the route request, intermediate nodes record the address of the neighbor from which the first copy of the broadcast packet is received. This record is stored in their route tables, which helps for establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. The reply is sent using the reverse path.

For route maintenance, when a source node moves, it can re-initiate a route discovery process. If any intermediate node moves within a particular route, the neighbor of the drifted node can detect the link failure and sends a link failure notification to its upstream neighbor. This process continues until the failure

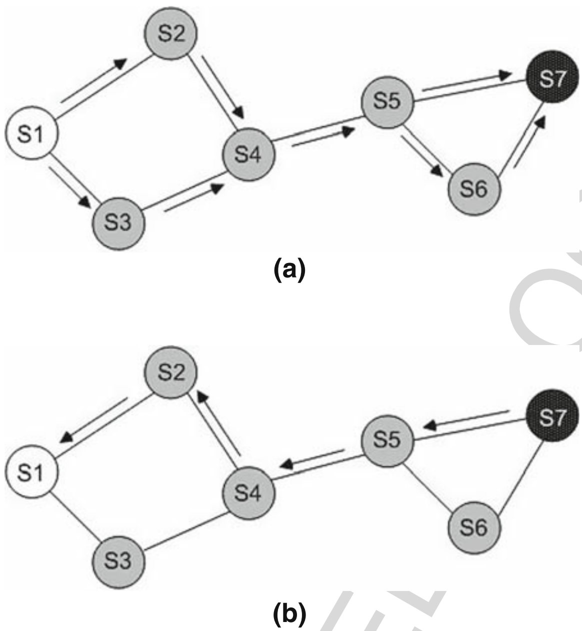


Fig. 4. 11 AODV protocol **(a)** Source node broadcasting the route request packet. **(b)** Route reply is sent by the destination using the reverse path

notification reaches the source node. Based on the received information, the source might decide to re-initiate the route discovery phase. Figure 4.11 shows an example of AODV protocol's operational mechanism.

Example 4.11 In Fig. 4.11, S1 is the source node and S7 is the destination node. The source initiates the route request and the route is created based on demand. Route reply is sent using the reverse path from the destination.

4.3.3.3 Hybrid Routing Protocols

Dual-Hybrid Adaptive Routing

Dual-Hybrid Adaptive Routing (DHAR) [25] uses the Distributed Dynamic Cluster Algorithm (DDCA) presented in [26]. The idea of DDCA is to dynamically partition the network into some non-overlapping clusters of nodes consisting of one parent and zero or more children. Routing is done in DHAR utilizing a dynamic two-level hierarchical strategy, consisting of optimal and least-overhead table-driven algorithms operating at each level.

DHAR implements a proactive least-overhead level-2 routing protocol in combination with a dynamic binding protocol to achieve its hybrid characteristics. The level-2 protocol in DHAR requires that one node generates an update on behalf of its cluster. When a level-2 update is generated, it must be flooded to all the nodes in each neighboring cluster. Level-2 updates are not transmitted beyond the neighboring clusters. The node with the lowest node ID in each cluster is designated to generate level-2 updates. The binding process is similar to a reactive route discovery process; however, a priori knowledge of clustered topology makes it significantly more efficient and simpler to accomplish the routing. To send packets to the desired destination, a source node uses the dynamic binding protocol to discover the current cluster ID associated with the destination. Once determined, this information is maintained in the dynamic cluster binding cache at the source node. The dynamic binding protocol utilizes the knowledge of the level-2 topology to efficiently broadcast a binding request to all the clusters. This is achieved using reverse path forwarding with respect to the source cluster.

Adaptive Distance Vector Routing

Adaptive Distance Vector (ADV) [27] routing protocol is a distance-vector routing algorithm that exhibits some on-demand features by varying the frequency and the size of routing updates in response to the network load and mobility patterns. This protocol has the benefits of both proactive and reactive routing protocols. ADV uses an adaptive mechanism to mitigate the effect of periodic transmissions of the routing updates, which basically relies on the network load and mobility conditions. To reduce the size of routing updates, ADV advertises and maintains routes for the active receivers only. A node is considered active if it is the receiver of any currently active connection. There is a *receiver flag* in the routing entry, which keeps the information about the status of a receiver whether it is active or inactive. To send data, a source node broadcasts network-wide an *init-connection* control packet. All the other nodes turn on the corresponding *receiver flag* in their own routing tables and start advertising the routes to the receiver in future updates. When the destination node gets the *init-connection* packet, it responds to it by broadcasting a *receiver-alert* packet and becomes active. To close a connection, the source node broadcasts network-wide an *end-connection* control packet, indicating that the connection is to be closed. If the destination node has no additional active connection, it broadcasts a *non-receiver-alert* message. If the *init-connection* and *receiver-alert* messages are lost, the source advertises the receiver's entry with its *receiver flag* set in all future updates. ADV also defines some other parameters like trigger meter, trigger threshold, and buffer threshold. These are used for limiting the network traffic based on the network's mobility pattern and network speed.

Zone Routing Protocol

Zone Routing Protocol (ZRP) [28] is suitable for wide variety of MANETs, especially for the networks with large span and diverse mobility patterns. In this protocol, each node proactively maintains routes within a local region, which is termed as routing zone. Route creation is done using a query-reply mechanism. For creating different zones in the network, a node first has to know who its neighbors are. A neighbor is defined as a node with whom direct communication can be established, and that is, within one hop transmission range of a node. Neighbor discovery information is used as a basis for Intra-zone Routing Protocol (IARP), which is described in detail in [29]. Rather than blind broadcasting, ZRP uses a query control mechanism to reduce route query traffic by directing query messages outward from the query source and away from covered routing zones. A covered node is a node which belongs to the routing zone of a node that has received a route query. During the forwarding of the query packet, a node identifies whether it is coming from its neighbor or not. If yes, then it marks all of its known neighboring nodes in its same zone as covered. The query is thus relayed till it reaches the destination. The destination in turn sends back a reply message via the reverse path and creates the route.

Sharp Hybrid Adaptive Routing Protocol

Sharp Hybrid Adaptive Routing Protocol (SHARP) [30] combines the features of both proactive and reactive routing mechanisms. SHARP adapts between reactive and proactive routing by dynamically varying the amount of routing information shared proactively. This protocol defines the proactive zones around some nodes. The number of nodes in a particular proactive zone is determined by the node-specific zone radius. All nodes within the zone radius of a particular node become the member of that particular proactive zone for that node. If for a given destination a node is not present within a particular proactive zone, reactive routing mechanism (query-reply) is used to establish the route to that node. Proactive routing mechanism is used within the proactive zone. Nodes within the proactive zone maintain routes proactively only with respect to the central node. In this protocol, proactive zones are created automatically if some destinations are frequently addressed or sought within the network. The proactive zones act as collectors of packets, which forward the packets efficiently to the destination, once the packets reach any node at the zone vicinity.

Example 4.12 In Fig. 4.12, some proactive zones are shown in a sample MANET. Here, we have four destination nodes, A, B, C, and D. As destination D is not used heavily, no proactive zone is created within its surroundings.

But for the other three destinations, A, B, and C, proactive zones of different sizes are created. As node A has the highest number of calls within the network as a destination, its proactive zone is the largest among all the destinations. Any routing within the proactive zone is done using proactive routing mechanisms. But, outside of the proactive zones, reactive routings are employed. The zone radius acts as a virtual knob to control the mix of proactive and reactive routing for each destination in SHARP. For example, in case of destination D in the figure, reactive mechanism is used.

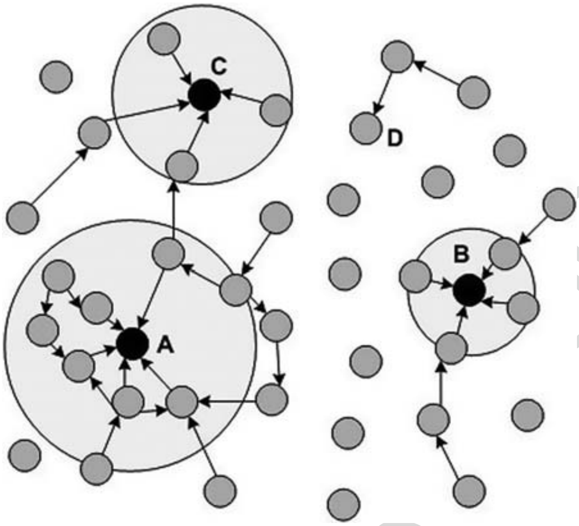


Fig. 4.12 Proactive zones around the hot destinations in SHARP

Neighbor-Aware Multicast Routing Protocol

Neighbor-Aware Multicast Routing Protocol (NAMP) [31] is a tree-based hybrid routing protocol, which utilizes neighborhood information. The routes in the network are built and maintained using the traditional request and reply messages or on-demand basis. This hybrid protocol uses neighbor information of two-hops away for transmitting the packets to the receiver. If the receiver is not within this range, it searches the receiver using dominant pruning flooding method [32] and forms a multicast tree using the replies along the reverse path. Although the mesh structure is known to be more robust against topological changes, the tree structure is better in terms of packet transmission. As NAMP targets to achieve less end-to-end delay of packets, it uses the tree structure.

There are mainly three operations addressed in NAMP:

- Multicast tree creation
- Multicast tree maintenance
- Joining and leaving of nodes from the multicast group

All the nodes in the network keep neighborhood information of up to two-hop away nodes. This neighborhood information is maintained using a proactive mechanism. Periodic *hello* packet is used for this. To create the multicast tree, the source node sends a *flood request* packet to the destination with data payload attached. This packet is flooded in the network using dominant pruning method, which actually minimizes the number of transmissions in the network for a particular *flood request* packet. During the forwarding process of the packet, each node selects a forwarder and creates a secondary forwarder list (*SFL*). The secondary forwarder list (*SFL*) contains the information about the nodes that were primarily considered as possible forwarders but finally were not selected for that purpose. Each intermediate node uses the chosen forwarder to forward the packet, but keeps the knowledge about other possible forwarders in *SFL*. Secondary forwarder list is used for repairing any broken route in the network. In fact, link failure recovery is one of the greatest advantages of NAMP. The next example shows some figures to explain NAMP's operations in brief.

Example 4.13 Figure 4.13 shows a sample network where NAMP has created the multicast tree consisting of the source, destination, and intermediate nodes (forwarders). Here, S1 is the source, S12 is the destination. Nodes S3, S6, S9, and S11 are the forwarding nodes. For each forwarding hop, each forwarder maintains the information of the neighboring nodes in the secondary forwarder list. In case of a link failure as shown in Fig. 4.13(b), S3 immediately finds an alternate path to repair the existing route for the S1-S12 source–destination pair. Figure 4.13(c) shows that S3 repairs the path to use the existing route to

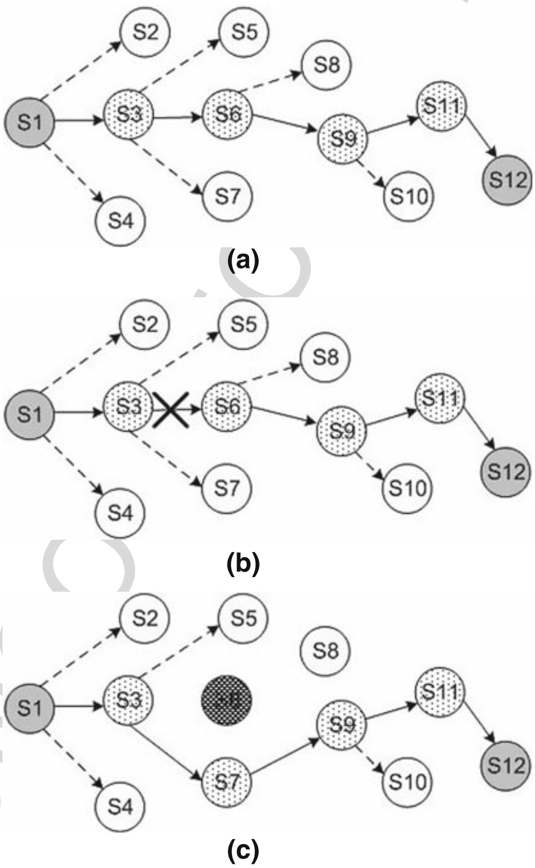


Fig. 4.13 **(a)** Network sample **(b)** Link failure **(c)** Link failure recovery in NAMP

reach the destination using the alternate node S7. Link failure recovery is done locally in NAMP, which is one of its greatest advantages.

4.3.3.4 Other Routing Protocols

In addition to the mentioned routing protocols for MANET, there are some other routing protocols that do not rely on any traditional routing mechanisms, instead rely on the location awareness of the participating nodes in the network. Generally, in traditional MANETs, the nodes are addressed only with their IP addresses. But, in case of location-aware routing mechanisms, the nodes are often aware of their exact physical locations in the three-dimensional world. This capability might be introduced in the nodes using Global Positioning System (GPS) or with any other geometric methods. GPS is a worldwide, satellite-based radio navigation system that consists of 24 satellites in six orbital planes. By connecting to the GPS receiver, a mobile node can know its current physical location. Also sometimes the network is divided into several zones or geographic regions for making routing little bit easier. Based on these concepts, several geocast and location-aware routing protocols have already been proposed. Geocasting is basically a variant of the conventional multicasting where the nodes are considered under certain groups within particular geographical regions. In geocasting, the nodes eligible to receive packets are implicitly specified by a physical region; membership in a geocast group changes whenever a mobile node moves in or out of the geocast region.

The major feature of these routing protocols is that, when a node knows about the location of a particular destination, it can direct the packets toward that particular direction from its current position, without using any route discovery mechanism. Recently, some of the researchers proposed some location-aware protocols that are based on these sorts of idea. Some of the examples of them are Geographic Distance Routing (GEDIR) [33], Location-Aided Routing (LAR) [34], Greedy Perimeter Stateless Routing (GPSR) [35], GeoGRID [36], Geographical Routing Algorithm (GRA) [37], etc. Other than these, there are a number of multicast routing protocols for MANET. Some of the mentionable multicast routing protocols are: Location-Based Multicast Protocol (LBM) [38], Multicast Core Extraction Distributed Ad hoc Routing (MCEDAR) [39], Ad hoc Multicast Routing protocol utilizing Increasing id-numberS (AMRIS) [40], Associativity-Based Ad hoc Multicast (ABAM) [41], Multicast Ad hoc On-Demand Distance-Vector (MAODV) routing [42], Differential Destination Multicast (DDM) [43], On-Demand Multicast Routing Protocol (ODMRP) [44], Adaptive Demand-driven Multicast Routing (ADMR) protocol [45], Ad hoc Multicast Routing protocol (AMRoute) [46], Dynamic Core-based Multicast routing Protocol (DCMP) [47], Preferred Link-Based Multicast protocol (PLBM) [48], etc. Some of these multicast protocols use location information and some are based on other routing protocols or developed just as the extension of another unicast routing protocol. For

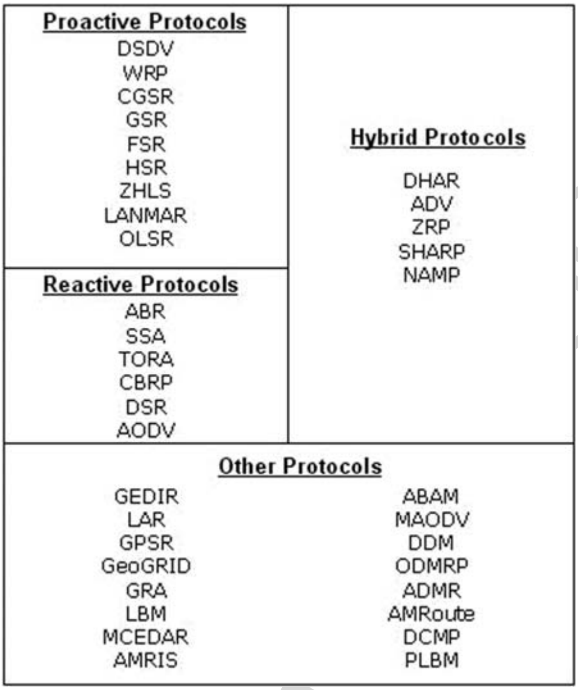


Fig. 4.14 Major Routing Protocols for MANET at a glance

example, MAODV is the multicast-supporting version of AODV. Figure 4.14 shows the major routing protocols for MANET at a glance.

4.3.3.5 Other Recent Works on MANET Routing for Reference

In this section, we mention a list of references of the recent works on routing in MANET so that it could be used as a reference by the practitioners. Some of these works have taken the major routing protocols as their bases and some of them have enhanced various performances of the previous routing protocols. Mentionable recent works are: node-density-based routing [49], load-balanced routing [50], optimized priority-based energy-efficient routing [51], reliable on-demand routing with mobility prediction [52], QoS routing [53], secure distributed anonymous routing protocol [54], robust position-based routing [55], routing with group motion support [56], dense cluster gateway based routing protocol [57], dynamic backup routes routing protocol [58], gathering-based routing protocol [59], QoS-aware multicast routing protocol [60], recycled path routing [61], QoS multicast routing protocol for clustering in MANET [62], secure anonymous routing protocol with authenticated key exchange [63], self-healing on-demand geographic path routing protocol [64], stable weight-based on-demand routing protocol [65], fisheye zone routing protocol [66], on-demand utility-based power control routing [67], secure position-based routing protocol [68], scalable multi-path on-demand routing [69], virtual coordinate-based routing [70], etc.

4.3.4 Criteria for Performance Evaluation of MANET Routing Protocols

Performance of a particular routing protocol depends on the requirements and settings of a mobile ad hoc network. One routing protocol might seem to be efficient in a scenario while it might not be efficient in a different scenario. However, to analyze the routing protocols in MANET, we generally take some common criteria as the basis of comparison. Commonly used criteria are the end-to-end delay, control overhead, processing overhead of nodes, memory requirement, and packet-delivery ratio. Of these criteria, packet-delivery ratio mainly tells about the reliability of the protocol. So, reliability of a routing protocol depends on how efficiently it can transmit data from source to the destination. The less the packet loss ratio is, the better the performance of that routing protocol. Often security becomes the key aspect of MANET. In such cases, the protocol that might ensure better security is considered as more efficient for that application.

So far, we have talked about different types of routing protocols. We mainly categorized them into reactive, proactive, and hybrid protocols. Generally speaking, reactive protocols require less amount of memory, processing power, and energy than that of the proactive protocols. Having the knowledge of the MANET routing protocols and their comparison criteria, let us now investigate the key influencing factors for routing performance in different settings of MANETs.

4.3.4.1 Mobility Factors

- *Velocity of nodes*: The velocity of the mobile nodes within a MANET is not fixed. As there is no speed limitation of the wireless devices, high speed of nodes might affect the performance of many protocols. A protocol is considered good for MANET if it can perform well both in relatively static and in fully dynamic network state, though it is true that routing in a highly mobile MANET is a tough task.
- *Direction of mobility*: The direction of a node's mobility is not known in advance. It is a very common incident that a node travels to a direction where the number of neighbor nodes is less or there is no neighbor node. This is called drifting away of a node from a MANET. A hard-state approach or a soft-state approach could be used to handle such incidents. In hard-state approach, the node explicitly informs all the other nodes in the MANET about its departure or movement from a position, while in a soft-state approach a time out value is used to detect the departure.

- *Group or individual mobility*: MANETs are often categorized as Pure MANET and Military MANET. In a pure MANET, it is not obvious that the nodes should move in groups, but in case of military MANET, group mobility is the main concern. A military MANET can maintain a well-defined chain of commands, which is absent in case of a pure MANET. So the routing strategies could vary depending upon this factor. Two MANET protocols considered as good for supporting group mobility are: LANMAR [16], developed by University of California at Los Angeles, and OLSR [18], which is developed by the French National Institute for Research in Computer Science and Control (INRIA).
- *Frequency of changing of mobility model*: Routing strategy could also vary depending on the mobility model of the MANET. The topology of an ad hoc network could definitely change over time. But, the key factor here is the change of overall mobility model in a fast or relatively slow fashion. If the nodes change their relative positions too frequently, the maintenance cost of the overall network gets higher. For example, a MANET formed with war planes, tanks, helicopters, and ships is highly dynamic, while an ad hoc network formed with some laptops and palmtops carried by the participants in a conference is relatively less dynamic.

4.3.4.2 Wireless Communication Factors

- *Consumption of power*: Power is a valuable resource in wireless networking. Especially for routing, power is highly needed. According to an experiment by Kravets and Krishnan (1998), power consumption caused by networking-related activities is approximately 10% of the overall power consumption of a laptop computer. This figure rises up to 50% in handheld devices [71]. In ad hoc network, every node has to contribute for maintaining the network connections. Hence, routing protocol should consider everything to save power of the participating battery-powered devices.
- *Bandwidth*: For any type of wireless communications, bandwidth available for the network is a major concern. An efficient routing protocol should try to minimize the number of packet-transmissions or control overhead for the maintenance of the network.
- *Error rate*: Wireless communication is always susceptible to high error rate. Packet loss is a common incident. So, the routing strategies should be intelligent enough to minimize the error rate for smooth communications among the nodes.
- *Unidirectional link*: Sometimes it is convenient for a routing protocol to assume routes as unidirectional links.

4.3.4.3 Security Issues

- *Unauthorized access*: Security has recently become a major issue for ad hoc network routing. Most of the ad hoc network routing protocols that are currently proposed lack security. A wireless network is more vulnerable than a wired network. So, based on the requirement, sometimes preventing unauthorized access to the network becomes the major concern.

- *Accidental association with other networks*: Accidental associations between a node in one wireless network and a neighboring wireless network are just now being recognized as a security concern, as enterprises confront the issue of overlapping networks. At the routing level it should be ensured that the nodes can recognize their own network.

4.3.4.4 Other Factors

- *Reliability of the network*: Reliability is sometimes defines as how efficiently a routing protocol can dispatch packets to the appropriate destinations. A routing protocol must be efficient enough to handle successful packet delivery so that an application may rely on it.
- *Size of the network*: The overall network size could be a crucial factor. A routing protocol might be good for a small network, but might not be fit for use in a large ad hoc network or vice versa.
- *Quality of service*: In the real-time applications, QoS becomes a key factor for evaluating the performance of a routing protocol.
- *Timing*: Regardless of the method of communication used, access time and tuning time must be considered. Tuning time is the measure of the amount of time each node spends in active mode. In the active mode a node consumes maximum power. So, minimizing the tuning time is one of the critical factors to conserve power.

4.4 Thoughts for Practitioners

It is still a matter of debate whether the routing protocols for mobile ad hoc networks should be predicted based on the network overhead or the optimization of the network path. In this chapter, we have learnt about a number of routing protocols for MANET, which are broadly categorized as proactive and reactive. Proactive routing protocols tend to provide lower latency than that of the on-demand protocols, because they try to maintain routes to all the nodes in the network all the time. But the drawback for such protocols is the excessive routing overhead transmitted, which is periodic in nature without much consideration for the network mobility or load. On the other hand, though reactive protocols discover routes only when they are needed, they may still generate a huge amount of traffic when the network changes frequently.

Depending on the amount of network traffic and number of flows, the routing protocols could be chosen. When there is congestion in the network due to heavy traffic, in general case, a reactive protocol is preferable. Sometimes the size of the network might be a major considerable point. For example, AODV, DSR, OLSR are some of the protocols suitable for relatively smaller networks, while the routing protocols like TORA, LANMAR, ZRP are suitable for larger networks. Network mobility is another factor that can degrade the performance of certain protocols. When the network is relatively static, proactive routing protocols can be used, as storing the topology information in such case is more efficient. On the other hand, as the mobility of nodes in the network increases, reactive protocols perform better.

Overall, the answer to the debating point might be that the mobility and traffic pattern of the network must play the key role for choosing an appropriate routing strategy for a particular network. It is quite natural that one particular solution cannot be applied for all sorts of situations and, even if applied, might not be optimal in all cases. Often it is more appropriate to apply a hybrid protocol rather than a strictly proactive or reactive protocol as hybrid protocols often possess the advantages of both types of protocols.

4.5 Directions for Future Research

The structure of the Internet that is used today is based mainly on wired communications. The emerging technologies like fiber optics–based high-speed wired networks would flourish in the near future. With this existing network of networks, semi-infrastructure and infrastructure-less wireless networks will also be used in abundance. Figure 4.15 shows a conceptual view of the future global Internet structure. MANETs would definitely play an important role in the future Internet structure, especially for the mobile Internet. Hence, in some cases, it might be necessary that the routing protocols of MANET work in perfect harmony with their wired counterparts. Considering different approaches of routing, a hybrid approach might be more appropriate for such scenarios.

More and more efficient routing protocols for MANET might come in front in the coming future, which might take security and QoS (Quality of Service) as the major concerns. So far, the routing protocols mainly focused on the

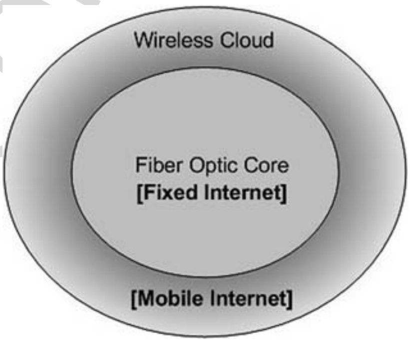


Fig. 4.15 Future Global Internet Structure

methods of routing, but in future a secured but QoS-aware routing protocol could be worked on. We should keep this in mind that ensuring both of these parameters at the same time might be difficult. A very secure routing protocol surely incurs more overhead for routing, which might degrade the QoS level. So an optimal trade-off between these two parameters could be searched.

We saw that in the recent years some multicast routing protocols have been proposed. The reason for the growing importance of multicast is that this strategy could be used as a means to reduce bandwidth utilization for mass distribution of data. As there is a pressing need to conserve scarce bandwidth over wireless media, it is natural that multicast routing should receive some attention for ad hoc networks. So it is, in most of the cases, advantageous to use multicast rather than multiple unicast, especially in ad hoc environment where bandwidth comes at a premium. Another advantage of multicasting is that it provides group communication facility. A group of nodes can be addressed at the same time using only a group identifier. So it is an efficient communication tool for using in multipoint applications.

Ad hoc wireless networks find applications in civilian operations (collaborative and distributed computing) emergency search-and-rescue, law enforcement, and warfare situations, where setting up and maintaining a communication infrastructure is very difficult. In all these applications, communication and coordination among a given set of nodes are necessary. Considering all these, in future the routing protocols might especially emphasize the support for multicasting in the network.

4.6 Conclusions

In this chapter, we have talked about MANET, the challenges for routing in MANET, major routing protocols, the major features of MANET routing protocols, key aspects for routing in MANET, and future research issues for routing in MANET. We categorized the proposed routing protocols based on their working principles and discussed which type of protocol might be used in which situation.

The proliferation of mobile ad hoc networks is looming on the horizon. Exploitation of these types of infrastructure-less networks are expected to flourish in future, not only for civil but also for military reconnaissance scenarios. It is quite reasonable to think that the security and QoS (Quality of Service) requirements might differ largely for different types of civil and military applications. Based on these two critical aspects, appropriate routing protocols should have to be chosen for the application at hand. Some of the routing protocols proposed in the recent days for MANETs are considered as *promising* for use in real workplaces. However, *One cannot satisfy all*. This might also be true for any routing protocol that could emerge in the near future. So the ultimate solution is the use of different routing protocols for different situations. In that case, the cooperation among dissimilar routing protocols would be the major issue to address in future. Though the collaboration of different routing strategies is more or less well defined in case of wired networks, for mobile ad hoc networks there still remains a lot of scope of research on this issue.

Terminologies

MANET (Mobile Ad Hoc Network) – A Mobile Ad Hoc Network (MANET) is a kind of wireless network that could be formed on the fly where a number of wireless mobile nodes work in cooperation, without the engagement of any centralized access point or any fixed infrastructure.

QoS (Quality of Service) – The ability of a network (including applications, hosts, and infrastructure devices) to deliver traffic with minimum delay and maximum availability.

NPDU (Network Protocol Data Unit) – A frame of data transmitted over the physical layer of a network.

MRL (Message Retransmission List) – In case of Wireless Routing Protocol (WRP), each node maintains a Message Retransmission List (MRL). MRL is used for confirming the reception of update messages by neighboring nodes.

MPR (MultiPoint Relay) – OLSR protocol relies on the selection of multipoint relay (MPR) nodes. MPRs are selected among the one-hop neighborhood of a node using the bidirectional links, and they are used to minimize the amount of broadcast traffic in the network.

DRP (Dynamic Routing Protocol) – Signal Stability–Based Adaptive Routing Protocol (SSA) uses DRP.

SRP (Static Routing Protocol) – Signal Stability–Based Adaptive Routing Protocol (SSA) uses SRP.

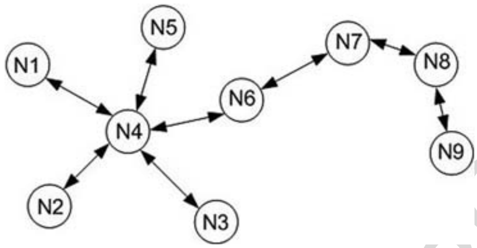
DDCA – Distributed Dynamic Cluster Algorithm
IARP – Intra-Zone Routing Protocol
SFL – Secondary Forwarder List
DSDV – Dynamic Destination-Sequenced Distance-Vector
WRP – Wireless Routing Protocol
CGSR – Cluster Gateway Switch Routing
GSR – Global State Routing
FSR – Fisheye State Routing
HSR – Hierarchical State Routing
ZHLS – Zone-Based Hierarchical Link State
LANMAR – Landmark Ad Hoc Routing
OLSR – Optimized Link State Routing
ABR – Associativity-Based Routing
SSA – Signal Stability–based Adaptive

TORA – Temporarily Ordered Routing Algorithm
CBRP – Cluster Based Routing Protocol
DSR – Dynamic Source Routing
AODV – Ad Hoc On-Demand Distance Vector
DHAR – Dual-Hybrid Adaptive Routing
ADV – Adaptive Distance Vector
ZRP – Zone Routing Protocol
SHARP – Sharp Hybrid Adaptive Routing Protocol
NAMP – Neighbor-Aware Multicast routing Protocol
GEDIR – GEographic DIstance Routing
LAR – Location-Aided Routing
GPSR – Greedy Perimeter Stateless Routing
GeoGRID – Geographical GRID
GRA – Geographical Routing Algorithm
LBM – Location-Based Multicast
MCEDAR – Multicast Core Extraction Distributed Ad hoc Routing
AMRIS – Ad hoc Multicast Routing protocol utilizing Increasing id-numberS
ABAM – Associativity-Based Ad hoc Multicast
MAODV – Multicast Ad hoc On-Demand Distance Vector
DDM – Differential Destination Multicast
ODMRP – On-Demand Multicast Routing Protocol
ADMR – Adaptive Demand-driven Multicast Routing
AMRoute – Ad hoc Multicast Routing
DCMP – Dynamic Core-based Multicast routing Protocol
PLBM – Preferred Link-Based Multicast

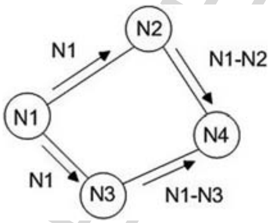
Questions

1. What are the major challenges for routing in MANET?
2. Why do not we use the routing protocols for wired networks for MANETs?
3. Suppose that we have a MANET where the nodes are frequently moving from one place to another. If we use DSDV as the routing protocol for this network, which method of updates would be better? Why?
4. What is a gateway in cluster-based routing protocols for MANET?
5. What is a *scope* in Fisheye State Routing?
6. How is the fisheye concept beneficial for routing?
7. What is a *landmark* in LANMAR?
8. How does OLSR reduce traffic in case of a broadcast procedure?
9. What does “Height” mean in TORA?
10. What is a Hybrid routing protocol?

11. Look at the figure below. Construct the route table advertised by node N4 if DSDV is used as the routing protocol (three columns: *Destination*, *Metric*, and *Sequence Number*).



12. Which criteria could affect the performance of the routing protocols for MANET?
13. Which protocol is the best among all the proposed routing protocols for MANET? Why? Justify your answer.
14. In the figure below, which path will be chosen to reach the destination N4 from the source N1, if Dynamic Source Routing is used? Why? Justify your answer.



References

1. Kahn RE (1977) The organization of computer resources into a packet radio network. IEEE Transactions on Communications, Volume COM-25, Issue 1:169–178
2. Jubin J, Tornow JD (1987) The DARPA Packet Radio Network Protocols. Proceedings of the IEEE, Volume 75, Issue 1:21–32
3. Freebersyser J, Leiner B (2001) A DoD Perspective on Mobile Ad Hoc Networks. In: Perkins CE (ed) Ad Hoc Networking, Addison-Wesley:29–51
4. Yang H, Luo H, Ye F, Lu S, Zhang, L (2004) Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications, Volume 11, Issue 1:38–47
5. Deng H, Li W, Agrawal DP (2002) Routing Security in Wireless Ad Hoc Networks. IEEE Communications Magazine, Volume 40, Issue 10:70–75
6. Maihöfer C (2004) A Survey of Geocast Routing Protocols. IEEE Communications Surveys & Tutorials, Volume 6, Issue 2:Q2:32–42
7. Perkins CE, Bhagwat P (1994) Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. Proceedings of ACM SIGCOMM 1994:234–244
8. Cheng C, Riley R, Kumar SPR, Garcia-Luna-Aceves JJ (1989) A Loop-Free Extended Bellman-Ford Routing Protocol Without Bouncing Effect. ACM SIGCOMM Computer Communications Review, Volume 19, Issue 4:224–236

9. Murthy S, Garcia-Luna-Aceves JJ (1996) An Efficient Routing Protocol for Wireless Networks. Mobile Networks and Applications, Volume 1, Issue 2:183–197
10. Humblet PA (1991) Another Adaptive Distributed Shortest-Path Algorithm. IEEE Transactions on Communications, Volume 39, Issue 6:995–1003
11. Rajagopalan B, Faiman M (1991) A Responsive Distributed Shortest-Path Routing Algorithm Within Autonomous Systems. Journal of Internetworking Research and Experiment, Volume 2, Issue 1:51–69
12. Chiang C-C, Wu H-K, Liu W, Gerla M (1997) Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel. Proceedings of IEEE SICON:197–211
13. Chen T-W, Gerla M (1998) Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks. Proceedings of IEEE ICC 1998:171–175
14. Iwata A, Chiang C-C, Pei G, Gerla M, Chen T-W (1999) Scalable Routing Strategies for Ad Hoc Wireless Networks. IEEE Journal on Selected Areas in Communications, Volume 17, Issue 8:1369–1379
15. Jao-Ng M, Lu I-T (1999) A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks. IEEE Journal on Selected Areas in Communications, Volume 17, Issue 8:1415–1425
16. Pei G, Gerla M, Hong X (2000) LANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Network with Group Mobility. First Annual Workshop on Mobile and Ad Hoc Networking and Computing 2000 (MobiHoc 2000):11–18
17. Tsuchiya PF (1988) The Landmark Hierarchy: A New Hierarchy for Routing in Very Large Networks. Computer Communication Review, Volume 18, Issue 4:35–42
18. Jacquet P, Mühlethaler P, Clausen T, Laouiti A, Qayyum A, Viennot L (2001) Optimized Link State Routing Protocol for Ad Hoc Networks. IEEE INMIC 2001:62–68
19. Toh C-K (1996) A Novel Distributed Routing Protocol to Support Ad-Hoc Mobile Computing. Proceedings of the 1996 IEEE 15th Annual International Phoenix Conference on Computers and Communications:480–486
20. Dube R, Rais CD, Wang K-Y, Tripathi SK (1997) Signal Stability-Based Adaptive Routing (SSA) for Ad Hoc Mobile Networks. IEEE Personal Communications, Volume 4, Issue 1:36–45
21. Park VD, Corson MS (1997) A highly adaptive distributed routing algorithm for mobile wireless networks. Proceedings of IEEE INFOCOM 1997, Volume 3:1405–1413
22. Jiang M, Li J, Tay YC (1999) Cluster Based Routing Protocol (CBRP). IETF Draft, August 1999, available at http://tools.ietf.org/html/draft-ietf-manet-cbrp-spec-01. Accessed 21 February 2008
23. Broch J, Johnson DB, Maltz DA (1999) The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. IETF Draft, October, 1999, available at http://tools.ietf.org/id/draft-ietf-manet-dsr-03.txt. Accessed 21 February 2008
24. Perkins CE, Royer EM, Chakeres ID (2003) Ad Hoc On-Demand Distance Vector (AODV) Routing. IETF Draft, October, 2003, available at http://tools.ietf.org/html/draft-perkins-manet-aodvbis-00. Accessed 21 February 2008
25. McDonald AB, Znati T (2000) A Dual-Hybrid Adaptive Routing Strategy for Wireless Ad-Hoc Networks. Proceedings of IEEE WCNC 2000, Volume 3:1125–1130
26. McDonald AB, Znati T (1999) A Mobility Based Framework for Adaptive Clustering in Wireless Ad-Hoc Networks. IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, Volume 17, Issue 8:1466–1487
27. Boppana RV, Konduru SP (2001) An Adaptive Distance Vector Routing Algorithm for Mobile, Ad Hoc Networks. Proceedings of IEEE INFOCOM 2001:1753–1762
28. Haas ZJ, Pearlman MR, Samar P (2002) The Zone Routing Protocol (ZRP) for Ad Hoc Networks. IETF draft, July 2002, available at http://tools.ietf.org/id/draft-ietf-manet-zone-zrp-04.txt. Accessed 21 February 2008

29. Haas ZJ, Pearlman MR, Samar P (2002) Intrazone Routing Protocol (IARP). IETF Internet Draft, July 2002, available at http://tools.ietf.org/wg/manet/draft-ietf-manet-zone-ierp/draft-ietf-manet-zone-ierp-02-from-01.diff.txt. Accessed 21 February 2008
30. Ramasubramanian V, Haas ZJ, Sirer, EG (2003) SHARP: A Hybrid Adaptive Routing Protocol for Mobile Ad Hoc Networks. Proceedings of ACM MobiHoc 2003:303–314
31. Pathan A-SK, Alam MM, Monowar MM, Rabbi MF (2004) An Efficient Routing Protocol for Mobile Ad Hoc Networks with Neighbor Awareness and Multicasting. Proceedings of IEEE E-Tech, July, 2004:97–100
32. Lim H, Kim C (2000) Multicast Tree Construction and Flooding in Wireless Ad Hoc Networks. Proceedings of the 3rd ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems:61–68
33. Lin X, Stojmenovic I (1999) GEDIR: Loop-Free Location Based Routing in Wireless Networks. Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Systems:1025–1028
34. Ko Y-B, Vaidya NH (2000) Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. Wireless Networks, Volume 6:307–321
35. Karp B, Kung HT (2000) GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. ACM MOBICOM 2000:243–254
36. Liao W-H, Tseng Y-C, Lo K-L, Sheu J-P (2000) GeoGRID: A Geocasting Protocol for Mobile Ad Hoc Networks based on GRID. Journal of Internet Technology, Volume 1, Issue 2:23–32
37. Jain R, Puri A, Sengupta R (2001) Geographical Routing Using Partial Information for Wireless Ad Hoc Networks. IEEE Personal Communications, Volume 8, Issue 1:48–57
38. Ko Y-B, Vaidya NH (1998) Location-based multicast in mobile ad hoc networks. Technical Report TR98-018, Texas A&M University
39. Sinha P, Sivakumar R, Bharghavan V (1999) MCEDAR: Multicast Core-Extraction Distributed Ad Hoc Routing. Proceedings of IEEE WCNC, Volume 3:1313–1317
40. Wu CW, Tay TC (1999) AMRIS: A Multicast Protocol for Ad Hoc Wireless Networks. IEEE MILCOM 1999, Volume 1:25–29
41. Toh C-K, Guichal G, Bunchua S (2000) ABAM: On-Demand Associativity-Based Multicast Routing for Ad Hoc Mobile Networks. Proceedings of IEEE VTS-Fall VTC 2000, Volume 3:987–993
42. Royer EM, Perkins CE (2000) Multicast Ad Hoc On-Demand Distance Vector (MAODV) Routing. IETF Draft, draft-ietf-manet-maodv-00, 15 July, 2000, available at http://tools.ietf.org/html/draft-ietf-manet-maodv-00. Accessed 21 February 2008
43. Ji L, Corson MS (2001) Differential Destination Multicast-A MANET Multicast Routing Protocol for Small Groups. Proceedings of IEEE INFOCOM 2001, Volume 2:1192–1201
44. Lee S, Su W, Gerla M (2002) On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks. ACM/Kluwer Mobile Networks and Applications (MONET), volume 7, Issue 6:441–453
45. Jetcheva JG, Johnson DB (2001) Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks. Proceedings of ACM MobiHoc 2001:33–44
46. Xie J, Talpade RR, Mcauley A, Liu M (2002) AMRoute: Ad Hoc Multicast Routing Protocol. Mobile Networks and Applications, Volume 7, Issue 6:429–439
47. Das SK, Manoj BS, Murthy CSR (2002) A Dynamic Core Based Multicast Routing Protocol for Ad Hoc Wireless Networks. Proceedings of ACM MobiHoc 2002:24–35
48. Sisodia RS, Karthigeyan I, Manoj BS, Murthy CSR (2003) A Preferred Link Based Multicast Protocol for Wireless Mobile Ad Hoc Networks. Proceedings of IEEE ICC 2003, Volume 3:2213–2217
49. Quintero A, Pierre S, Macabéo B (2004) A routing protocol based on node density for ad hoc networks. Ad Hoc Networks, Volume 2, Issue 3:335–349
50. Saigal V, Nayak AK, Pradhan SK, Mall R (2004) Load balanced routing in mobile ad hoc networks. Computer Communications, Volume 27, Issue 3:295–305

51. Wei X, Chen G, Wan Y, Mtenzi F (2004) Optimized priority based energy efficient routing algorithm for mobile ad hoc networks. Ad Hoc Networks, Volume 2, Issue 3:231–239
52. Wang N-C, Chang S-W (2005) A reliable on-demand routing protocol for mobile ad hoc networks with mobility prediction. Computer Communications, Volume 29, Issue 1:123–135
53. Bür K, Ersoy C (2005) Ad hoc quality of service multicast routing. Computer Communications, Volume 29, Issue 1:136–148
54. Boukerche A, El-Khatib K, Xu L, Korba L (2005) An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks. Computer Communications, Volume 28, Issue 10:1193–1203
55. Moaveninejad K, Song W-Z, Li X-Y (2005) Robust position-based routing for wireless ad hoc networks. Ad Hoc Networks, Volume 3, Issue 5:546–559
56. Rango FD, Gerla M, Marano S (2006) A scalable routing scheme with group motion support in large and dense wireless ad hoc networks. Computers & Electrical Engineering, Volume 32, Issues 1–3:224–240
57. Ghosh RK, Garg V, Meitei MS, Raman S, Kumar A, Tewari N (2006) Dense cluster gateway based routing protocol for multi-hop mobile ad hoc networks. Ad Hoc Networks, Volume 4, Issue 2:168–185
58. Wang Y-H, Chao C-F (2006) Dynamic backup routes routing protocol for mobile ad hoc networks. Information Sciences, Volume 176, Issue 2:161–185
59. Ahn CW (2006) Gathering-based routing protocol in mobile ad hoc networks. Computer Communications, Volume 30, Issue 1:202–206
60. Sun B, Li L (2006) QoS-aware multicast routing protocol for Ad hoc networks. Journal of Systems Engineering and Electronics, Volume 17, Issue 2:417–422
61. Eisbrener J, Murphy G, Eade D, Pinnow CK, Begum K, Park S, Yoo S-M, Youn J-H (2006) Recycled path routing in mobile ad hoc networks. Computer Communications, Volume 29, Issue 9:1552–1560
62. Layuan L, Chunlin L (2007) A QoS multicast routing protocol for clustering mobile ad hoc networks. Computer Communications, Volume 30, Issue 7:1641–1654
63. Lu R, Cao Z, Wang L, Sun C (2007) A secure anonymous routing protocol with authenticated key exchange for ad hoc networks. Computer Standards & Interfaces, Volume 29, Issue 5:521–527
64. Giruka VC, Singhal M (2007) A self-healing On-demand Geographic Path Routing Protocol for mobile ad-hoc networks. Ad Hoc Networks, Volume 5, Issue 7:1113–1128
65. Wang N-C, Huang Y-F, Chen J-C (2007) A stable weight-based on-demand routing protocol for mobile ad hoc networks. Information Sciences: an International Journal, Volume 177, Issue 24:5522–5537
66. Yang C-C, Tseng L-P (2007) Fisheye zone routing protocol: A multi-level zone routing protocol for mobile ad hoc networks. Computer Communications, Volume 30, Issue 2:261–268
67. Min C-H, Kim S (2007) On-demand utility-based power control routing for energy-aware optimization in mobile ad hoc networks. Journal of Network and Computer Applications, Volume 30, Issue 2:706–727
68. Song J-H, Wong VWS, Leung VCM (2007) Secure position-based routing protocol for mobile ad hoc networks. Ad Hoc Networks, Volume 5, Issue 1:76–86
69. Reddy LR, Raghavan SV (2007) SMORT: Scalable multipath on-demand routing for mobile ad hoc networks. Ad Hoc Networks, Volume 5, Issue 2:162–188
70. Zhao Y, Chen Y, Li B, Zhang Q (2007) Hop ID: A Virtual Coordinate-Based Routing for Sparse Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing, Volume 6, Issue 9:1075–1089
71. Kravets R, Krishnan P (1998) Power Management Techniques for Mobile Communication. Proceedings of ACM MOBICOM 1998:157–168