Enhanced On-Demand Multipath Routing for Wireless Networks

Enhanced On-Demand Multipath Routing for Wireless Networks

By

Periyasamy Pitchaipillai

Cambridge
Scholars
Publishing

Enhanced On-Demand Multipath Routing for Wireless Networks

By Periyasamy Pitchaipillai

This book first published 2018

Cambridge Scholars Publishing

Lady Stephenson Library, Newcastle upon Tyne, NE6 2PA, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Copyright © 2018 by Periyasamy Pitchaipillai

All rights for this book reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the copyright owner.

ISBN (10): 1-5275-1151-0
ISBN (13): 978-1-5275-1151-4

TABLE OF CONTENTS

PREFACE

Rapid deployment of independent mobile users will be the need of the next generation of wireless communication systems. The Mobile Ad hoc NETwork (MANET) is one of the most vibrant and active research fields in wireless communication systems. Mobile Ad hoc Networks (MANETs), are a collection of mobile devices by wireless links forming a dynamic topology without much physical network infrastructure such as routers, servers, access points/cables or centralized administration. The nodes of MANETs intercommunicate through single-hop and multi-hop paths in a peer-to-peer fashion. Intermediate nodes between a pair of communicating nodes act as routers. Hence each mobile device functions as a router as well as a node. Some of the wireless devices forming a MANET are PDAs, laptops, mobile phones, smart phones, tablets, etc. Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol has the common characteristic features of all popular multi-path routing algorithms in Mobile Ad hoc Networks and is also widely being used in highly dynamic ad hoc networks because of its generic feature.

As the wireless nodes have a limited battery life, energy efficiency is the most important design consideration in mobile ad hoc networks. Many multipath routing schemes are possibly exploiting multiple node disjoint routes between any source and destination pair in order to provide aggregated bandwidth, fault-tolerance and load-balancing properties. AOMDV is selected for QoS enhancement due to its edge over other multipath routing protocols.

Due to the increase of mobile users in a dynamic multitasking environment, it is essential to concentrate on maximizing the lifetime of the entire network by finding energy optimized routes using Optimized Minimal Maximal Residual nodal Energy AOMDV (OMMRE-AOMDV), which is the extension of Minimal Maximal Residual nodal Energy AOMDV (MMRE-AOMDV). In this work, the iteration for finding the minimal residual energy of a path does not take the destination node’s energy into account because the destination is the ultimate recipient of all messages. Hence the route update rules of MMRE-AOMDV are slightly modified in OMMRE-AOMDV. The routing table of OMMRE-AOMDV carries an additional field called **re_energy** which carries minimal nodal residual energy. It reduces the energy consumption, average end-to-end delay and normalized routing overhead. It also reduces the routing overhead better than AOMDV and increases the routing overhead better than MMRE-AOMDV. It improves the packet delivery ratio and throughput.

Secondly, all routing protocols (both single and multipath) use Link Expiration Time (LET) for measuring link stability. When a link between nodes is alive (the LET of that link along the path has not expired) but is not within the transmission range, it fails to transmit data. In addition to this, the Cumulative Expected Transmission Count (CETX) of the path has been used along with the traditional metric hop count for selecting link reliable shortest multiple paths, called the Link Reliable Multipath Routing (LRMR) protocol. Hence the route update rules of AOMDV are slightly modified in LRMR. The routing table of LRMR carries an additional field called **cetx** which carries the cumulative expected transmission count. Simulation results reveal the effectiveness of the LRMR protocol.

Thirdly, a node failure occurs when the minimal nodal residual energy of the path does not meet the energy required for data transmission. In addition to this, the Cumulative Expected Transmission Energy (CETE) of the path has been considered for selecting link reliable energy efficient routes between any source and destination pair for data transmission. Thus the proposed work uses an integrated routing metrics approach consisting of the Path Length, the Path-Link Quality Estimator (P-LQE) and a novel Path-Node Energy Estimator (P-NEE) for selecting link reliable energy efficient multiple routes for data transmission, called the Link Reliable Energy Efficient AOMDV (LR-EE-AOMDV) routing protocol. Hence the route update rules of LRMR are slightly modified in LR-EE-AOMDV. The routing table of LR-EE-AOMDV carries three additional fields called **cetx**, **cete** and **mre** which carry the cumulative expected transmission count, cumulative expected transmission energy and minimal nodal residual energy respectively. Each RREQ and RREP of LR-EE-AOMDV carries three additional fields, namely **CETX**, **CETE** and **re_energy**. From the simulation results, it is found that the LR-EE-AOMDV routing protocol outperforms LRMR, AOMDV, MMRE-AOMDV and OMMRE-AOMDV routing protocols.

Finally, the deployment of conversational real-time applications like VoIP and video conferencing faces new challenges on the Internet. The quality of video delivered over the Internet has been determined in terms of Quality of Service (QoS) and Quality of Experience (QoE). QoS includes the Packet delivery ratio, End-to-end delay, Throughput, etc. QoE is a qualitative measure of videos transmitted over the Internet such as the **PSNR (Peak Signal-to-Noise Ratio)**, **MOS (Mean Opinion Score)**, etc.

The proposed protocols have been evaluated in the More Realistic Video Streaming Environment using the EvalVID Evaluation Framework. Among them, the LR-EE-AOMDV easily outperforms other protocols.

P. Periyasamy

ACKNOWLEDGEMENTS

This book is one of the research outputs of the project "*Design and development of Link Reliable Energy Efficient Ad hoc On-demand Multipath Distance Vector (LR-EE-AOMDV) routing protocol for Mobile Ad hoc Networks*", realized by Dr. E. Karthikeyan, Assistant Professor and Head of the Computer Science Department, Government Arts College, Udumalpet, Tirupur, Tamil Nadu, India, of P. Periyasamy, in the period 2010-2016. I feel immensely happy to share my gratitude to my wife Mrs. D. Priya, P.G. Assistant in English. As for my wife, I find it difficult to express my appreciation because it is so boundless. She is my most enthusiastic cheer leader. Without her love and support I would be lost. I am grateful to her not just because she has given up so much to make my career a priority in our lives, but because she has been with me through the ups and downs of the entire research process. She has shared this entire amazing journey with me.

I also wish to thank Sue Morecroft for her valuable proof-reading. It would not have been possible to finalize this book without the dedicated, timely, and always kind support of Hannah Fletcher, Camilla Harding, Adam Rummens, Amanda Millar and Victoria Carruthers at Cambridge Scholars Publishing. The views expressed in the seven chapters reflect the innovations and contributions of the author in the field of Wireless Networks.

P. Periyasamy
Bharathiar University, Tamil Nadu, India, May 2018

CHAPTER ONE

GETTING STARTED

1.1 Mobile Ad hoc Networks

Rapid deployment of independent mobile users will be the need of the next generation of wireless communication systems. A Mobile Ad hoc NETwork (MANET) is one of the most vibrant and active research fields in wireless communication systems. A MANET [1, 2] is a collection of mobile devices by wireless links forming a dynamic topology without much physical network infrastructure such as routers, servers, access points/cables or centralized administration as shown in Figure 1.1.

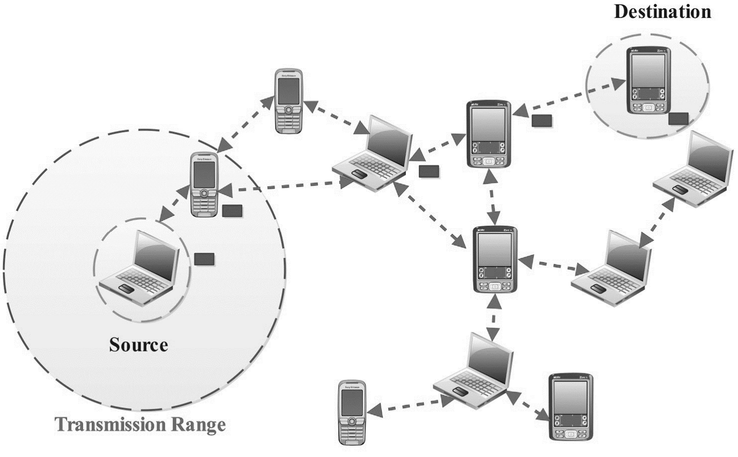

Figure 1.1 A mobile ad hoc network

The nodes of MANETs [3] intercommunicate through single-hop and multi-hop paths in a peer-to-peer fashion. Intermediate nodes between a pair of communicating nodes act as routers. Hence each mobile device functions as a router as well as a node. Some of the wireless devices forming a MANET are PDAs, laptops, mobile phones, smart phones, tablets, etc.

1.2 Characteristics of MANETs

A MANET is distinguished from other types of networks by the following characteristics [4]:

(i) **Self-creation, self-organization and self-administration:** Each node in a MANET does not require extensive knowledge of network parameters prior to joining the network and has autonomous processing capabilities and moves independently in any direction. Due to the lack of infrastructure or central administration, nodes should be able to form themselves into a network.

(ii) **Dynamic topology:** Since all nodes of a MANET are free to move, the network topology may change rapidly at unpredictable times. As nodes move in and out of range of each other, some links break while new links between nodes are created.

(iii) **Unreliable wireless medium:** Compared to the wired network, the communication through the wireless medium is unreliable and subject to errors. Also, due to varying environmental conditions such as high levels of electro-magnetic interference (EMI) or inclement weather, the quality of the wireless link may be unpredictable.

(iv) **Multi-hopping:** Nodes in a MANET use the wireless channel to transmit data, and due to the limited number of a node's neighbors, intermediate nodes are used to relay the packets.

(v) **Resource-constrained nodes:** Nodes in a MANET are typically battery powered as well as limited in storage and processing capabilities. Moreover, they may be situated in areas where it is not possible to re-charge and thus have limited lifetimes. Because of these limitations, they must have algorithms which are energy efficient as well as operating with limited processing and memory resources. The available bandwidth of the wireless medium may also be limited because nodes may not be able to sacrifice the energy consumed by operating at full link speed.

(vi) **Scalability:** In some applications (e.g., battlefield deployments), a MANET may grow up to several thousand nodes. A MANET suffers from scalability problems in channel capacity, because channel capacities are very limited and the maximum use of channel capacity can be reached faster. Due to the multi-hopping nature of MANETs, their scalability is related to the routing protocols they employ.

1.3 Applications of MANETs

MANETs [7] are very useful in many application environments where immediate infrastructure establishment is difficult. Some of the application areas of MANETs are given below:

(i) **Disaster recovery:** Responding to emergency situations such as disaster recovery has been yet another naturally fitting application in the ad hoc networking domain. During the time of emergencies, several mobile users (policemen, firefighters, and first response personnel) with different types of wireless devices need to not only communicate but also to maintain the connectivity for a long period of time.

(ii) **Commercial and civilian environments:** A MANET is used to make electronic payments anytime and anywhere in E-commerce. It is also used to facilitate dynamic database access and construction of mobile offices in Business. In Vehicular networks, it avoids accidents by transmitting information about road and weather conditions. It is also used in the taxi cab network, inter-vehicle networks, communication in sports stadiums, trade fairs and shopping malls. It is also used to exchange information among the networks of visitors at airports.

(iii) **Home and enterprise networking:** Wireless computers can create an ad hoc network environment where each node can communicate with others without taking their original point of attachment into consideration by assigning multiple IP addresses to each wireless device in order to recognize their services such as Home/office wireless networking, conferences, meeting rooms, Personal Area Networks (PAN) and Networks at construction sites. Collaborative computing is the most important application where the mobile users need to collaborate on a project outside the typical office environment.

(iv) **Education:** A MANET is used in Universities and campus settings, virtual classrooms and communications during meetings or lectures.

(v) **Tactical networks:** Automated battlefields, Military communication and operations can also create an ad hoc network environment where nodes can communicate with each other in a secured fashion.

(vi) **Entertainment:** The services offered under this category are Multi-user games, Wireless Point-to-Point (P2P) networking, Outdoor Internet access, Robotic pets, and Theme parks.

(vii) Sensor networks and wildlife monitoring: In home applications, smart sensors and actuators are embedded in consumer electronics for monitoring purposes. Smart sensors are used in Body Area Networks (BAN) and Data tracking of environmental conditions, animal movements, and chemical/biological detection. In hazardous or dangerous situations, it makes sense to distribute groups of sensors with wireless transceivers to obtain critical information about the unknown site by the creation of ad hoc networks of these sensors.

(viii) Embedded computing applications: Several ubiquitous computing internetworking machines offer flexible and efficient ways of establishing communication methods with the help of ad hoc networking. Many of the mobile devices already have add-on inexpensive wireless components, such as PDAs with wireless ports and Bluetooth radio devices. Bluetooth provides a wireless technology built-in to many of the current PDAs and up to eight PDAs, called a *piconet*, can exchange information.

(ix) Automotive/PC Interaction: The interaction between many wireless devices (laptop, PDA, and so on) being used in the car for different purposes can create an ad hoc network in order to carry out tasks more efficiently. An example can be finding the best possible mechanic shop to fix a car problem in a new city on the way to a meeting.

1.4 Issues of MANETs

Due to the limitations in the characteristics of MANETs, the following are the major issues [3, 5, 6]:

(i) Unpredictable link properties: The wireless medium is very unpredictable. Packet collision is intrinsic to the wireless network. Signal propagation faces difficulties such as signal fading, interference, and multipath cancellation. All these properties lead to unpredictable bandwidth and delay of a wireless link.

(ii) Node mobility: Mobility of the nodes creates a dynamic network topology. Links will be dynamically formed when two nodes come into the transmission range of each other and are torn down when they move out of range.

(iii) Limited battery life: Mobile devices generally depend on finite battery sources. Resource allocation for Quality of Service (QoS) provisioning must consider the residual battery power and rate of battery consumption corresponding to resource utilization. Thus, all the techniques for QoS provisioning should be power-aware and power-efficient.

(iv) Hidden and Exposed Terminal Problems: In a MAC layer with the traditional carrier sense multiple access (CSMA) protocol, multi-hop packet relaying introduces the hidden terminal and exposed terminal problems. The hidden terminal problem happens when signals of two nodes, say A and B, that are out of each other's transmission ranges collide at a common receiver, say node C. With the same nodal configuration, an exposed terminal problem will result from a scenario where node B attempts to transmit data (to someone other than A or C) while node C is transmitting to node A. In such a case, node B is exposed to the transmission range of node C and thus defers its transmission even though it would not interfere with the reception at node A.

(v) Route maintenance: The dynamic nature of the network topology and the changing behavior of the communication medium make the precise maintenance of network state information very difficult. Thus, the routing algorithms in MANETs have to operate with inherently imprecise information. Furthermore, in ad hoc networking environments, nodes can join or leave at any time. The established routing paths may break even during the process of data transfer. Thus, the need arises for the maintenance and reconstruction of routing paths with minimal overhead and delay. QoS-aware routing would require the reservation of resources at the routers (intermediate nodes). However, with the changes in topology the intermediate nodes also change, and new paths are created. Thus, reservation maintenance with updates in the routing path becomes cumbersome.

(vi) Security: Security can be considered as one of the most important QoS attributes. Without adequate security, unauthorized access and usage may violate QoS negotiations. The nature of broadcasts in wireless networks potentially results in more security exposure. Since the physical medium of communication is inherently insecure, boundaries of MANETs lead to attacks such as passive eavesdropping, active interfering, and leakage of secret information, data tampering, message replay, message contamination, and denial of service (DoS). So we need to design security-aware routing algorithms for MANETs.

1.5 Routing Protocols of MANETs

Routing is a mechanism by which data packets are forwarded to the next neighbor, who either has a path to the solicited destination or is the destination itself. Routing in wireless networks is distinct from routing in wired networks, in the former the routing of packets happens on a hop-by-hop basis called a multi-hop routing while in the latter routing is done on a single dedicated path.

Among the many issues to be addressed in Section 1.4, the MANET routing is one of the very important problems to be considered. Normally single path routing protocols find an optimal route (single route) between a pair of source and destination. Here a new route discovery is needed for every route break that leads to high overhead and latency.

But multipath routing protocols establish communication from source to destination by having backup routes. During end-to-end communication, if a primary route fails, the backup routes are used for the efficient delivery of messages at their destination. The ad hoc multipath routing protocols can be classified into three major groups based on the routing strategy as shown in Figure 1.2.

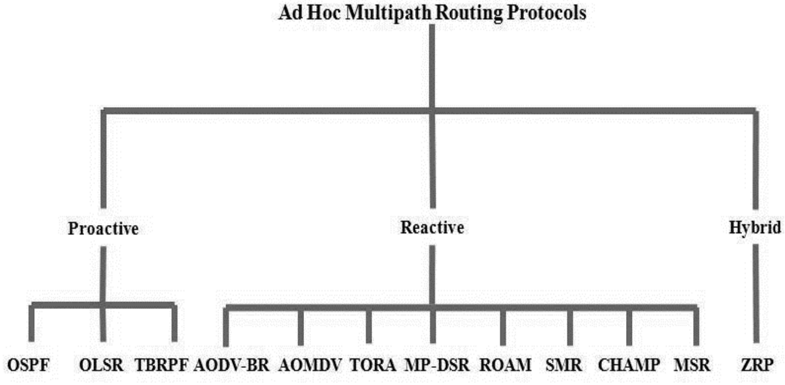

Figure 1.2 Classification of ad hoc multipath routing protocols

1.5.1 Proactive multipath routing protocols

In proactive/table-driven multipath routing protocols, each node maintains up-to-date routing information for each and every node in the network. The routing information is stored in a number of different tables. These tables are periodically updated when the network topology changes or there is any update in the network in order to maintain a consistent network view. The way of detecting and updating routing information is kept in a routing table and the number of routing tables differs from each of these protocols. This section describes the characteristics and functionality of the existing proactive multipath routing protocols.

1.5.1.1 Open Shortest Path First (OSPF)

The two primary characteristics of OSPF [8] are that it is an open protocol, which means its specification is in the public domain and it is a protocol based on the shortest path first (SPF) algorithm, which in turn is termed as Dijkstra's algorithm. Unlike other protocols which use the distance-vector or Bellman-Ford method, OSPF uses the link-state or SPF-based method in order to build and calculate the shortest path to all well-known destinations. The link-state database is formed in the network by flooding the individual link-state advertisements (LSAs) which describe small pieces of the routing domain. The routers in OSPF have identical link-state databases, which are synchronized through a reliable flooding algorithm. The link-state database is used for each router to build a routing table by calculating a shortest-path tree, rooted at the router itself.

In OSPF, with the existence of several equal-cost routes to a destination, the traffic is distributed equally among them. These multiple routes need not be node-disjoints or even link-disjoints. Each node listens to its neighbors via HELLO messages. These messages are not only used for acquiring neighbors, but are also used to keep-alive packets.

The properties of OSPF are [9] (i) working based on Shortest Path First (SPF or Dijkstra's algorithm); (ii) link-state protocol; (iii) common link-state database formed by individual Link-State Advertisements (LSAs); (iv) each node computes a shortest-path tree from the link-state database; (v) each node periodically sends out an LSA; and (vi) multiple paths from source to destination are possible.

1.5.1.2 Optimized Link State Routing (OLSR)

The OLSR [10, 11] protocol is an optimization of a pure link state protocol by compacting the size of the control packets that contain link-state information and reducing the number of transmissions needed to flood those control packets to the entire network. The multipoint relaying technique is used to flood its control messages in an efficient and economical way. The main aim of multipoint relay is to minimize the flooding of broadcast packets in the network by reducing the number of retransmissions in the same region. In OLSR, each node selects a set of 1-hop neighbor nodes, called the multipoint relays (MPRs) of that node, which retransmits its packets. The neighbors of any node N do not retransmit the broadcast packets received from node N if they are not in the MPR set whereas they can read and process packets. Each node maintains a set of neighbors for the retransmission of packets called MPR Selectors.

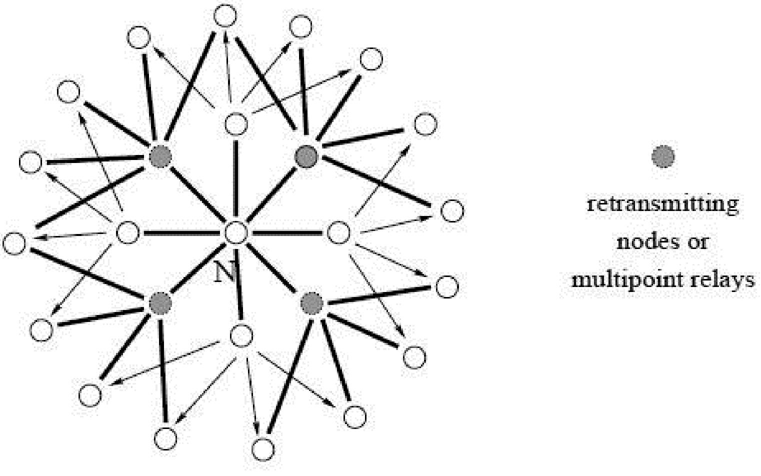

Figure 1.3 Selection of MPR around node N

All the neighbor nodes (radio range) within two hops away from N must be covered by the MPRs of N. These two-hop neighborhoods of N must have bi-directional links with the MPRs of N. The selection of MPR around a node N is shown in Figure 1.3.

Each node N periodically broadcasts HELLO messages to its one-hop neighbors for selecting the MPRs. Each HELLO message has a list of neighbors that are connected to N via bidirectional links and it also has the list of neighbors that are heard by N but are not connected via bidirectional links. On receiving the HELLO message, each node can learn the link-state information of all neighbors up to two hops.

The MPRs are selected via the information contained in a neighbor table. Each node is broadcasting specific control messages called Topology Control (TC) messages. Each TC message originating from a node N has the list of MPRs of N with a sequential number and is forwarded only by the MPRs of the network. Each node maintains a topology table which is constructed from the information obtained from the TC messages for representing the topology of the network. Each node also maintains a routing table in which each entry in the routing table corresponds to an optimal route, in terms of the number of hops, to a particular destination. Each entry has a destination address, a next-hop address, and the number of hops to the destination. The routing table is constructed based on the information available in the neighbor table and the topology table. Each route is a sequence of hops through the multipoint relays from every source to destination.

The properties of OLSR are [9] (i) optimization of pure link-state protocol; (ii) neighbors are discovered via HELLO messages containing all neighbors and link-states; (iii) routes are created from multipoint relays (MPRs) (intermediate nodes are all MPR nodes); (iv) MPRs are 1-hop neighbors via a bi-directional link covering all 2-hop neighbors; (v) multiple routes to the destination are possible; and (vi) no complete routes are known at the source (only next hops).

1.5.1.3 Topology Broadcast Based on Reverse Path Forwarding (TBRPF)

TBRPF [12] is a link-state based routing protocol, which uses the concept of reverse-path forwarding to broadcast link-state updates in the reverse direction along with the spanning tree formed by minimum-hop paths from all nodes to the source of the update. Unlike a pure link-state routing algorithm, TBRPF requires only the non-leaf nodes in the broadcast tree to forward update packets. Hence the TBRPF generates less update traffic than pure link-state routing algorithms. The use of a minimum-hop tree makes the broadcast tree more stable than a shortest-path tree and also has less communication cost to maintain the tree. In TBRPF, each node maintains a list of its one-hop neighbors and a topology table. In the topology table, each entry for a link contains the most recent cost and sequence number associated with that link. With this information each node can compute a source tree in order to provide shortest paths to all reachable remote nodes.

The properties of TBRPF are [9] (i) the broadcast link-state is updated with the help of a minimum-hop spanning tree; (ii) a minimum-hop spanning tree is rooted at the update of the source; (iii) a minimum-hop tree is maintained with info received from the tree itself; (iv) each node is provided with full topology information; and (v) multiple paths to destinations are possible.

1.5.2 Reactive multipath routing protocols

Reactive or on-demand multipath routing protocols are reducing the overheads in proactive multipath protocols by maintaining the information for active routes only. This means that the routes are determined and maintained whenever nodes need to send data to a particular destination. Route discovery happens by flooding route request packets through the network. When a node with a route to the destination (or the destination itself) is reached, it sends a route reply packet back to the source node using link reversal if the route request has travelled through bi-directional links or by piggy-backing the route via flooding. The two categories of reactive multipath protocols based on routing strategy [5] are *(i) source routing* and *(ii) hop-by-hop routing*.

In **source routing** [5], the complete source to the destination address is carried by each data packet. The intermediate nodes then forward these packets based on the information kept in the header of each packet. It means that the intermediate nodes need not maintain up-to-date routing information for each active route in order to forward the packet towards its destination. Moreover, these nodes need not maintain the neighbor connectivity through periodic beaconing messages. The major drawback of the source routing protocols is that they do not perform well in large networks due to two main reasons: (i) the probability of route failure is directly proportional to the growth of the intermediate nodes in each route; and (ii) the amount of overhead carried in the header of each data packet depends upon the number of intermediate nodes in each route. These protocols may not scale well in large networks with significant levels of multi-hopping and high levels of mobility.

In **hop-by-hop routing (also called point-to-point routing)** [5], only the destination address and the next hop address are carried by each data packet. Moreover, each intermediate node in the path to the destination uses its routing table in order to forward each data packet towards its destination. The main advantage of this strategy is that the routes are adaptable to the dynamically changing environment of MANETs, since each node can update its routing table upon receiving the fresh topology information and hence the data packets are forwarded over fresh and better routes. The fresh route requires a few route recalculations during data transmission. The main disadvantage of this strategy is that each intermediate node must store and maintain routing information for each active route and each node may need to be aware of its surrounding neighbors through the use of beaconing messages. Numerous reactive routing protocols have been proposed to increase the performance of reactive routing. This section describes the characteristics and functionality of existing reactive multipath routing protocols.

1.5.2.1 Ad hoc On-demand Distance Vector—Backup Routing (AODV-BR)

The AODV-BR [13] protocol uses the same AODV's [14] RREQ (route request) propagation process. When a source needs to initiate a data session to a destination and there is no route to that destination in its route cache, it searches for a route by flooding a RREQ packet. Each of these RREQ packets has a unique identifier in order to detect and drop duplicate packets by the nodes. When an intermediate node is receiving a non-duplicate RREQ, it records the previous hop and the source node information in its routing table (i.e., backward learning) and then broadcasts the packet, or sends back a RREP (route reply) packet to the source when a route to the destination is known. On receiving the first RREQ or subsequent RREQs that traversed a better route (fresher or shorter route) than the previously replied route, the destination node sends a RREP through that selected route.

The slight modification (for the consideration of the broadcast nature of wireless communications) in the AODV’s RREP (route reply) phase establishes the mesh and multipath without transmitting any extra control message. When a node that is not part of the selected route overhears a RREP packet not directed to itself, transmitted by the neighbor (on the primary routes), it records the sending neighbor as the next hop to the destination in its alternate route table. In this way, a node may receive numerous RREPs for the same route when it is within the radio propagation range of more than one intermediate node of the primary route. Therefore, it chooses the best route among them and inserts it into the alternate route table. When the source of the route is receiving the RREP packet, the primary route between the source and the destination has been established for instant use. Nodes that have an entry to the destination in their alternate route table are forming the mesh. The primary and alternate routes together are forming a mesh which is similar to a fish bone as shown in Figure 1.4.

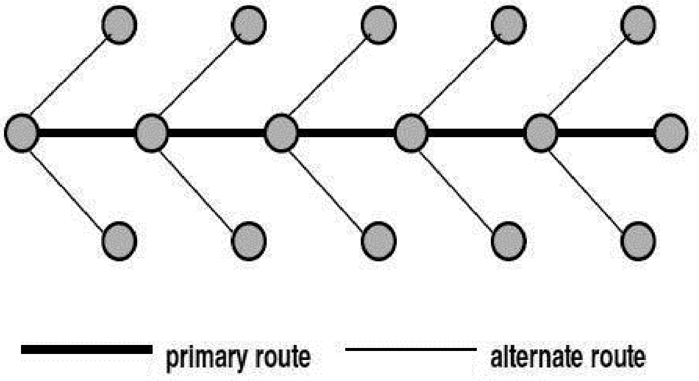

Figure 1.4 Multiple routes forming a fish bone structure

For example, the node Z forwards the packet from B to the destination D directly without sending it through node C if the link between nodes B and C fails. Hence the packet is delivered through the path <S--A--B--Z--D> and has the same hop length as the primary route <S--A--B--C--D> as shown in Figure 1.5.

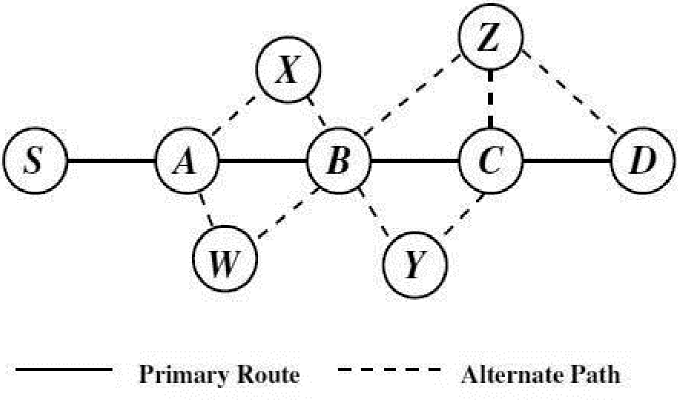

Figure 1.5 An alternate path with the same path length as the primary route

The properties of AODV-BR are [9] (i) the extension of AODV; (ii) flood RREQs with unique IDs hence the duplicates are discarded; (iii) each node maintains a backup route(s) in its alternative route table; (iv) distance vector protocol, so only the destination, the next hop and the number of hops are known; (v) alternative (backup) route(s) used when the primary fails; (vi) multiple complete routes are not available; (vii) alternative route(s) determined in the RREP phase by overhearing RREPs to other nodes; and (viii) a source does not know the complete route(s) information.

1.5.2.2 Ad hoc On-demand Multipath Distance Vector Routing (AOMDV)

AOMDV [15] is the extension of AODV [14] so as to eliminate the occurrence of frequent link failures and route breaks in highly dynamic ad hoc networks. It adds some extra fields in routing tables and control packets, and follows two rules during a route discovery phase in order to compute loop-free and link-disjoint multiple routes between source and destination. The rules are (i) a route update rule establishes and maintains multiple loop-free paths at each node; and (ii) a distributed protocol finds link-disjoint paths. Link failures may occur because of node mobility, node failures, congestion in traffic, packet collisions, and so on.

There is no common link among the multiple routes between a source and destination pair in the link-disjoint routes. To achieve loop-freedom, every node maintains a variable called the advertised hop count. The advertised hop count is added in each RREQ (route request) or RREP (route reply) and in addition to the routing table has the usual fields that are used for AODV. The advertised hop count field of a node is set to the length of the longest available path to the destination expressed in terms of the number of hops if it initiates a RREQ or RREP with a particular destination sequence number and remains unchanged till the associated destination sequence number is changed.

The loop-freedom rule says that if a node receives a RREQ/RREP for a particular destination with a destination sequence number: (a) it should update its routing information with the information obtained from the received RREQ/RREP if the destination sequence number is higher than the one stored in its routing table; (b) it can re-send the received RREQ/RREP when the advertised hop count in the RREQ/RREP is greater than the corresponding value in its routing table and if the destination sequence number is equal to the one stored in its routing table; and (c) it can update its routing table with the information contained in the received RREQ/RREP when the advertised hop count in the RREQ/RREP is less than the corresponding value in its routing table if the destination sequence number is equal to the one stored in its routing table.

For link-disjointness, each node maintains a route list in its routing table for a particular destination and its route list contains the next hop, last hop, and hop count information for the destination. The next hop represents a downstream neighbor through which the destination can be reached. The last hop refers to the node immediately preceding the destination. The hop count is used to measure the distance from the node to the destination through the associated next and last hops. The link-disjointness among all the paths can be achieved if a node can ensure that those paths to a destination from itself differ in their next and last hops. Using this observation, AOMDV ensures link-disjointness among multiple routes for the same source and destination pair and also adds a last hop field in each RREQ and RREP.

In AOMDV, all copies of RREQ are examined for the potential alternate reverse paths during route discovery. On receiving a RREQ, an intermediate node creates a reverse path if the RREQ satisfies the rules for loop-freedom and link-disjointness. Moreover, it checks if it has one or more valid next hop entries for the destination. The intermediate node generates a RREP, and sends it back to the source along the reverse path if such an entry is found. Otherwise, it rebroadcasts the RREQ. The destination follows the same rules for creating reverse paths if it receives RREQ copies. Unlike the intermediate nodes, it generates a RREP for every copy of a RREQ that arrives via a loop-free path, for increasing the possibility of finding more disjoint routes.

The AOMDV routing protocol updates its routing table periodically on-demand upon receiving a RREQ/RREP based on the following route update rules as shown in **Algorithm 1** [15].

Algorithm 1: Route Update Rules of AOMDV Protocol [15]

```
if ($seqnum_i^d < seqnum_j^d$) then
  $seqnum_i^d := seqnum_j^d$;
  if ($i \neq d$) then
      $advertised\_hopcount_i^d := \infty$;
  else
      $advertised \_hopcount_i^d := 0$;
  end if
  $route \_list_i^d = NULL$;
  insert ($j$ , $advertised\_hopcount_j^d$ +1) into $\mathrm{route\_list}_i^d$;
else if ($seqnum_i^d = seqnum_j^d$) and (($advertised\_hopcount_i^d$,i) > ($advertised\_hopcount_j^d$,j)) then
   insert ($j$ , $advertised\_hopcount_j^d$ +1) into $\mathrm{route\_list}_i^d$;
end if
```

The properties of AOMDV are [9] (i) the extension of AODV; (ii) RREQs from different neighbors of the source are accepted at intermediate nodes; (iii) multiple link-disjoint (node-disjoint) routes are created; (iv) the maximum hop count to each destination is called an advertised hop count which is used to avoid loops; (v) multiple routes are established in a single route discovery process; (vi) nodes maintain next-hop information for destinations (may have multiple next-hops); (vii) a source does not know complete route(s) information; and (vii) the occurrence of frequent link failures and route breaks in highly dynamic ad hoc networks is eliminated.

1.5.2.3 Temporally-Ordered Routing Algorithm (TORA)

TORA [16] is a highly adaptive, distributed routing protocol based on the Light-weight Mobile Routing (LMR) protocol, which uses similar link reversal, route repair and the query/reply procedure to create DAGs as in LMR in order to provide multiple loop-free paths for a source and destination pair. The two main advantages of TORA are (1) the far-reaching control messages to a set of neighboring nodes are reduced even if the topology change has occurred; and (2) it also provides multicasting support even if this is not incorporated into its basic operation. This protocol has three basic functions: route creation, route maintenance and route erasure.

A **directed acyclic graph (DAG)** is created based on a **"height"** metric, in order to establish and maintain routes. The height of a node is defined by the parameters such as a reference level and a delta with respect to the reference level, which differs per destination and also one DAG per destination. The height of the destination is always zero, whereas the heights of other intermediate nodes increase by 1 towards the source node via increasing the delta value. In TORA, the new routes are created using **query (QRY)** and **update (UPD)** packets. Each node initiates a route by broadcasting a QRY to its neighbors. The QRY is re-broadcasted through the network as long as it reaches the destination or a node has a route to the destination. When a node is the destination or a route to the destination is replied via UPD packets back to the source, which contains its height with respect to the destination. On receiving the UPD, each node sets its own height, which is greater than the height sent from the neighbor as shown in Figure 1.6 (a).

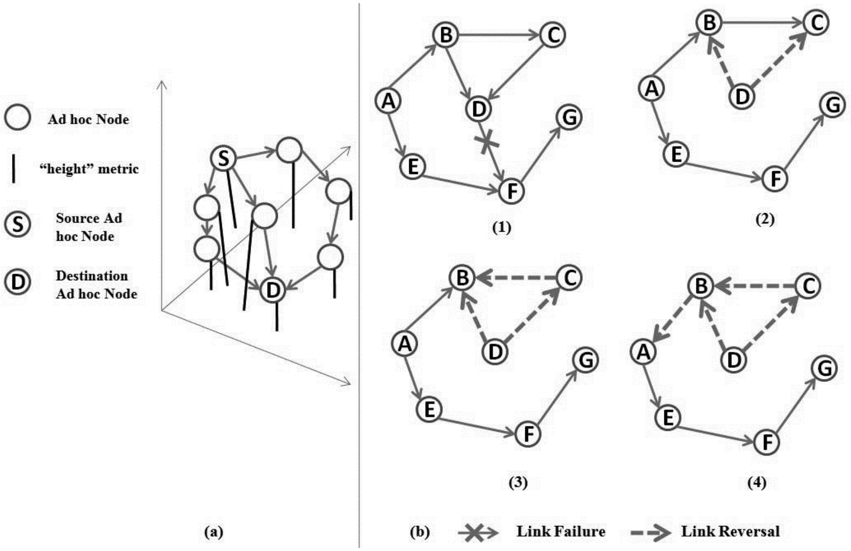

Figure 1.6 (a) Route creation; and (b) Route Maintenance in TORA

From Figure 1.6 (b), a node generates a new reference level based on the propagation of the reference level, by neighbors' effective co-ordination and structured reaction, if it loses its last downstream link. The node erases the invalid routes to the destination by flooding a clear (CLR) packet throughout the network. Therefore, the links are reversed in order to adopt the new reference level by changing the direction of links if a node has no downstream links. Since the "height metric" depends on the logical time of a link failure (time-dependent), all nodes have a common clock. TORA's metric is a quintuple which consists of: (1) the logical time of the link failure; (2) the unique ID of the node defining the new reference level; (3) a reflection indicator bit; (4) a propagation ordering parameter; and (5) the unique ID of the node. The first three elements represent the reference level. The internodal co-ordination of TORA can be quite unstable due to link failures. The link failures can be avoided by the route erasure and link reversal procedures.

The properties of TORA are [9] (i) the routes are created using a DAG; (ii) QRYs are sent and replied to with UPDs to create DAG(s); (iii) a DAG is formed using height metrics; (iv) the link failures get new reference levels (heights) and links are reversed to notify the source; (v) all nodes need to have a common clock; (vi) it provides multiple routes to the destination; (vii) there may not be optimum routes between a source and destination pair; and (viii) a source does not know complete route(s) information.

1.5.2.4 MultiPath Dynamic Source Routing (MP-DSR)

MP-DSR [17] is a QoS-aware multipath source routing protocol, based on the Dynamic Source Routing protocol (DSR) which creates and selects routes based on a newly defined QoS metric, end-to-end reliability. This protocol computes a set of routes in order to satisfy a minimum end-to-end reliability requirement. In MP-DSR, multiple node-disjoint paths for data transmission are discovered for the specific end-to-end reliability requirement. The probability of having a successful transmission between two nodes in the network within the specific period is called end-to-end reliability. Unlike DSR [18], the MP-DSR provides a minimum end-to-end requirement based on the determination of the number of paths needed (m_0) and the lowest path reliability ($\prod_{lower}$) requirement by every path for route discovery. The relationship between m$_0$ and $\prod_{lower}$ is that there are fewer paths between a source and a destination (m$_0$ is low), more reliable paths are required ($\prod_{lower}$ is higher) to ensure the end-to-end reliability. The $\prod_{lower}$ is computed using $\prod_{lower} = 1 - \sqrt[m_0]{1 - P_u}$, where $P_u = P(t)$ is the required end-to-end reliability and $P(t)$ is the resulting end-to-end reliability. The link availability of m_0 neighbors is greater than $\prod_{lower}$ used to determine m_0. To keep the data and RREQ traffic at a minimum end-to-end reliability requirement, this protocol starts the route discovery process by setting m_0 to 1 and incrementing it by 1 every time as long as the neighbors did not satisfy $\prod_{lower}$. This means that the procedure is stopped if the required end-to-end reliability is met. More reliable paths are preferred from the fewer paths between a source and destination pair if $\prod_{lower}$ is higher and then the source sends m_0 and RREQs, each of which contains $\prod_{lower}$, the path traversed, the corresponding path reliability, etc.

On receiving the RREQ message, each node checks whether the message meets the path reliability requirement. If so, that node updates the RREQ message and forwards multiple copies of this message based on the number of neighbors that can receive this RREQ without failing the path reliability, and bounding with m_0 to restrict the message to be forwarded across the network. The destination selects node-disjoint paths and replies sending RREP messages back to source along these disjoint paths when it receives the RREQ messages. The source node starts data transmission via the routes from which it receives the RREPs.

The properties of MP-DSR are [9] (i) the extension of DSR; (ii) source routing, so that the packets contain a complete path in their header; (iii) the source has complete route information; (iv) QoS awareness: the probability of having a successful transmission between two nodes in the network within the specific period is called end-to-end reliability; (v) it provides multiple node-disjoint routes between a source and a destination pair; (vi) an intermediate node compares the received RREQs with the required end-to-end reliability in order to determine whether they will be forwarded or discarded; and (vii) the destination sends RREPs back to the source along the node-disjoint paths which are meeting the end-to-end reliability so that the source initiates the data transmission.

1.5.2.5 Routing On-demand Acyclic Multipath (ROAM)

The ROAM [19] routing protocol is an extension of the diffusing update algorithm (DUAL) [20] in order to provide on-demand routing. It uses internodal coordination along directed acyclic subgraphs defined by the routers' distance to the destination. This operation is called a *"diffusing computation"*. It also eliminates the search-to-infinity problem present in some of the on-demand routing protocols by stopping multiple searches if the required destination is no longer reachable. In the ROAM, each router maintains entries in a routing table to destinations by flowing data packets through them (i.e. the router is a node which completes/connects a router to the destination) to reduce the significant amount of storage space and