Mobile Ad Hoc Networks

Current Status and Future Trends

Edited by
Jonathan Loo, Jaime Lloret Mauri, and Jesús Hamilton Ortiz

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Mobile Ad Hoc Networks

Current Status and Future Trends

Mobile Ad Hoc Networks

Current Status and Future Trends

Edited by

Jonathan Loo, Jaime Lloret Mauri, and Jesús Hamilton Ortiz

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
Version Date: 20111026

International Standard Book Number: 978-1-4398-5650-5 (Hardback)

Library of Congress Cataloging-in-Publication Data

Mobile ad hoc networks : current status and future trends / editors, Jonathan Loo, Jaime Lloret Mauri, Jesus Hamilton Ortiz.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-4398-5650-5 (hardback)
1. Ad hoc networks (Computer networks) 2. Mobile communication systems. I. Loo, Jonathan. II. Lloret Mauri, Jaime. III. Ortiz, Jesus Hamilton.

TK5105.77.M63 2011
004.6'167--dc23 2011038265

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

Contributors

Ali Naser Al-Khwildi
Commission of Media and Communications (CMC)
Jadreiah, Iraq

Marcelo Atenas
Universidad Politécnica de Valencia
València, Spain

Luigi Atzori
Department of Electrical and Electronic Engineering (DIEE)
University of Cagliari
Cagliari, Italy

Saeed Bastani
School of Information Technologies
University of Sydney
New South Wales, Australia

Deniz Cokuslu
Ege University International Computer Institute
Bornova, Izmir, Turkey

and

Computer Engineering Department
Izmir Institute of Technology
Urla, Izmir, Turkey

Jose Costa-Requena
School of Electrical Engineering
Department of Communications and Networking
Aalto University
Aalto, Finland

Orhan Dagdeviren
Computer Engineering Department
Izmir University
Uckuyular, Izmir, Turkey

and

Ege University International Computer Institute
Bornova, Izmir, Turkey

Kayhan Erciyes
Computer Engineering Department
Izmir University
Uckuyular, Izmir, Turkey

Mahmood Fathy
Computer Engineering Department
Iran University of Science and Technology
Narmak, Tehran, Iran

Dominique Gaiti
Autonomic Networking Environment
ICD/ERA CNRS UMR-STMR 6279
University of Technology of Troyes
Troyes, France

Miguel García
Universidad Politécnica
de Valencia
València, Spain

Hasan Gumus
Aselsan Ltd. Corporation
Ataturk Organize Sanayi Bolgesi
Cigli, Izmir, Turkey

Julie Hsieh
Department of Computer Science
San José State University
San José, California

Katherine Isaacs
Department of Computer Science
San José State University
San José, California

Bego Blanco Jauregui
Department of Computer Languages
and Systems
University of the Basque Country

and

EUITI Bilbao
Plaza de la Casilla
Bilbao, Spain

Shafiullah Khan
School of Engineering and Information
Sciences,
Computer Communications Department,
Middlesex University,
London, United Kingdom

and

Kohat University of Science and Technology
(KUST)
Kohat, Pakistan

Lyes Khoukhi
Autonomic Networking Environment
ICD/ERA CNRS UMR-STMR 6279
University of Technology of Troyes
Troyes, France

Ilias Kiourktsidis
School of Engineering and Design
Brunel University
London, United Kingdom

Panagiotis Kokkinos
Research Academic Computer Technology
Institute,
University of Patras
Patras, Greece

Grigorios Koulouras
Department of Electronics
Technological Education Institute (T.E.I) of
Athens
Athens, Greece

Raquel Lacuesta
Computer Science and Systems Engineering
University of Zaragoza
Teruel, Spain

Bernardo Leal
Department of Industrial Technology,
Simón Bolivar University
Miranda State, Venezuela

Jaime Lloret
Universidad Politécnica de
Valencia
València, Spain

Jonathan Loo
School of Engineering and Information
Sciences
Computer Communications
Department
Middlesex University
London, United Kingdom

Juan Carlos López
Computer Architecture and Networks,
School of Computer Science,
University of Castilla-La Mancha
Ciudad Real, Spain

Fidel Liberal Malaina
Department of Electronics and
Telecommunications
University of the Basque Country

and

ETSI
Alameda de Urkijo S/N
Bilbao, Spain

Ali El Masri
Autonomic Networking Environment
ICD/ERA CNRS UMR-STMR 6279
University of Technology of Troyes
Troyes, France

Mohammad Reza Meybodi
Department of Computer Engineering and IT
Amirkabir University of Technology
Tehran, Iran

Melody Moh
Department of Computer Science,
San José State University
San José, California

Jesús Hamilton Ortiz
Computer Architecture and Networks,
School of Computer Science,
University of Castilla-La Mancha
Ciudad Real, Spain

Guillermo Palacios
Computer Science and Systems Engineering
University of Zaragoza
Teruel, Spain

Christos Papageorgiou
Research Academic Computer Technology
Institute
University of Patras
Patras, Greece

Jorge Luís Perea Ramos
System Engineering
University of Cartagena
Cartagena, Colombia

Julio Cesar Rodríguez Ribons
System Engineering
University of Cartagena
Cartagena, Colombia

Sandra Sendra
Universidad Politécnica de
Valencia
València, Spain

Javad Akbari Torkestani
Department of Computer Engineering
Islamic Azad University
Arak Branch, Arak, Iran

Emmanouel Varvarigos
Research Academic Computer Technology
Institute
University of Patras
Patras, Greece

Luiz Filipe M. Vieira
Computer Science Department
Federal University of
Minas Gerais
Belo Horizonte, Brazil

Onur Yılmaz
Ege University International
Computer Institute
Bornova, Izmir, Turkey

and

Computer Engineering Department
Izmir University of Economics
Balcova, Izmir, Turkey

Saleh Yousefi
Computer Department
Faculty of Engineering
Urmia University
Urmia, Azarbaijan, Iran

Christos K. Zachos
IP Partners
Thessaloniki, Greece

I

FUNDAMENTAL OF MANET—MODELING AND SIMULATION

Chapter 1

Mobile Ad Hoc Network

Jonathan Loo, Shafiullah Khan, and Ali Naser Al-Khwildi

Contents

1.1 Introduction

Wireless industry has seen exponential growth in the last few years. The advancement in growing availability of wireless networks and the emergence of handheld computers, personal digital assistants (PDAs), and cell phones is now playing a very important role in our daily routines. Surfing Internet from railway stations, airports, cafes, public locations, Internet browsing on cell phones, and information or file exchange between devices without wired connectivity are just a few examples. All this ease is the result of mobility of wireless devices while being connected to a gateway to access the Internet or information from fixed or wired infrastructure (called *infrastructure-based wireless network*) or ability to develop an on-demand, self-organizing wireless network without relying on any available fixed infrastructure (called *ad hoc networks*). A typical example of the first type of network is office wireless local area networks (WLANs), where a wireless access point serves all wireless devices within the radius. An example of mobile ad hoc networks (MANETs) [1] can be described as a group of soldiers in a war zone, wirelessly connected to each other with the help of limited battery-powered devices and efficient ad hoc routing protocols that help them to maintain quality of communication while they are changing their positions rapidly. Therefore, routing in ad hoc wireless networks plays an important role of a data forwarder, where each mobile node can act as a relay in addition to being a source or destination node.

1.2 Wireless Networks

Wireless networks can be broadly categorized into two classes: infrastructure-based wireless networks and infrastructure-less wireless networks (ad hoc wireless networks). Infrastructure-based wireless networks rely on an access point, which is a device that acts as a bridge between the wired and wireless networks. With the help of such an access point, wireless nodes can be connected to the existing wired networks. Examples of infrastructure-based wireless networks are wireless networks set up in airports, offices, homes, and hospitals, where clients connect to the Internet with the help of an access point. Figure 1.1 shows an infrastructure mode wireless network.

The other type of wireless networks does not rely on fixed infrastructure, and it is more commonly called an *ad hoc wireless network*. The word *ad hoc* can be translated as "improvised" or "not organized," which often has a negative meaning; however, in this context the sense is not negative, but it only describes the dynamic network situation. An ad hoc mode is used to connect wireless clients directly together, without the need for a wireless access point or a connection to an existing wired network. There are different example of MANET in ad hoc mode such as building-to-building, vehicle-to-vehicle, ship-to-ship etc.; they communicate with each other by relying on peer-to-peer routing. A typical ad hoc mode wireless network is shown in Figure 1.2.

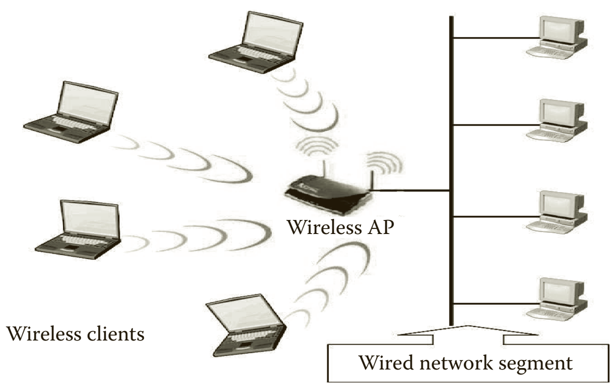

Figure 1.1 Infrastructure mode wireless network.

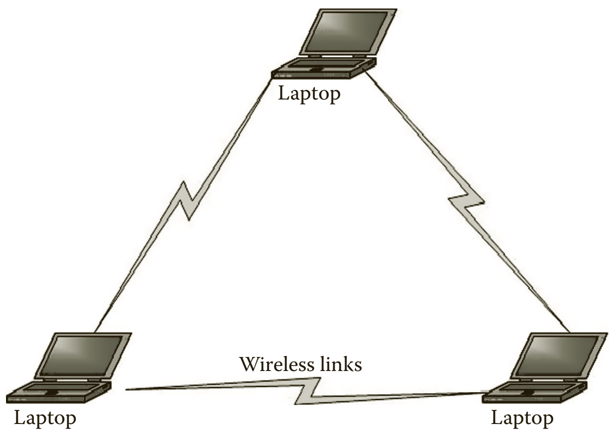

Figure 1.2 Ad hoc mode wireless network.

In wireless network communication, nodes communicate with other nodes via wireless channels. There are two important metrics that are used in the wireless networks: spectrum ranges and different radio frequencies. For example, IEEE 802.11a [2], IEEE 802.11b [3], and IEEE 802.11g [4] use a radio frequency of 5.15–5.35, 2.4–2.58, and 2.4–2.58 GHz, respectively. The signal strength in a wireless medium decreases when the signal travels further beyond a certain distance, and it reduces to the point where reception is not possible [5]. Several medium access (MAC) layers are used in wireless networks to control the use of the wireless medium: Bluetooth MAC layer 802.15 [6] and WLAN MAC layer 802.11 [3]. The topology of the wireless network can be different with time because of the mobility feature. Besides the concept of mobility, another type of mobility is defined and well studied. For example, in wireless networks, the hosts or subnets may be moved from one place to another. Traditional networks require reconfiguration of the IP address used by these hosts or subnets at the new place. A network enabled with mobile IP [7] allows these hosts or subnets to move without any manual IP address reconfiguration. The hosts can remain connected while they are moving around.

1.3 Mobile Ad Hoc Network

A *wireless ad hoc network* is a collection of two or more wireless devices having the capability to communicate with each other without the aid of any centralized administrator. Each node in a wireless ad hoc network functions as both a host and a router. The network topology is in general dynamic because the connectivity among nodes may vary with time due to node mobility, node departures, and new node arrivals. Hence, there is a need for efficient routing protocols to allow the nodes to communicate.

Ad hoc nodes or devices should be able to detect the presence of other such devices so as to allow communication and information sharing. Besides that, it should also be able to identify types of services and corresponding attributes. Since the number of wireless nodes changes on the fly, the routing information also changes to reflect changes in link connectivity. Hence, the topology of the network is much more dynamic and the changes are often unpredictable as compared to the fixed nature of existing wired networks.

The dynamic nature of the wireless medium, fast and unpredictable topological changes, limited battery power, and mobility raise many challenges for designing a routing protocol. Due to the immense challenge in designing a routing protocol for MANETs, a number of recent developments focus on providing an optimum solution for routing. However, a majority of these solutions attain a specific goal (e.g., minimizing delay and overhead) while compromising other factors (e.g., scalability and route reliability). Thus, an optimum routing protocol that can cover most of the applications or user requirements as well as cope up with the stringent behavior of the wireless medium is always desirable.

However, there is another kind of MANET nodes called the *fixed network*, in which the connection between the components is relatively static; the sensor network is the main example for this type of fixed network [8]. All components used in the sensor network are wireless and deployed in a large area. The sensors can collect the information and route data back to a central processor or monitor. The topology for the sensor network may be changed if the sensors lose power. Therefore, the sensors network is considered to be a fixed ad hoc network.

Each of the nodes has a wireless interface and communicates with each other over either radio or infrared frequency. Laptop computers and PDAs that communicate directly with each other are some examples of nodes in an ad hoc network. Nodes in the ad hoc network are often mobile, but can also consist of stationary nodes, such as access points to the Internet. Semi-mobile nodes can be used to deploy relay points in areas where relay points might be needed temporarily. Figure 1.3 shows a simple ad hoc network with three nodes. The outermost nodes are not within the transmitter range of each other. However, the middle node can be used to forward packets between the outermost nodes. Node B is acting as a router and nodes A, B, and C have formed an ad hoc network.

An ad hoc network uses no centralized administration. This ensures that the network would not collapse just because one of the mobile nodes moves out of the transmitter range of the other nodes. Nodes should be able to enter or leave the network as they wish. Because of the limited transmitter range of the nodes, multihops may be needed to reach other nodes. Every node wishing to participate in an ad hoc network must be willing to forward packets to other nodes. Thus, every node acts both as a host and as a router. A node can be viewed as an abstract entity consisting of a router and a set of affiliated mobile hosts. A router is an entity that, among other things, runs a routing protocol. A mobile host is simply an IP-addressable host or entity in the traditional sense.

Ad hoc networks are also capable of handling topology changes and malfunctions in nodes. They are fixed through network reconfiguration. For instance, if a node leaves the network and

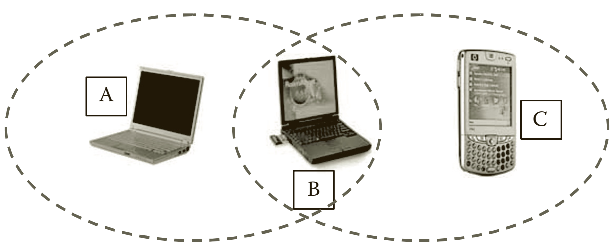

Figure 1.3 Connectivity between nodes A, B, and C.

causes link breakages, affected nodes can easily request new routes and the problem will be solved. This will slightly increase the delay, but the network will still be operational.

1.4 Mobile Ad Hoc Network History

The history of wireless networks dates back to 1970s, and the interest has been growing ever since. During the last decade, the interest has almost exploded, probably because of the fast-growing Internet. The tremendous growth of personal computers and the handy usage of mobile devices necessitate the need for ad-hoc connectivity.

The first generation goes back to 1972. At the time they were called PRNET (packet radio network). In conjunction with ALOHA (areal locations of hazardous atmospheres) [1], approaches for MAC control and a type of distance vector routing PRNET were used on a trial basis to provide different networking capabilities in a combat environment.

The second generation of ad hoc networks emerged in 1980s, when the ad hoc network was further enhanced and implemented as a part of the SURAN (Survivable Adaptive Radio Networks) project that aimed at providing ad hoc networking with small, low-cost, low-power devices with efficient protocols for improved scalability and survivability [9]. This provided a packet-switched network to the mobile battlefield in an environment without infrastructure.

In the 1990s, the concept of commercial ad hoc networks arrived with notebook computers and other viable communications equipment. At the same time, the idea of a collection of mobile nodes was proposed at several research conferences.

The IEEE 802.11 subcommittee had adopted the term "ad hoc networks" and the research community had started to look into the possibility of deploying ad hoc networks in other areas of application. Meanwhile, work was going on to advance the previously built ad hoc networks. GloMo (global mobile information systems) and the NTDR (near-term digital radio) are some of the results of these efforts [10]. GloMo was designed to provide an office environment with Ethernet-type multimedia connectivity anywhere and anytime in handheld devices.

1.5 Mobile Ad Hoc Network Definition

A clear definition of precisely what is meant by an ad hoc network is difficult to identify. In today's scientific literature, the term "ad hoc network" is used in many different ways. There are many different definitions that describe ad hoc networks, but only three are presented here. The first one is given by the Internet Engineering Task Force group [11], the second one is given by National Institute of Standard and Technology [12], and the final definition is given by the INTEC Research group [13].

In MANETs, the wireless nodes are free to move and still connected using the multihop with no infrastructure support. The goal of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Ad hoc networks have no fixed routers; all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Nodes of these networks function as routers, which discover and maintain routes to other nodes in the network. Example applications of ad hoc networks are emergency search and rescue operations, meetings, and conventions in which a person wishes to make a quick connection for sharing information.

1.6 MANET Applications and Scenarios

With the increase of portable devices as well as progress in wireless communication, ad hoc networking is gaining importance because of its increasing number of widespread applications. Ad hoc networking can be applied anywhere at anytime without infrastructure and its flexible networks. Ad hoc networking allows the devices to maintain connections to the network as well as easily adds and removes devices to and from the network. The set of applications of MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks to small and static networks that are constrained by limited power. Besides the legacy applications that move from traditional infrastructure environment to the ad hoc context, a great deal of new services can and will be generated for the new environment. Typical applications include the following:

- Military battlefield: Military equipment now routinely contains some sort of computer equipment. Ad hoc networking can be very useful in establishing communication among a group of soldiers for tactical operations and also for the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. Ad hoc networks also fulfill the requirements of communication mechanism very quickly because ad hoc network can be set up without planning and infrastructure, which makes it easy for the military troops to communicate with each other via the wireless link. The other important factor that makes MANET very useful and let it fit in the military base is the fact that the military objects, such as airplanes, tanks, and warships, move at high speeds, and this application requires MANET's quick and reliable communication. Because of the information that transfers between the troops, it is very critical that the other side receives secure communication, which can be found through ad hoc networks. At the end, the primary nature of the communication required in a military environment enforced certain important requirements on ad hoc networks, such as reliability, efficiency, secure, and support for multicast routing. Figure 1.4 shows an example of the military ad hoc network.
- Commercial sector: The other kind of environment that uses an ad hoc network is emergency rescue operation. The ad hoc form of communications is especially useful in public-safety and search-and-rescue applications. Medical teams require fast and effective communications when they rush to a disaster area to treat victims. They cannot afford the time to run cabling and install networking hardware. The medical team can employ ad hoc networks (mobile nodes) such as laptops and PDAs and can communicate via the wireless

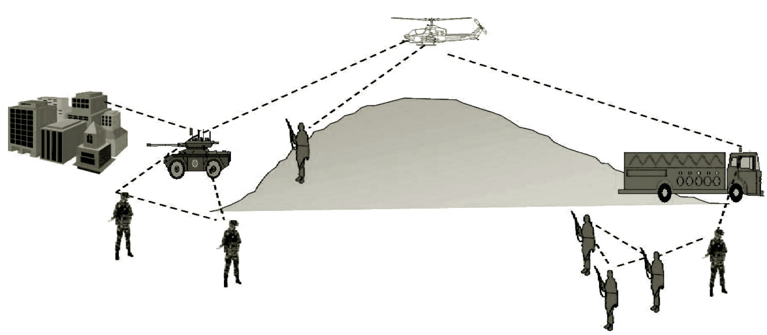

Figure 1.4 Military application.

link with the hospital and the medical team on-site. For example, a user on one side of the building can send a packet destined for another user on the far side of the facility, well beyond the point-to-point range of WLAN, by having the data routed from client device to client device until it gets to its destination. This can extend the range of the WLAN from hundreds of feet to miles, depending on the concentration of wireless users. Real-time communication is also important since the voice communication predominates data communication in such scenarios. Figure 1.5 shows the ad hoc search-and-rescue application.

- Local level: Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at conferences, at meetings, or in classrooms. Another appropriate local level application might be in home networks, where devices can communicate directly to exchange information. Similarly, in other civilian environments such as taxicab, sports stadium, boat, and small aircraft, mobile ad hoc communications will have many applications.
- Personal area network (PAN): It is the interconnection of information technology devices within the range of an individual person, typically within a range of 10 m. For example, a person traveling with a laptop, a PDA, and a portable printer could interconnect them without having to plug anything in by using some form of wireless technology. Typically, this type of PAN could also be interconnected without wires to the Internet or other networks. A wireless personal area network (WPAN) is virtually a synonym of PAN since almost any PAN would need to function wirelessly. Conceptually, the difference between a PAN and a WLAN is that the former tends to be centered around one person while the latter is a local area network (LAN) that is connected without wires and serve multiple users.

Bluetooth is an industrial specification for WPANs. A Bluetooth PAN is also called a *piconet* and is composed of up to eight active devices in a master–slave relationship (up to 255 devices can be connected in the "parked" mode). The first Bluetooth device in the piconet is the master, and all other devices are slaves that communicate with the master. A piconet has a range of 10 m that can reach up to 100 m under ideal circumstances, as shown in Figure 1.6.

The other usage of the PAN technology is that it could enable wearable computer devices to communicate with nearby computers and exchange digital information using the electrical conductivity of the human body as a data network. Some concepts that belong to the PAN technology are considered in research papers, which present the reasons why those concepts might be useful:

Figure 1.5 Search-and-rescue application.

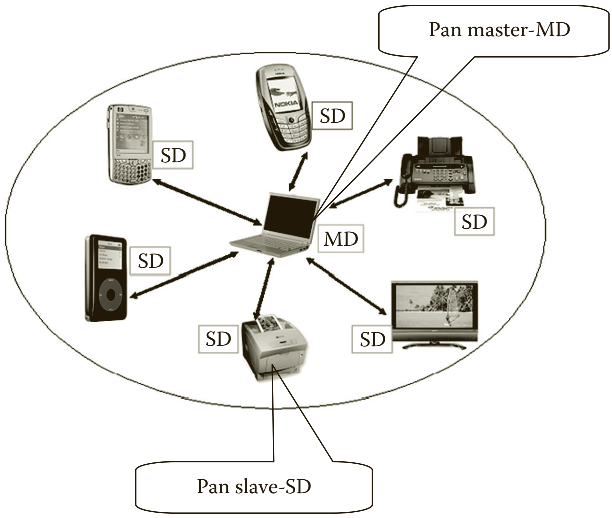

Figure 1.6 Personal area network.

- Small size of the device
- No need for huge power (lower power requirements)
- Not expensive
- Used specially for bodies and for sensitive information
- No methods for sharing data
- Networking can reduce function of input/output
- Allow new conveniences and services

1.7 Ad Hoc Network Characteristics

MANETs have the following features that are necessary to consider while suggesting or designing solutions for these types of networks:

- MANET has a feature of distributed operation because in MANET each node operates independently and there is no centralized server or computer to manage this network. Instead this job is distributed among all operating nodes. Each node works with another node in cooperation to implement functions such as security and routing.
- MANETs have lower bandwidth capacity as compared with wired networks. MANETs can experience a problem of bit error rate and lower bandwidth capacity because end-to-end link paths are used by several nodes in the network. Also, the channel used for communication can be affected by other factors such as fading and interference.
- Another feature of MANET that can be used is energy in mobile devices. As all mobile devices will get their energy from batteries, which is a limited resource, whatever energy the mobile nodes have, it has to be used very efficiently.
- Security is the most important concern in MANETs because the nodes and the information in MANETs are not secured from threats, for example, denial of service attacks. Also, mobile devices imply higher security risks compared with fixed operating devices, because portable

devices may be stolen or their traffic may insecurely cross wireless links. Eavesdropping, spoofing, and denial of service attacks are the main threats for security.

- In MANETs the network topology is always changing because nodes in the ad hoc network change their positions randomly as they are free to move anywhere. Therefore, devices in a MANET should support dynamic topology. Each time the mobility of node causes a change in the topology and hence the links between the nodes are always changing in a random manner. This mobility of nodes creates frequent disconnection; hence, to deal with this problem the MANET should adapt to the traffic and transmission conditions according to the mobility patterns of the mobile network nodes.
- A MANET includes several advantages over wireless networks, including ease of deployment, speed of deployment, and decreased dependences on a fixed infrastructure. A MANET is attractive because it provides an instant network formation without the presence of fixed base stations and system administration.

1.8 Classification of Ad Hoc Networks

There is no generally recognized classification of ad hoc networks in the literature. However, there is a classification on the basis of the communication procedure (single hop/multihop), topology, node configuration, and network size (in terms of coverage area and the number of devices).

1.8.1 Classification According to the Communication

Depending on the configuration, communication in an ad hoc network can be either single hop or multihop.

1.8.1.1 Single-Hop Ad Hoc Network

Nodes are in their reachable area and can communicate directly, as shown in Figure 1.7. Single-hop ad hoc networks are the simplest type of ad hoc networks where all nodes are in their mutual

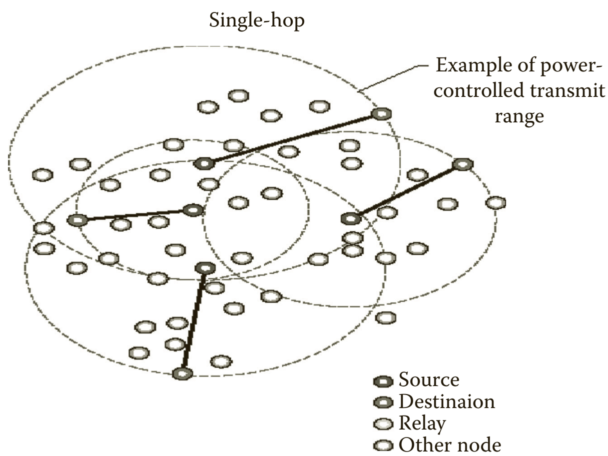

Figure 1.7 Single-hop ad hoc network.

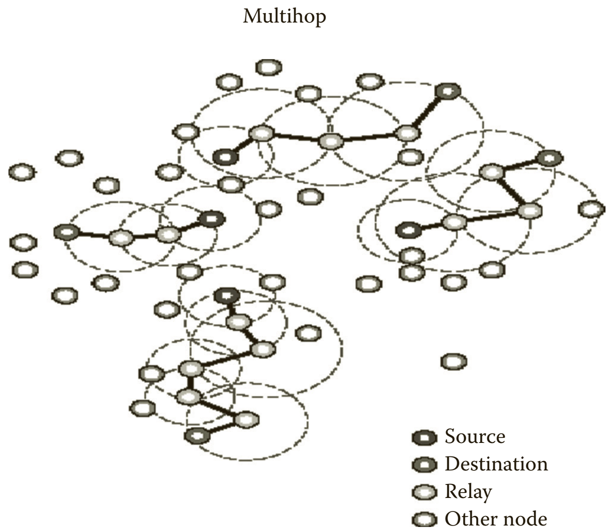

Figure 1.8 Multihop ad hoc networks.

range, which means that the individual nodes can communicate directly with each other, without any help of other intermediate nodes. The individual nodes do not have to be static; they must, however, remain within the range of all nodes, which means that the entire network could move as a group; this would not modify anything in the communication relations.

1.8.1.2 Multihop Ad Hoc Network

This class in the literature is the most examined type of ad hoc networks. It differs from the first class in that some nodes are far and cannot communicate directly. Therefore, the traffic of these communication endpoints has to be forwarded by other intermediate nodes. Figure 1.8 shows the communication path of far nodes as black lines. With this class also, one assumes that the nodes are mobile. The basic difficulty of the networks of this class is the node mobility, whereby the network topology is subjected to continuous modifications. The general problem in networks of this class is the assignment of a routing protocol. High-performance routing protocols must be adaptive to the fast topology modification.

1.8.2 Classification According to the Topology

Ad hoc networks can be classified according to the network topology. The individual nodes in an ad hoc network are divided into three different types with special functions: flat, hierarchical, and aggregate ad hoc networks.

1.8.2.1 Flat Ad Hoc Networks

In flat ad hoc networks, all nodes carry the same responsibility and there is no distinction between the individual nodes, as shown in Figure 1.9. All nodes are equivalent and can transfer all functions in the ad hoc network. Control messages have to be transmitted globally throughout the network, but they are appropriate for highly dynamic network topology. The scalability decreases when the number of nodes increases significantly.

1.8.2.2 Hierarchical Ad Hoc Networks

Hierarchical ad hoc networks consist of several clusters, each one represents a network and all are linked together, as indicated in Figure 1.10. The nodes in hierarchical ad hoc networks can be categorized into two types:

- Master nodes: Administer the cluster and are responsible for passing the data on to the other cluster.
- Normal nodes: Communicate within the cluster directly together and with nodes in other clusters with the help of the master node. Normal nodes are also called *slave nodes*.

One assumes that the majority of communication (control messages) takes place within the cluster and only a fraction between different clusters. During communication within a cluster, no forwarding of communication traffic is necessary. The master node is responsible for the switching of a connection between nodes in different clusters.

The no single point of failure is of great importance for a message to reach its destination. This means that if one node goes down, the rest of the network will still function properly. In the

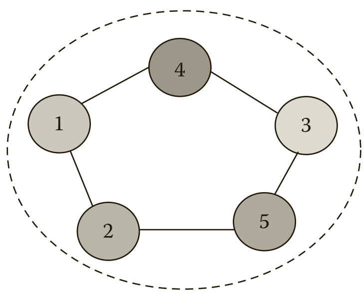

Figure 1.9 Flat ad hoc network.

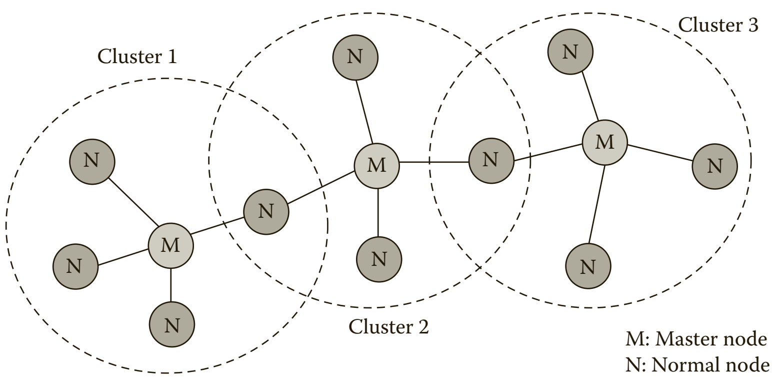

Figure 1.10 Hierarchical ad hoc networks.

hierarchical approach, this is altogether different. If one of the cluster heads goes down, that section of the network will not be able to send or receive messages from other sections for the duration of the downtime of the cluster head.

Hierarchical architectures are more suitable for low-mobility cases. The flat architectures are more flexible and simpler than hierarchical ones; hierarchical architectures provide a more scalable approach.

1.8.2.3 Aggregate Ad Hoc Networks

Aggregate ad hoc networks bring together a set of nodes into zones. Therefore, the network is partitioned into a set of zones as shown in Figure 1.11. Each node belongs to two levels of topology: low-level (node-level) topology and high-level (zone-level) topology. Also, each node may be characterized by two ID numbers: node ID number and zone ID number. Normally, aggregate architectures are related to the notion of zone. In aggregate architectures, we find both intrazone and interzone architectures, which in turn can support either flat or hierarchical architectures.

1.8.3 Classification According to the Node Configuration

A further classification of ad hoc networks can be performed on the basis of the hardware configuration of the nodes. There are two types of node configurations: homogeneous networks and heterogeneous networks. The configuration of the nodes in a MANET is important and can depend very strongly on the actual application.

1.8.3.1 Homogeneous Ad Hoc Networks

In homogeneous ad hoc networks, all nodes possess the same characteristics regarding the hardware configuration as processor, memory, display, and peripheral devices. Most well-known representatives of homogeneous ad hoc networks are wireless sensor networks. In homogeneous

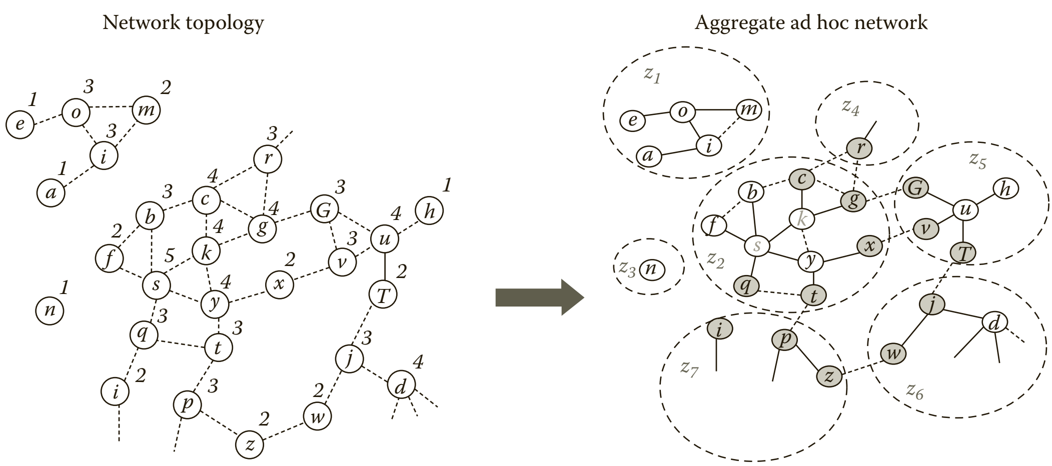

Figure 1.11 Aggregate network architecture.

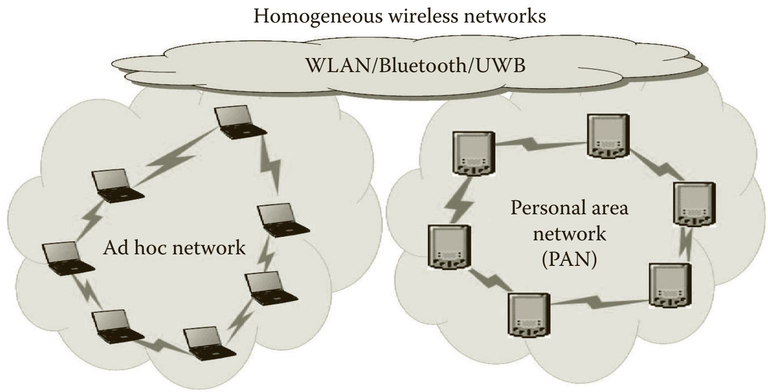

Figure 1.12 Homogeneous networks.

ad hoc networks, applications can proceed from certain prerequisites; for example, the localization is considerably facilitated by the presence of control components in each node, as shown in Figure 1.12.

1.8.3.2 Heterogeneous Ad Hoc Networks

In heterogeneous ad hoc networks, the nodes differ according to the hardware configuration. Each node has different characteristics, resources, and policies. In ad hoc networks of this class, all nodes cannot provide the same services, as shown in Figure 1.13.

1.8.4 Classification According to the Coverage Area

As shown in Figure 1.14, ad hoc networks can be categorized, depending on their coverage area, into several classes: depending on their coverage area, into several classes: body area network (BAN), personal area network (PAN), local area network (LAN), metropolitan area network (MAN), and wide area network (WAN) [13,14]. WAN and MAN are mobile multihop wireless networks presenting many challenges that are still being solved (e.g., addressing, routing, location management, and security), and their availability is not on immediate horizon.

A BAN is strongly correlated with wearable computers. The components of a wearable computer are distributed on the body (e.g., head-mounted displays, microphones, and earphones), and a BAN provides the connectivity among these devices. The communicating range of a BAN corresponds to the human body range, i.e., 1–2 m. As wiring around a body is generally cumbersome, wireless technologies constitute the best solution for interconnecting wearable devices. The PAN connects mobile devices carried by users to other mobile and stationary devices, while BAN is devoted to the interconnection of one-person wearable devices. A PAN has a typical communication range of up to 10 m. WPAN technologies in the 2.4–10.6-GHz band are the most promising technologies for the widespread PAN deployment. Spread spectrum is typically employed to reduce interference and utilize the bandwidth [15].

In the last few years, the application of wireless technologies in the LAN environment has become increasingly important, and WLAN can be found in different environments such as homes, offices, urban roads, and public places. WLAN, also called *wireless fidelity* (Wi-Fi), is

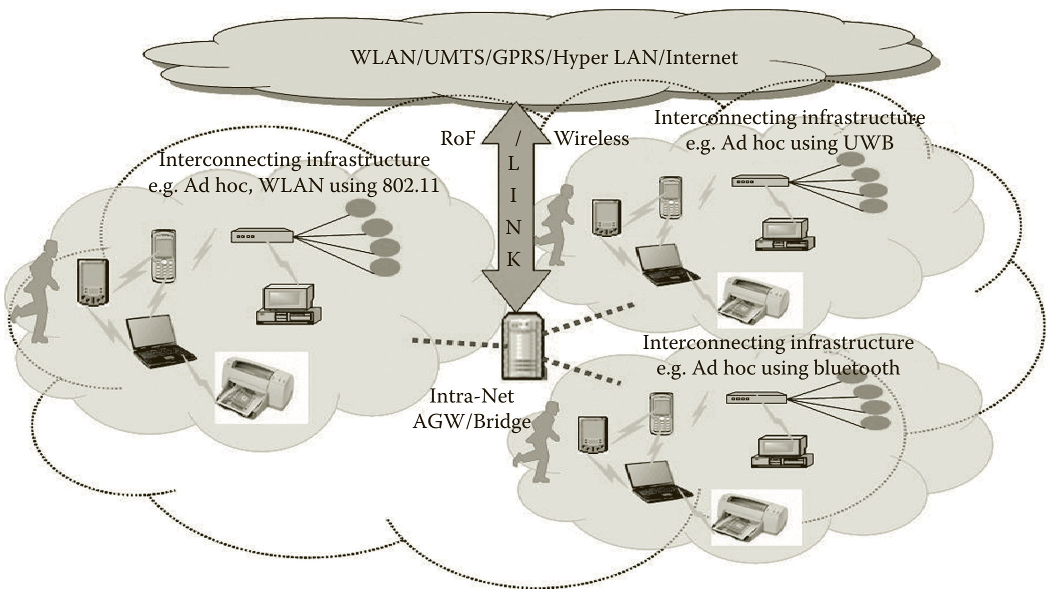

Figure 1.13 Heterogeneous networks.

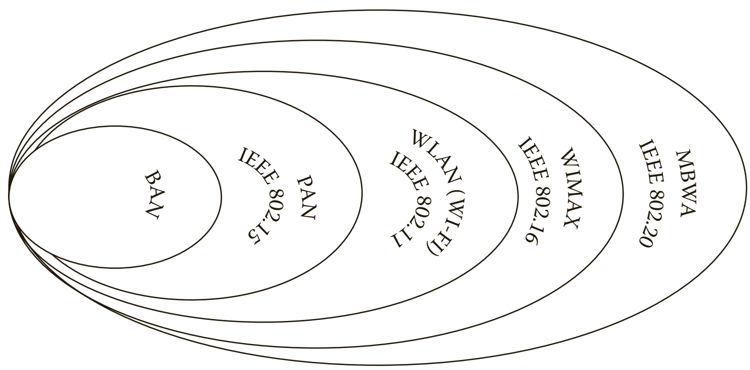

Figure 1.14 Ad hoc network taxonomy according to coverage area.

based on the 802.11 standard. It gives freedom to Internet users; also, they offer greater flexibility than the wired LANs. Most of the personal computers, laptops, phones, and PDAs are capable of connecting to the Internet via WLAN. Currently, there are five major specifications in the WLAN family 802.11 namely 802.11a, 802.11b, 802.11g and 802.11n. All use CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) for medium sharing which are standardized in 802.11c, 802.11d, 802.11e and 802.11f.

WIMAX is based on the 802.16 IEEE standard and defined as a wireless MAN technology that will provide a wireless alternative to wire and digital subscriber line (DSL) for last mile broadband access. WIMAX has a communication range of up to 50 km, which also allows the users to get broadband connections without directly connecting to the base station, and provides shared data rates of up to 70 Mbps, which is enough bandwidth to support more than 60 T1 link and hundreds of home and office DSL connections. Likewise, WIMAX fully supports the quality of service. Finally, the last but not the least wireless technology called mobile broadband wireless access (MBWA) is approved by the IEEE standard board and defined as 802.20. The MBWA is similar to the IEEE 802.16e in that its uses Orthogonal Frequency Division Multiple Access (OFDMA), provides very high mobility, and has a shared data rate of up to 100 Mbps. At present, no operator has committed to the MBWA technology.

Conclusion

The chapter has presented the overview of wireless networks and different aspects of MANET, such as, definition, application, classification, special features and various routing protocols of MANET. The applications of MANETs are described with examples and how those applications work with different environments. The MANET characteristic features are also pointed out such as distributed operation, lower bandwidth capacity, dynamic topology and security. This chapter also briefly covered the classification of MANETs in terms of communication procedure (single hop/multi hop), topology, (node configuration) and network size (coverage area and number of devices).

References

1. F. Dressler. Self-organization in ad hoc networks: overview and classification. Technical Report 02/06. Department of Computer Science 7, University of Erlangen.
2. C.E. Perkins. *Ad Hoc Networking*. Addison-Wesley, 2001.
3. S. Basagni, M. Conti, S. Giordano, and I. Stojmeovic. *Mobile Ad Hoc Networking*. Wiley-IEEE Press, 2004.
4. M. Gast. *802.11 Wireless Networks the Definitive Guide, Second Edition*. O'Reilly Media, 2005.
5. C. Siva Ram Murthy and B.S. Manoj. *Ad Hoc Wireless Networks Architectures and Protocols*. Prentice Hall, 2004.
6. M. Iiyas. *The Handbook of Ad Hoc Wireless Networks*. CRC Press, 2002.
7. M. Frodigh, P. Johansson, and P. Larsson. Wireless ad hoc networking: the art of networking without a network. *Ericsson Review*, no. 4, 2000, pp. 248–263.
8. B.-J. Kwak, N.-O. Song, and L.E. Miller. On the scalability of ad hoc networks. *IEEE Communication Letter*, vol. 8, no. 8, 2004, pp. 503–505.
9. J. Jubin and J.D. Tornow. The DARPA packet radio network protocols. *Proceedings of the IEEE*, vol. 75, no. 1, 1987, pp. 21–32.
10. R. Ramanathan and J. Redi. A brief overview of ad hoc networks: challenges and directions. *IEEE Communications Magazine*, vol. 40, no. 5, 2002, pp. 20–22.
11. http://www.ietf.org/html.charters/wg-dir.html (Accessed July 2011)
12. http://www.antd.nist.gov/ (Accessed July 2011)
13. Wireless local area network hits the public. Available at http://www.touchbriefings.com/pdf/744/wire041_vis.pdf (Accessed March 2011).
14. Chlamtac, M. Conti, and J.N. Jennifer. Mobile ad hoc networking: imperatives and challenges. In: *Elsevier Proceeding for Ad Hoc Networks*, vol. 1, 2003, pp. 13–64.
15. M. Abolhasan, T. Wysocki, and E. Dutkiewicz. *A Review of Routing Protocols for Mobile Ad Hoc Networks*, vol. 2, no. 1, 2004, pp. 1–22.

Chapter 2

Mobile Ad Hoc Routing Protocols

Jonathan Loo, Shafiullah Khan, and Ali Naser Al-Khwildi

Contents

The development of omnipresent mobile computing devices has fueled the need for dynamic reconfigurable networks. Mobile ad hoc network (MANET) routing protocols facilitate the creation of such networks, without a centralized infrastructure. One of the challenges in the study of MANET routing protocols is the evaluation and design of an effective routing protocol that works at low data rates and responds to dynamic changes in network topology due to node mobility. Several routing protocols have been standardized by the Internet Engineering Task Force to address ad hoc routing requirements. The classification of these protocols and some existing ad hoc routing protocols are discussed in this chapter [1–3].

2.1 Taxonomy of Ad Hoc Routing Protocols

Several ad hoc protocols have been designed for accurate, fast, reliable routing for a high volume of changeable network topology. Such protocols must deal with the typical limitations of changeable network topology, which include high power consumption, low bandwidth, and high error rates. As shown in Figure 2.1, these routing protocols may generally be categorized into three main types: proactive or table-driven, reactive or on-demand-driven, and hybrid. This classification differentiates the routing protocols according to their technique, their hop count, link state, and source routing in a route-discovery mechanism. In protocols based on a hop count technique, each node contains next-hop information in its routing table, linked to the destination. Link state routing protocols maintain a routing table for complete topology, which is built up by finding the shortest path of link costs. In the source routing technique, all data packets carry their routing information as their header. The originating node can obtain this routing information, for example, by means of a source routing protocol. The next section will present details for each routing category, including some of the existing routing protocols used for those categories [4–11].

2.2 On-Demand Ad Hoc Routing Protocols

Reactive protocols are also called *on-demand routing protocols*. These protocols create routes to a destination only when required. The route discovery procedure is triggered whenever a source wants to send data to find a destination node, and the route is maintained through the route maintenance procedure until the route is no longer required. In this manner, communication overhead is reduced and battery power is conserved as compared to proactive routing protocols. As shown in Figure 2.2, there is no topology table in each node. When there is a request in node A to transmit data to node D, the route discovery process starts by broadcasting to all nodes searching for node D. When node D receives this message, it responds to the request to build the route to node A. The process is complete once a route is found or all possible route permutations have been examined. Once a route has been established, it is maintained by a route maintenance procedure

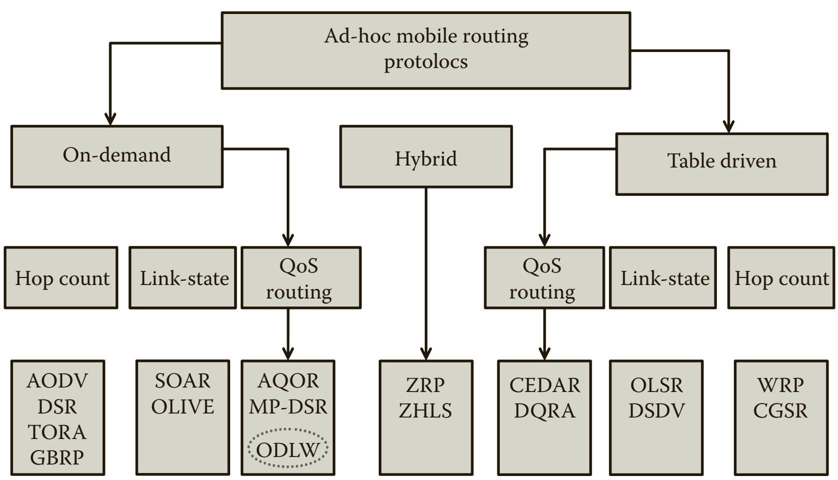

Figure 2.1 Categorization of ad hoc routing protocol.

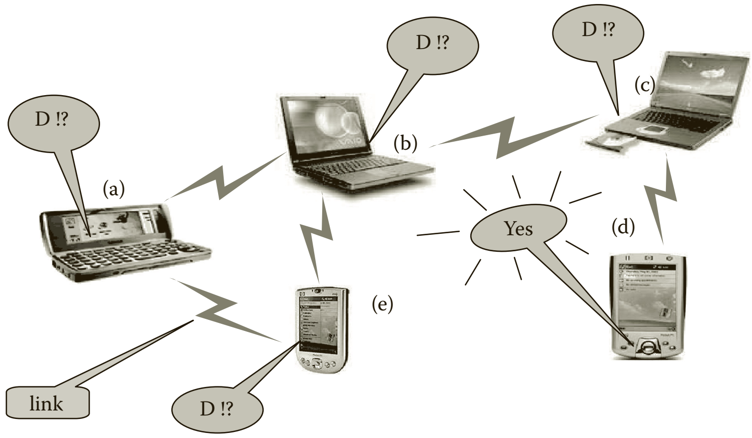

Figure 2.2 On-demand (reactive) ad hoc protocol.

until either the destination becomes inaccessible along every path from the source or the route is no longer desired.

A network using an on-demand protocol will not maintain correct routing information for all nodes at all times. As an alternative, such routing information is obtained on demand. If a node needs to transmit a message and does not have sufficient routing information to send the message to the destination, the necessary information has to be obtained. Typically, the node at least wants to identify the next hop (among its neighbors) for the packet. Although the node could just broadcast the packet to all neighbors, this leads to severe congestion in numerous instances. However, such broadcasts are used in a route discovery process, since there is no other next-hop information available yet.

The advantage of on-demand routing protocols lies in the fact that the wireless channel (a scarce resource) does not require to carry a large amount of routing overhead data for routes that are no longer used. This advantage may be reduced in certain scenarios where there is heavy traffic to a wide range of nodes. Thus, these scenarios have a strong impact on performance. In a scenario including large amounts of traffic to several nodes, the route setup traffic can rise higher than the constant background traffic to preserve the correct routing information at every node. Still, if sufficient capacity is available, the compact efficiency (increased overhead) may not influence other performance methods such as throughput or latency. Examples for on-demand protocols include the following: ad hoc on-demand distance vector (AODV), dynamic source routing (DSR), Temporally-Ordered Routing Algorithm (TORA) Associativity Based Routing (ABR), and Stability based Adaptive (SSA) [12–16].

2.3 Table-Driven Ad Hoc Routing Protocols

Proactive routing protocols enable each node to keep up-to-date routing information in a routing table. This routing table is exchanged periodically with all other nodes, as well as when network topology changes. Thus, when a node needs to send a packet, the route is readily available. However, most of the routing information that is exchanged is undesired. Proactive routing protocols are also called *table-driven routing protocols*.

Figure 2.3 illustrates the concept of proactive protocols. For example, if node A wanted to send some data to node D, all it would have to do is find node D on the previously prepared

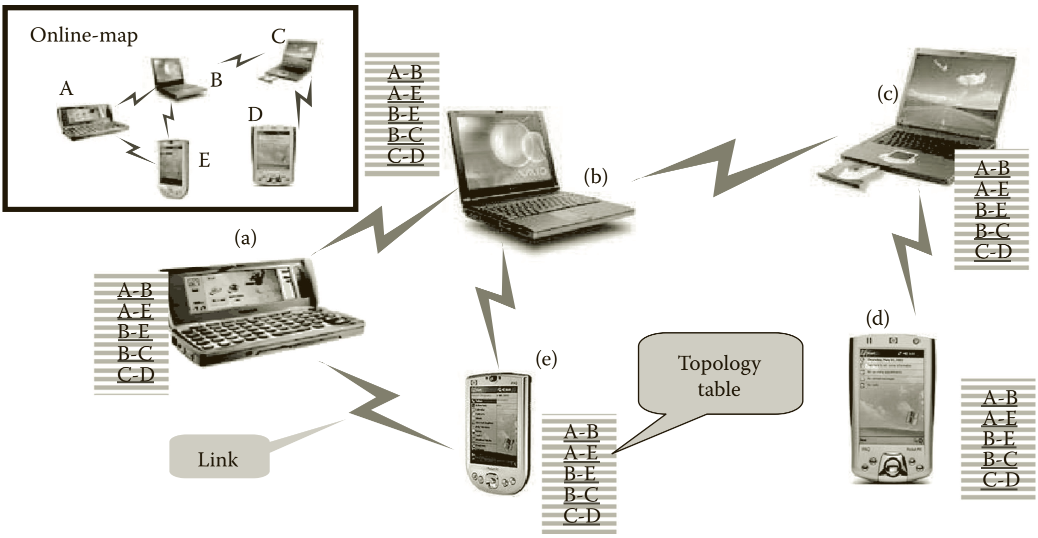

Figure 2.3 Proactive ad hoc protocol.

topology table, which is stored in node A. Table parsing is faster and requires less power than searching the entire network for a destination. If the network nodes do not have frequent mobility, then the topology table will not consume too much power.

In ad hoc networks based on proactive protocols, power and bandwidth consumption increase due to topology table exchange among nodes after each change in the nodes' location. This takes place even if the network is in stand-by mode (e.g., no data transmissions in the network). The best network context for proactive protocols is the low (or no) mobility networks. Some well-known proactive protocols include optimized link state routing (OLSR), destination sequenced distance vector Clusterhead Gateway Switch Routing (CGSR), and Wireless Routing Protocol (WRP) [11,17–19].

2.4 Hybrid Ad Hoc Routing Protocols

Based on the combination of both table- and demand-driven routing protocols, some hybrid routing protocols have been proposed to combine the advantages of both proactive and reactive protocols. The most typical hybrid protocol is a zone routing protocol [20]. With regard to the main division of routing protocols, Table 2.1 provides a comparison of table-driven, demand-driven, and hybrid routing protocols. Some hybrid routing protocols include zone routing protocol (ZRP), Zone-Based Hierarchical Link State (ZHLS), and core extraction distributed ad hoc routing(CEDAR) [21–23].

2.5 Description of Current Ad Hoc Routing Protocols

Many routing protocols have been proposed for ad hoc networks, which are different in the approach used for the routing discovery mechanism, maintaining the existing route when link failure occurs or the node moves away from the existing networks. In the next section, we will

Table 2.1 Characteristic Comparison of Proactive, Reactive, and Hybrid Routing Protocol

	Table-Driven	*Demand-Driven*	*Hybrid*
Network organization	Flat/hierarchical	Flat	Hierarchical
Topology dissemination	Periodical	On-demand	Both
Route latency	Always available	Available when needed	Both
Mobility handling	Periodic updates	Route maintenance	Both
Communication overhead	High	Low	Medium

present the operation and routing mechanism for well-known routing protocols, such as AODV, DSR, temporally ordered routing algorithm (TORA), OLSR, DSDV, ZRP, CEDAR, and ad hoc quality of service (QoS) on-demand routing (AQOR) [24].

The major differences between all the described protocols are shown in Table 2.2. The data were used for this investigation to enhance the overview of the interworking between the different protocols.

2.5.1 AODV

The AODV [12] routing protocol uses the on-demand approach for finding routes; that is, the route is established only when it is required by a source node for transmitting data packets. It employs a destination sequence number to identify the most recent path. In AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission.

When a source requires a route to a destination, it floods the network with a *route request* (RREQ) packet. On its way through the network, the RREQ packet initiates the creation of temporary route table entries for the reverse path at every node it passes, and when it reaches the destination, a *route reply* (RREP) packet is unicast back along the same path on which the RREQ packet was transmitted. A mobile node can become aware of neighboring nodes by employing several techniques, one of which involves broadcasting *Hello* messages. Route entries for each node are maintained using a timer-based system. If the route entry is not used immediately, it is deleted from the routing table. AODV does not repair broken paths locally. When a path breaks between nodes, both nodes initiate *route error* (RERR) packets to inform their end nodes about the link break. The end nodes delete the corresponding entries from their table. The source node reinitiates the path-finding process with a new broadcast ID and the previous destination sequence number. The main advantage of this protocol is that the routes are established on demand and destination sequence numbers are used to find the latest route to the destination. The disadvantage of this protocol is that the intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher, but not the latest, destination sequence number, thereby hosting stale entries. This is illustrated in Figure 2.4.

Table 2.2 Characteristic Comparison of Proactive, Reactive, and Hybrid Routing Protocols

	AODV	*DSR*	*TORA*	*OLSR*	*DSDV*	*ZRP*	*CEDAR*	*AQOR*
Routing type	Reactive	Reactive	Reactive	Proactive	Proactive	Hybrid	Hybrid	QoS-Reactive
Alternative route	Not available	Not available	Available	Not available	Not available	Not available	Not available	Not available
Routing mechanism	Next hop	Source routing	Next hop	Next hop	Next hop	N/A	N/A	Next hop
Routing metrics	Shortest path	Shortest path	Shortest path	Shortest path	Shortest path	Shortest path	Shortest path	Shortest path
Update routing	Yes-Hello message	No	No	Yes	Yes	Half way Yes	Half way Yes	Yes-Hello message
Network size	Large	Small	Medium	Large	Large	Large	Large	Large
Routing adaption	No	No	No	No	No	No	No	Yes
QoS support	No	No	No	No	No	No	No	Yes
Security	No	No	No	No	No	No	No	No
Mobility	Good	Bad	Bad	Good	Good	Good	Good	Good

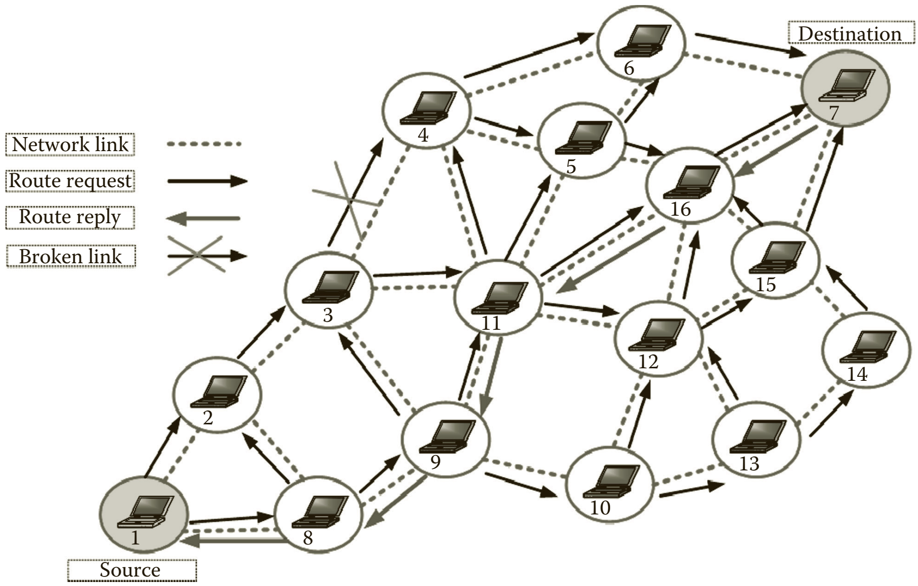

Figure 2.4 AODV routing mechanism.

2.5.2 DSR

DSR [13] is another on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc networks by eliminating the periodic table-update message required in the table-driven approach. The key distinguishing feature of DSR is the use of source routing. The sender knows the complete hop-by-hop route to the destination, and those routes are stored in a route cache. The data packet carries the source route in the packet header. There are two major phases in this protocol. The first is route discovery, which is achieved by flooding the network with RREQ packets. The destination node, upon receiving an RREQ, responds by sending an RREP packet back to the source along the same route traversed by the incoming RREQ packet. Any node can update its cache when it receives or forwards a packet containing source route information. The route cache can be used to reduce the number of packets flooding the network. The second phase is route maintenance. If any link on a source route is broken, the source node is notified through an RERR packet. The source removes any route using this link from its cache. A new route discovery process must be initiated by the source if this route is still needed. The advantage of this protocol is that it reduces overhead on route maintenance. This is done by using route caching. The disadvantage is that the packet header size grows with the route length due to both source routing and RREQ flooding that may potentially reach all nodes in the network. The DSR routing mechanism is shown in Figure 2.5.

2.5.3 TORA

TORA [14] is a source-initiated on-demand routing protocol, which uses a link reversal algorithm and provides loop-free multipath routes to a destination node. In TORA, each node maintains its one-hop local topology information and also has the capability to detect partitions. TORA is proposed to operate in a highly dynamic mobile networking environment. The key design concept

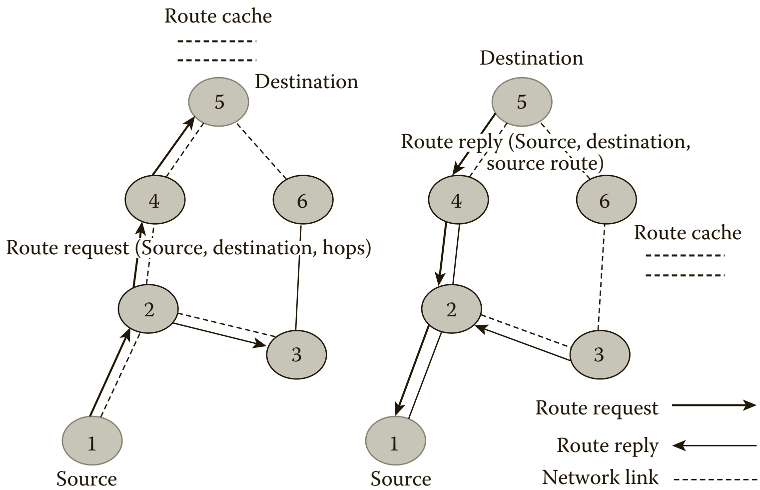

Figure 2.5 DSR routing mechanism.

of TORA is the location of control messages sent to a very small set of nodes near the occurrence of a topological change. The protocol performs three basic functions: (1) route creation, (2) route maintenance, and (3) route erasure.

During the route creation and maintenance phases, the nodes use a *height* metric, which establishes a direct acyclic graph (DAG) rooted at the destination. Therefore, links are assigned a direction (upstream or downstream) based on the relative height metric of neighboring nodes, as shown in Figure 2.6. The process for establishing a DAG is similar to the query/reply process in lightweight mobile routing. In times of node mobility, the DAG route is broken, and route maintenance is necessary to reestablish a DAG rooted at the same destination. Timing is an important factor for TORA because the height metric depends on the logical time of link failure. TORA assumes all nodes have synchronized clocks. In TORA, there is a potential for oscillations to occur, especially when multiple sets of coordinating nodes are concurrently detecting partitions, erasing routes, and building new routes based on each other. Because TORA uses internodal coordination, its instability problem is similar to the "count-to-infinity" problems.

2.5.4 OLSR

The OLSR protocol is a table-driven protocol [11]. In OLSR, nodes exchange messages with other nearby nodes of the network on a regular basis to update topology information on each node, as illustrated in Figure 2.7. Nodes determine their one-hop neighbors, i.e., nodes within their transmission radius, by transmitting Hello messages. Based on a selection criterion that will be elaborated upon in the subsequent sections, a set of nodes among the one-hop neighbors is chosen as multipoint relays (MPRs). Only these nodes forward topological information, providing every other node with partial information about the network. Furthermore, only these MPRs will generate link state information to be forwarded throughout the network. By these two optimizations, the amount of retransmission is minimized, thereby reducing overhead as compared to link state routing protocols. Each node will then use this topological information, along with the collected Hello messages, to compute optimal routes to all nodes in the network. In ad hoc radio networks,

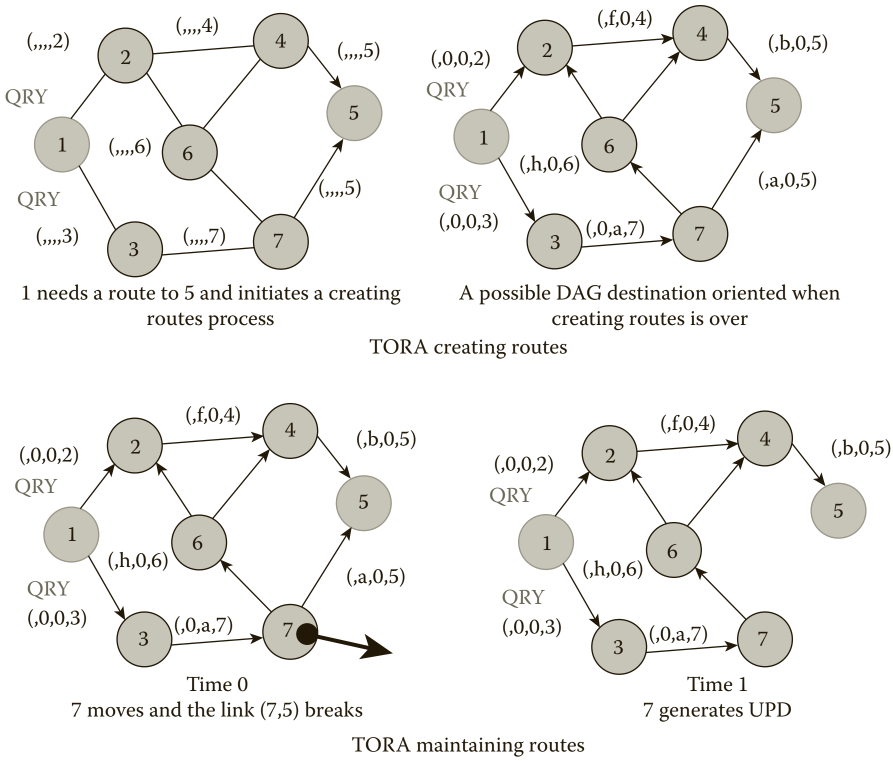

Figure 2.6 TORA routing mechanism.

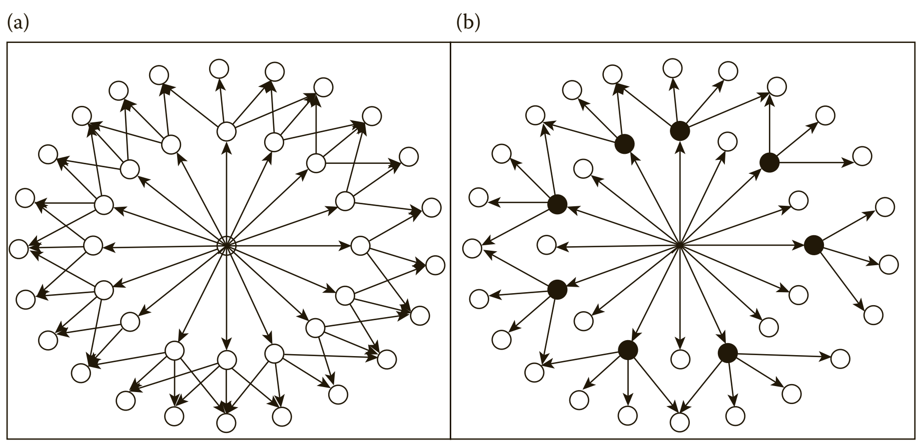

Figure 2.7 OLSR routing mechanism.

due to its limited bandwidth, a compromise has to be made between a small number of emissions and the reliability of delivery.

Every node periodically broadcasts Hello messages that contain one-hop neighbor information. The Time To Live (TTL) of a Hello message is 1, and so they are not forwarded by the neighbors. With the aid of Hello messages, every node obtains local topology information.

A node (also called a selector) chooses a subset of its neighbors to act as MPR nodes based on local topology information, which are later specified in the periodic Hello messages. MPR nodes have two roles:

a. When the selector sends or forwards a broadcast packet, only its MPR nodes among all its neighbors forward the packet.
b. The MPR nodes periodically broadcast the selector list throughout the MANET (again, by means of MPR flooding). Thus, every node in the network knows which MPR nodes could reach every other node.

Note that role (a) reduces the number of retransmissions of the topology information broadcast and role (b) reduces the size of the broadcast packet. As a result, much more bandwidth is saved compared with that saved by original link state routing protocols.

With global topology information stored and updated at every node, the shortest path from one node to every other node can be computed with Dijkstra's algorithm, which goes along a series of MPR nodes.

2.5.5 DSDV

DSDV [17] is a table-driven routing scheme for ad hoc mobile networks based on the Bellman–Ford algorithm. DSDV uses the shortest-path routing algorithm to select a single path to a destination. To avoid routing loops, destination sequence numbers have been introduced. In DSDV, full dumps and incremental updates are sent between nodes to ensure that routing information is distributed.

This protocol is the result of adapting an existing distance-vector routing algorithm to an ad hoc networking environment. DSDV is one of the first attempts to adapt an established routing mechanism to work with MANETs. Each routing table lists all destinations with their current hop count and a sequence number. Routing information is broadcast or multicast. Each node transmits its routing table to its neighbors. Routes with more recent sequence numbers render older routes obsolete. This mechanism provides loop freedom and prevents the use of stale routes. The routing information is transmitted every time a change in the topology has been detected (i.e., a change in the set of neighbors of a node). DSDV works only with bidirectional links. The drawback of this protocol is that it creates large amounts of overhead. Therefore, DSDV is not suitable for large networks, since it consumes more bandwidth than other protocols during the updating procedure.

2.5.6 ZRP

The MANET hybrid routing protocol is a combination of two ad hoc routing approaches: the reactive (on-demand) and the proactive (table-driven). The network in hybrid routing protocols such as ZRP [21] is divided into routing zones. The routing information within each routing zone is proactively distributed, while the global routing information is exchanged reactively. The ZRP approach has proved that it reduces the delay and the amount of routing overheads.

ZRP is a hybrid routing protocol suitable for a wide variety of MANETs, especially with a large network span and diverse mobility patterns. Around each node, ZRP defines a zone where the radius is measured in hops. Each node uses proactive routing within its zone and reactive routing outside its zone. Hence, a given node knows the identity of a route to all nodes within its zone.

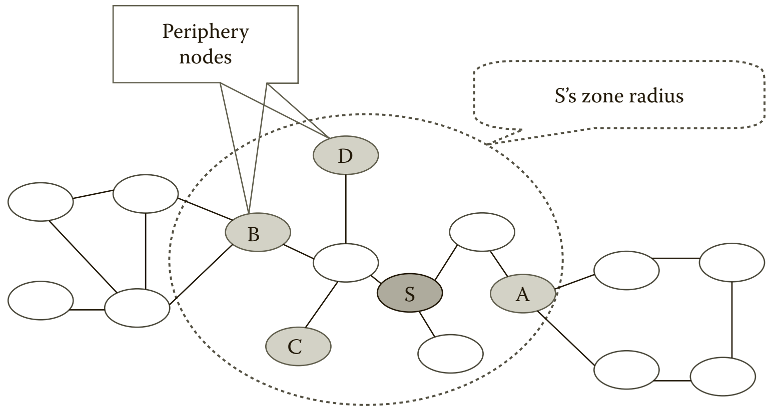

Figure 2.8 ZRP zone radius.

When a node has data for a particular destination node, it checks its routing table for a route. If the destination node is within the zone, a route will exist in the route table; if the destination node is not within the zone, the node will search for that specific destination to find the route.

The proactive maintenance of routing zones also helps to improve the quality of discovered routes by making them more sensitive to changes in the network topology. Zones in ZRP are configured by proper selection of only one parameter, the zone radius, which is measured in hops. The ZRP framework is designed to provide a balance between the contrasting proactive and reactive routing approaches. The proactive routing approach implemented in ZRP is the intrazone routing protocol (IARP). IARP is a link state protocol that maintains up-to-date information about all nodes within a zone. For example, S is a given node; the peripheral nodes of S are A, B, C, and D. The peripheral nodes with the shortest distance to S are defined, as shown in Figure 2.8. These nodes are important for reactive route discovery. The ZRP also utilizes the interzone routing protocol to discover routes to destination nodes outside the zone.

With regard to the route discovery process in ZRP, once the source node determines that the destination node is not within its zone, the source node broadcasts a query message to its peripheral nodes. This query message is relayed using trees constructed within the IARP topology. After receiving the message, the peripheral nodes check whether the destination is within their zone. If the destination is not located, the peripheral nodes broadcast the query message to their own peripheral nodes. This process continues until either the destination node is located or the entire network is searched. Once a node discovers the destination node, it unicasts a reply message to the source node, as shown in Figure 2.8.

The main concept for the ZRP is to integrate the features of both proactive and reactive routing protocols. With proactive (table-driven) protocols inside a limit zone, the connection establishment time can be reduced. On the contrary, reactive routing reduces the amount of control traffic by locating paths on demand for destinations outside the routing zone.

2.5.7 CEDAR

CEDAR is more of a routing framework scheme for QoS requirements than a MANET routing protocol. CEDAR dynamically establishes a core for the network and then incrementally propagates the link state of stable high-bandwidth links to the nodes of the core [23].

CEDAR has three key components. The first is the establishment and maintenance of a self-organizing routing infrastructure, called *the core*, for performing route computations. A subset of the nodes is selected to form a backbone within the network (the core). This structure is used for broadcast messages; hence, no flooding is needed. Each core node maintains the local topology of the nodes in its domain and also performs route computations on behalf of these nodes.

The second component of CEDAR is the propagation of the link state messages of high bandwidth and stable links in the core. The messages sent over the core network are *increase waves* (slow propagating) and *decrease waves* (fast), which notify the core of an increase or decrease in the available bandwidth. For unstable links that rise and fall frequently, the fast-moving decrease wave quickly overtakes and stops the slower-moving decrease wave from propagating, thus ensuring that the link state corresponding to dynamic links is kept local. Therefore, the propagation of these waves is dynamically limited, depending on the available bandwidth. As such, the relevant information for QoS is disseminated in an efficient way. Within the core network, any established ad hoc routing protocol may be used.

The last component of CEDAR is a QoS route computation algorithm that is executed at the core nodes using only locally available states. In order to establish QoS routes, the source node contacts its dominator (local core node) with an RREQ that contains the information on the source, destination, and required bandwidth. The source node then initiates a core broadcast to find the location of the receiver and simultaneously discover the core path. The dominator computes a QoS route, if this is feasible, and then continues to establish it. This includes the possible discovery of the dominator of the destination and a core path to it. Otherwise, if the dominator of the source node has already been cached and has a core path established to the dominator of the destination node, the source node's dominator proceeds with the QoS route establishment phase. If the dominator of the source node does not know the location of the destination node, it first locates the dominator of the destination node and simultaneously establishes a core path to it; this initiates the route computation phase.

A core path from source to destination results in a path in the core graph from the dominator of the source to the dominator of the destination. The dominator of the source then tries to find the shortest-widest-furthest admissible path along the core path. Based on its local information, the dominator of the source picks up the farthest reachable domain until it finds what it knows is an admissible path. It then computes the shortest-widest path to that domain, ending at some node, once again based on local information. Once this path is established, the dominator of the destination then uses its local state to find the shortest-widest-furthest admissible path to the domain along the core path, and so on. Eventually, either an admissible route to the destination is established or the algorithm reports a failure to find an admissible path.

2.5.8 AQOR

Ad hoc QoS on-demand routing (AQOR) provides end-to-end QoS support in terms of bandwidth and end-to-end delays in MANETs [24]. It is a resource reservation-based routing and signaling scheme that allows AQOR to make admission and resource reservation decisions. AQOR integrates on-demand route discovery between the source and the destination, signaling functions for resource reservation and maintenance and hop-by-hop routing. AQOR is also a source-initiated, on-demand routing protocol. It is built upon AODV routing, performing exploration of routes only when required.

The route discovery mechanism is in on-demand mode, broadcasting the RREQ and RREP packets between the source and destination nodes. The route discovery mechanism starts when the node broadcasts RREQ packets with QoS requirements to its neighboring nodes. The neighboring nodes that satisfy the requirement add a route entry to the source node's routing table and forward the RREQ until it reaches the destination. When the RREQ reaches the destination node, an RREP is sent back along the reverse route, reserving bandwidth at each node. Once the source node receives the RREP, it starts sending data out along the reserved route.

AQOR uses timers to detect route breaks and to trigger route recovery. If any node fails to receive a data packet before its reservation expires, a route recovery mechanism is triggered. The source node starts the route discovery process all over again by broadcasting an RREQ packet. Initiating a route discovery process each time a route break occurs can lead to high end-to-end delays. The QoS Multi-Mesh Tree (MMT) routing protocol, which is being designed for AQOR, allows each node to have multiple routes already discovered, with one primary route and other routes as secondary. In case a primary route fails, one of the secondary routes becomes the primary route and the node immediately starts sending data using the new primary route. This facility provided by QoS MMT leads to fast route failure recovery with immediate switch over and low end-to-end delays.

AQOR uses routing tables for keeping track of its routes. Every time a route failure occurs, AQOR must update its routing table entries, which may sometimes result in inconsistent entries due to the high dynamic nature of the network topology. On the contrary, QoS MMT will not use routing tables for facilitating its routing process. This leads to lower processing overheads and excellent consistencies.

None of the previously proposed routing protocols such as AODV and AQOR were able to satisfy all the different MANET application requirements. In this QoS MMT routing protocol being designed, the route discovery, bandwidth reservation, and forwarding is done at the data-link layer (Layer 2). This routing protocol includes all the features of other protocols, such as route discovery, link failure identification, bandwidth calculation, resource reservation, and resource release. It also takes the shared wireless medium and dynamic topology into consideration while providing QoS. To avoid possible loops during route exploration, AQOR uses a route sequence number to indicate the freshness of the control packets for each flow. The sequence number is maintained at each mobile node aware of the flow. The initial sequence number of any flow is 0. When sending out a route control packet for a flow (e.g., RREQ, RREP, or RERR), the initial node will increase its current sequence number by 1 and attach the value to the packet. When control packets are propagated through the network, only nodes with a lower sequence value of the flow will receive them. A node will forward only the first accepted control packet for a certain flow during one round of control packet propagation.

For discovered routes that meet QoS requirements, the admission control policy should guarantee for each flow the requested minimum flow bandwidth *Bmin* and the maximum end-to-end delay *Tmax*. A bandwidth admission control decision is made at every node in the exploration and registration phases, based on the detailed analyses of the traffic in shared channel wireless networks. In AQOR, the route with the shortest end-to-end delay, given it satisfies the bandwidth requirement, is selected.

2.6 Importance of Routing Protocols in MANET

The routing protocols for ad hoc wireless networks should be capable of handling multiple hosts with limited resources, such as bandwidth and energy. The main challenge for routing protocols is that they must also deal with host mobility. This means that hosts can appear and disappear in various locations. Thus, all hosts of the ad hoc network act as routers and must participate in the route discovery and maintenance of routes to the other hosts. For ad hoc routing protocols, it is essential to reduce routing messages overhead despite the increasing number of hosts and their mobility. Keeping the routing table small is another important issue, because the increase in the size of the routing table will affect the control packets sent in the network and this, in turn, will affect large link overheads [25].

The routing in MANETs has been of interest for quite some time in the research community. This section will present a short overview of the proposed work in MANET routing protocols. There are two main algorithms used and based on path selection for most of the existing MANET routing protocols: the Bellman–Ford algorithm [26] and Dijkstra's algorithm [27]. These algorithms are commonly used for the computation of a route in a link state routing protocol and distance vector routing protocols.

Many different routing approaches have been proposed so far to cope with different problems and meet different application requirements. For example, some routing protocols use proactive (table-driven) path discovery to reduce the route discovery delay (time) [11,17–19]. Other routing protocols use reactive (on-demand) path discovery to reduce and control overhead [12–16]. Some other approaches merge proactive and reactive path discoveries to reduce delay and control overhead. This type of protocol is called a *hybrid routing protocol* [21–23].

The hop count is used for path selection as an optimized metric in some routing protocols. Other cost metrics such as link quality and path quality have also been proposed [28,29]. The path filtering and path selection decisions can be made at different types of nodes, for example, at the source node, destination node, and intermediate node. Most routing protocols handle only single paths. However, some other protocols provide and maintain multiple paths [30,31]. The source-tree on-demand adaptive routing (SOAR) [32] is another routing approach that cannot be directly applied to the Bellman–Ford and Dijkstra's algorithms for path selection, because the standard for the choice of successor is determined both by the shortest path and by the set of neighbors that have advertised that route.

There are several approaches for QoS routing protocols based on the on-demand principle of route discovery. The first approach is based on a distributed on-demand path search, which uses a known link bandwidth between nodes [33]. Due to the distributed path calculation, this approach is scalable. Furthermore, by limiting the number of path search requests, flooding is prevented. The scalability and limited protocol overheads are clearly desirable in all ad hoc QoS routing techniques. There are some potential drawbacks to this approach. In particular, the path-finding procedure is not designed to take advantages of QoS information available at the Media Access Control (MAC) layer. The second approach of QoS implementation over ad hoc networks [34–37] focuses specifically on the MAC layer. It is based on the reservation of a node's MAC layer time. In this approach, single or multiple paths to the destination are discovered, and the path bandwidth to the destination node is calculated. However, acquiring the complete path information has several potential drawbacks, such as low scalability, poor tolerance to fast topology changes, and message flooding. The third approach is different from the above solution. It incorporates the QoS path-finding procedure, which is based on a bandwidth-scheduling mechanism. The routing protocol is made aware of the availability of bandwidth resources by coupling routing and MAC Time Division Multiple Access (TDMA) layers [38].

The other issue, which is considered deeply with regard to routing protocols, is the security of the routing protocol. Many proposed protocols are responsible for the creation of secure routing protocols (SRPs). An overview of secure routing in general can be found in the article by Xue and Ganz [39]. The first approach of securing the secure ad hoc on-demand distance vector protocol has been proposed by Gupte and Singhal [40]. In a second publication [41], the protocol was presented in greater detail. Further, related issues, such as key management, were presented briefly in the latter publication. Another secure routing protocol is ARIADNE [42], which is based on DSR. The security mechanism it uses is a broadcast encryption scheme called Timed Efficient Stream Loss-tolerant Authentication (TESLA). The other approach is called Authenticated Routing for Ad hoc Networks (ARAN), which is presented in [43]. ARAN is a reactive routing protocol based on AODV, using certificates. The SRP is another routing protocol with security, which is a reactive protocol relying on a shared secret exchanged *a priori* [44].

In our study, we have observed some shortcomings in existing MANET routing protocols:

- They have not covered all routing problems, such as reducing network load, data drop, and delay,, in some scenarios.
- They find the shortest path from the source to the destination, but for the worst-case scenario, when the shortest path is congested, a different path that might be longer but may be more efficient is used.
- Only the primary route is defined; however, if, for some reason, the primary route fails, then the protocol needs to rediscover the route, which will consume extra time and power.
- They exert extra load on the node in terms of memory size, processing power, and power consumption.
- They are not concerned with link reliability, such as the available data rate (bandwidth), delay, node battery life, and node selfishness, and thus, the path is not guaranteed to deliver the data from the source to the destination.
- Most existing MANET routing protocols find any path from source to destination, but it is not necessarily the optimum path. Such paths are not efficient for different applications.
- Most existing routing protocols send a Hello message or acknowledgment between the nodes, which increases the load and delay on the networks.

In view of the above shortcomings, we have drawn up a list of should-have features when designing a new routing protocol for a MANET. A new routing protocol should have the following features:

- Providing quick and high efficiency, for example, bandwidth, memory, and battery, in adapting to MANET topology change, especially in a high mobility environment
- Providing an alternative path in case the primary path fails; this will save time and power in an ever-changing MANET network topology
- Finding the optimum path instead of the shortest path when applications require QoS, for example, bandwidth, end-to-end delay, and packet losses, to deliver data from the source to the destination
- Providing quick establishment of paths, so that they can be used before an existing path becomes invalid
- Having a minimum control message overhead due to changes in the routing information when topology changes occur
- Consideration of QoS parameters, such as data rate, delay, and node battery life, when locating a path between the source and destination.

References

1. http://www.touchbriefings.com/pdf/744/wire041_vis.pdf
2. M. Abolhasan, T. Wysocki, and E. Dutkiewicz. *A Review of Routing Protocols for Mobile Ad hoc Networks,* vol. 2, no. 1, 2004, pp. 1–22.
3. E.M. Royer and C.K. Toh. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications Magazine*, vol. 6, no. 2, 1999, pp. 46–55.
4. C.Z. Zhang, M.C. Zhou, and M. Yu. Ad hoc network routing and security: a review. *International Journal of Communication Systems*, vol. 20, no. 8, 2007, pp. 909–925.
5. H. Zhou. A survey on routing protocols in MANETs. Technical Report MSU-CSE-03-08, March 2003.
6. J. Broch, D.A. Maltz, D.B. Johnson, Y.-C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking*, October 1998, pp. 85–97.
7. L.M. Feeney. *A Taxonomy for Routing Protocols in Mobile Ad Hoc Networks.* SICS Technical Report. Swedish Institute of Computer Science, 1999.
8. M.Y. Lee, J.-L. Zheng, X.-H. Hu, H.-H. Juan, C.-H. Zhu, Y. Liu, J.S. Yoon, and T.N. Saadawi. A new taxonomy of routing algorithms for wireless mobile ad hoc networks: the component approach. *IEEE Communications Magazine*, vol. 44, no. 11, 2006, pp. 116–123.
9. S.R. Das, C.E. Perkins, and E.M. Royer. Performance comparison of two on-demand routing protocols for ad hoc networks. *IEEE Personal Communications*, vol. 8, no. 1, 2001, pp. 16–28.
10. S.R. Chaudhry, A.N. Al-Khwildi, Y.K. Casey, H. Aldelou, and H.S. Al-Raweshidy. A system performance criteria of on-demand routing in mobile ad hoc networks. In *Wireless and Mobile Computing, Networking and Communications (IEEE WiMob2005)*, August 2005, Montreal, Canada.
11. A.N. Al-Khwildi, K.K. Loo, and H.S. Al-Raweshidy. *Performance Evaluation of Proactive and Reactive Routing in Wireless Ad-Hoc Networks.* In *International Conference on Digital Telecommunications IEEE (ICDT 2006)*, Paris, 2006.
12. A.N. Al-Khwildi, T H. Sulaiman, K.K. Loo, and H.S. Al-Raweshidy. Performance comparison for proactive and reactive routing protocol for wireless ad hoc networks. In *IEEE Science of Electronic Technology of Information and Telecommunications (SETIT 2007)*, Tunisia, 2007.
13. C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In *WMCSA Second IEEE Workshop*, 1999, pp. 90–100.
14. J.G. Jetcheva, Y. Hu, D. Johnson, and D. Maltz. The dynamic source routing protocol for mobile ad hoc networks (DSR). Internet Draft, IETF MANET Working Group, November 2001.
15. S. Corson and P. Vincent. Temporally ordered routing algorithm (TORA). Internet Draft, IETF MANET Working Group, August 2001.
16. C.-K. Toh. Associativity-based routing for ad hoc mobile networks. *Wireless Personal Communication*, vol. 4, no. 2, 1997, pp. 1–36.
17. P. Jacquet and T. Clausen. Optimized link state routing protocol (OLSR). Internet Draft, IETF MANET Working Group, October 2001.
18. C. Perkins and P. Bhagwat. Destination sequenced distance vector (DSDV). Internet Draft, IETF MANET Working Group, November 2001.
19. C.C. Chiang, H.K. Wu, W. Liu, and M. Gerla. Routing in clustered multi hop mobile wireless networks with fading channel. In *Proceedings of IEEE SICON.* Los Angeles: Computer Science Department, University of California, April 1997, pp. 197–211.
20. S. Murthy and J.J. Garcia-Luna-Aceves. An efficient routing protocol for wireless networks. *ACM Mobile Networks and Applications Journal,* vol. 1, no. 2 (Special Issue on Routing in Mobile Communication Networks), 1996, pp. 183–197.
21. L. Wang and S. Olariu. A two-zone hybrid routing protocol for mobile ad hoc networks. *IEEE Transactions on Parallel*, vol. 15, no. 12, 2004, pp. 1105–1116.
22. Z.J. Haas. The routing algorithm for the reconfigurable wireless networks. In *Proceedings of 6th International Conference on Universal Personal Communications (ICUPC)*, vol. 2, 1997, pp. 562–566.

23. M. Joa-Ng and I.T. Lu. A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, 1999, pp. 1415–1425.
24. R. Sivakumar, P. Sinha, and V. Bharghavan. CEDAR: a core-extraction distributed ad hoc routing algorithm. *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, 1999, pp. 1454–1465.
25. Z.A. Ang Eu, K.-G. Seah, and K.-S. Tan. Experimental performance modeling of MANET interconnectivity. In *Proceedings of the 11th International Conference Parallel and Distributed Systems*, vol. 2, July 2005, pp. 155–161.
26. T.H. Ali Ahmed. Modeling and simulation of routing protocol for ad hoc networks combing queuing network analysis and ANT colony algorithms. PhD thesis, University of Duisburg Essen, April 2005.
27. R. Bellman. On a routing problem. *Quarterly of Applied Mathematics*, vol. 16, no. 1, 1958, pp. 87–90.
28. E.W. Dijkstra. A note on two problems in connexion with graphs. *Numerische Mathematik*, vol. 1, 1959, pp. 269–271.
29. B.S. Manoj, R. Ananthapadmanabha, and C. Siva Ram Murthy. Link life based routing protocol for ad hoc wireless networks. In *Proceedings of the 10th IEEE International Conference on Computer Communications and Networks 2001 (IC3N 2001)*, October 2001.
30. D.S.J. De Couto et al. A high-throughput path metric for multi-hop wireless routing. In *Proceedings of the 9th ACM International Conference on Mobile Computing and Networking (MobiCom'03)*, San Diego, CA, September 2003.
31. V.D. Park and M.S. Corson. A highly adaptive distributed routing algorithm for mobile wireless networks. *In Proceedings of InfoCom'97*, April 1997.
32. S. De, C. Qiao, and H. Wu. Meshed multipath routing with selective forwarding: an efficient strategy in wireless sensor networks. *Computer Networks*, vol. 43, 2003, pp. 481–97.
33. S. Roy and J.J. Garcia-Luna-Aceves. An efficient path selection algorithm for on-demand link-state hop-by-hop routing. In *Computer Communications and Networks, Eleventh International Conference*, October 2002, pp. 561–564.
34. S. Chen and K. Nahrstedt. Distributed quality-of-service routing in ad hoc networks. *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, 1999, pp. 1488–1505.
35. T.-W. Chen, J.T. Tsai, and M. Gerla. QoS routing performance in multihop, multimedia, wireless networks. In *IEEE 6th International Conference Universal Personal Communications*, vol. 2, 1997, pp. 557–561.
36. C.H. Lin and J.S. Liu. QoS routing in ad hoc wireless networks. *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, 1999, pp. 1426–1438.
37. C.R. Lin and C.C. Liu. An on-demand QoS routing protocol for mobile ad hoc networks. In *Proceedings of the IEEE Global Telecommunications Conference*, vol. 3, 2000, pp. 1783–1787.
38. Y.K. Ho and R.S. Liu. On-demand QoS-based routing protocol for ad hoc mobile wireless networks. In *Proceedings of the ISCC Fifth IEEE Symposium on Computers and Communications*, 2000, pp. 560–565.
39. Q. Xue and A. Ganz. Ad hoc QoS on-demand routing (AQOR) in mobile ad hoc networks. *Journal of Parallel and Distributed Computing*, vol. 63, 2003, pp. 54–165.
40. S. Gupte and M. Singhal. Secure routing in mobile wireless ad hoc networks. *Ad Hoc Networks*, vol. 1, no. 1, 2003, pp. 151–174.
41. M.G. Zapata. 2002. Secure ad hoc on-demand distance vector routing. *SIGMOBILE Mob. Comput. Commun,* Rev. 6, 3 (June 2002), http://doi.acm.org/10.1145/581291.581312, 2002, pp. 106–107.
42. M.G. Zapata and N. Asokan. Securing ad-hoc routing protocols. In *Proceedings of the 2002 ACM Workshop on Wireless Security*, September 2002, pp. 1–10.
43. Y.-C. Hu, A. Perrig, and D.B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*, ACM, Atlanta, September 2002, pp. 12–23.
44. K. Sanzgiri, B.N. Levine, C. Shields, B. Dahill, and E.M. Belding-Royer. A secure routing protocol for ad hoc networks. In *Proceedings of the 10th IEEE International Conference on Network Protocols*, November 2002.

Chapter 3

Modeling and Simulation Tools for Mobile Ad Hoc Networks

Kayhan Erciyes, Orhan Dagdeviren, Deniz Cokuslu, Onur Yılmaz, and Hasan Gumus

Contents

A *model* is a simplified representation of a system that aids the understanding and investigation of the real system. *Simulation* is the manipulation of the model of a system that enables one to observe the behavior of the system in a setting similar to real life. By modeling and simulation of a mobile ad hoc network (MANET), it is possible to simplify many difficult real-life problems associated with them. Modeling and simulation of a MANET have limitations, and providing further flexibility in them such that a general MANET without much limitations can be modeled and simulated is an important research topic. In this chapter, we review network models, topology control models, mobility models, and simulators for MANETs by investigating their current limitations and future trends.

3.1 Introduction

Ad hoc networks are a key to the evolution of wireless networks. MANETs are nonfixed infrastructure networks that consist of dynamic collection of nodes with rapidly changing topologies of wireless links. Although military tactical communication is still considered the primary application for ad hoc networks, commercial interest in these types of networks continues to grow. Applications such as rescue missions in times of natural disasters, law enforcement operations, commercial and educational use of sensor networks, and personal area networking are just a few possible commercial examples. MANETs have the problems of bandwidth optimization, transmission quality, discovery, ad hoc addressing, self-routing, and power control. Power control is a very important issue in MANETs because nodes are powered by batteries only. Therefore, amount of communication should be minimized to avoid a premature dropout of a node from the network.

Links in a MANET change dynamically over time; thus, a functioning network must be able to deal with this dynamic nature. One key problem in MANETs is to model the mobile nodes and the communication edges of the network to provide a solution step for well-known problems such as medium access control (MAC) design, clustering, and backbone formation. These models should capture the behavior of the wireless transmission in different conditions since wireless transmissions in a MANET operating on a flat unobstructed environment may totally differ from the wireless transmissions in an ad hoc network of nodes each located on a building.

MANETs may be of large scale, consisting of even hundreds of nodes operating for the completion of an application. These nodes may be small and cheap devices as well as expensive military vehicles designed for operating in harsh conditions. Scientists aim to improve the operation quality and decrease the resource usage in MANETs by researching the various topics in communication layers. These studies may include theoretical analysis and extensive experiments to validate the superiority of the work. Since it is not feasible for researchers to afford the experiments on hundreds of moving nodes located on large areas, another key problem arises in MANETs: providing suitable simulation test beds.

3.1.1 Challenges

A MANET can be modeled as a graph $G(V, E)$, where V is the set of vertices and E is the set of edges. Two vertices (nodes) of a graph are connected only if there is a communication link between them. Once a MANET is represented as a graph, the next issue at hand is whether any graph property has any implications for the MANET. For example, a dominating set (DS) D of a graph is the set of vertices where a vertex $v \in V$ is either in D or adjacent to a vertex in D. If vertices of a DS are connected, the DS is called a *connected dominating set* (CDS), and forming a CDS in the graph model of the MANET provides a communication backbone for routing purposes in the actual mobile network. However, finding a minimum DS or a CDS is an NP-complete problem in graph theory, and hence approximation algorithms for such problems where suboptimal solutions using some heuristics are usually the only choice. However, designing an approximation algorithm with a favorable approximation ratio to the optimum solution to the problem is not sufficient, since one is dealing with a real network without any global information. Any algorithm employed must be distributed without any global knowledge. A distributed algorithm is run by all nodes of a MANET, provides exchange of information with its neighbor nodes by message passing only, and eventually results in reaching a determined state of the network [1]. Based on the above discussion, the challenge is in fact designing of distributed approximation algorithm with a favorable approximation ratio that can be implemented on the graph model of the MANET, which provides a solution to a graph problem that is usually extremal and has implications in the real MANET environment. Some other real-life considerations such as the battery lifetime of nodes in sensor networks or the mobility of the nodes in a MANET may have to be incorporated to the distributed approximation algorithm as the final adjustment.

Another example would be the vertex cover problem in a graph. A vertex cover of a graph is the set of vertices $S \in V$ such that any edge e is incident to at least one vertex in S. Finding a vertex cover of minimum size is NP-complete. For a distributed robot network such as a Special Weapons and Tactics (SWAT), finding a vertex cover is equivalent to placing robots at the corners of a maze such that every robot is in sight of at least another robot, which means all robots remain connected.

3.1.2 Scope

The scope of this chapter is to first specify basic models for MANETs. One such useful model is the graph representation, and once this is done, all of the graph theoretic results become available for the MANET. The key point then is the proper choice of some useful properties of graphs for the MANET as described earlier and designing of efficient and scalable distributed approximation algorithms. We show in Section 3.3 the external graph problems that have direct or indirect implementations for MANETs. We then provide detailed descriptions of the simulation platforms for MANETs. Section 3.2 outlines models for MANETs, whereas simulators for MANETs are discussed in Section 3.3. The conclusions are drawn in Section 3.4.

3.2 Modeling

In this section, we explain the network models, topology control models, and mobility models with their current limitations and future trends in modeling.

3.2.1 Network Models

3.2.1.1 Unit Disk Graph

A unit disk graph (UDG) is a special instance of a graph in which each node is identified with a disk of unit radius $r = 1$, and there is an edge between two nodes u and v if and only if the distance between u and v is at most 1 [2,3]. The model is depicted in Figure 3.1a. Each node's transmission range is drawn as a dotted circle. The edges, which connect nodes, are drawn as straight lines. The neighbors of node u are node v, node w, node y, and node z as shown in the simplified graph in Figure 3.1b.

This model is very simple yet captures the behavior of broadcast radio transmission; thus, it is good for modeling ad hoc and sensor networks [3]. It may be also suitable for modeling ad hoc networks located on unobstructed environments. Moreover, since this model is open for theoretical analysis due to its geometric properties, it is an important playground for the approximation algorithm designers. Efficient distributed approximation algorithms targeting to solve NP-complete network topology control problems such as finding minimum dominating set and maximum independent set, which will be described in the following sections, are studied by the researchers. Although UDG is a widely used networking model, it has drawbacks caused by its simplicity. In

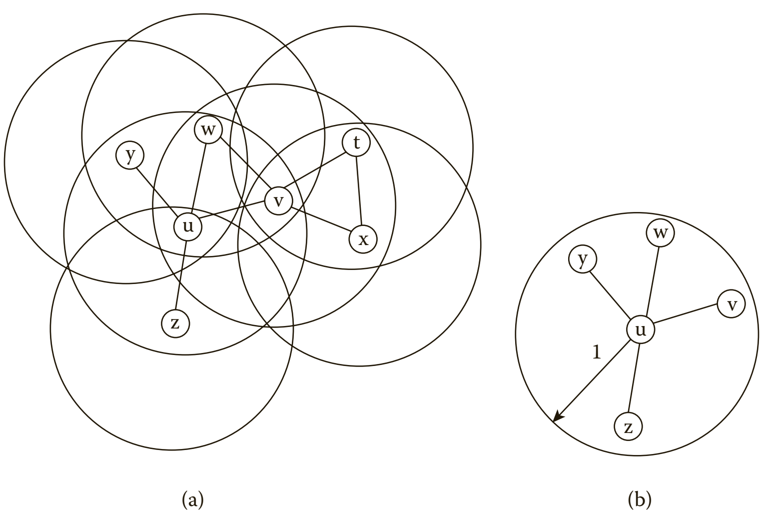

Figure 3.1 (a) Unit disk graph model. (b) Node *u*'s neighbors.

real configurations, the wireless transmission may be disturbed by even small obstacles between communicating parties; therefore, UDG is not a realistic model for ad hoc networks located on areas consisting of heterogeneous objects. It does not model the signal quality between nodes, so it may result in poor topology control for multihop communication. Also it lacks modeling node weights consisting of node mobility, energy, etc., which makes UDG not suitable for the selection of routes with high weighted nodes.

3.2.1.2 Quasi Unit Disk Graph

In a quasi unit disk graph (QUDG), each node is identified with two disks: one with unit radius $r = 1$ and other with radius $q = (0, 1]$. It can be observed that a QUDG with $q = 1$ is a UDG [4]. The edges between nodes d away from each other are identified with respect to the below listed rules:

- There is an edge between two nodes if $d = (0, q)$.
- There is a possible edge connecting two nodes if $d = (q, 1]$.
- There is no edge between two nodes if $d = (1, \infty]$.

The model is depicted in Figure 3.2a. The inner circles are drawn with the dashed lines. The bold lines are communication edges, and the other lines are possible edges. In Figure 3.2b, the connections of node *w* are shown. Node *y* is the neighbor of node *w*; other nodes are the candidates for being the neighbors of node *w*.

QUDG is an extended model of UDG in which probabilistic links can be modeled. Also in QUDG model, the effect of the small obstacles located in the network area can be handled by adjusting the parameter *q*. Although the QUDG model has these advantages over the UDG model, the other disadvantages of the UDG model given in the previous section still exist in the QUDG model.

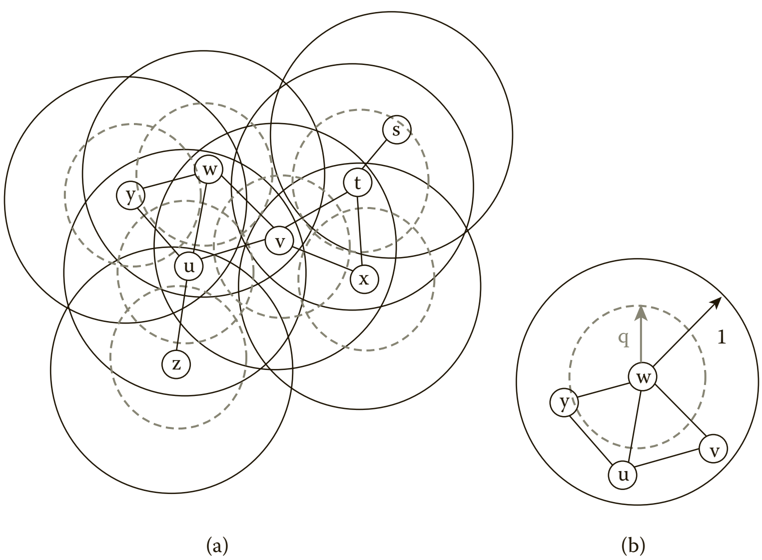

Figure 3.2 (a) Quasi unit disk graph model. (b) Node *w*'s neighbors.

3.2.1.3 Undirected Graph

An undirected graph (UG) is described as $G = (V, E)$, where V is the set of vertices or nodes ($V = \{V_1, V_2, V_3, \ldots, V_N\}$) and E is the set of edges between these vertices ($E = \{E_{12}, E_{21}, \ldots\}$). E_{xy} is an edge starting from vertex x and ending at vertex y. If there is a communication link between V_1 and V_2, then $E \in E_{12}$ and $E_{21.}$ Since the graph is undirected, links are assumed to be starting and ending on both sides. An example network with 10 nodes modeled with UG is depicted in Figure 3.3. In this model, the set of vertices is $V = \{V_1, V_2, V_3, \ldots, V_{10}\}$ and the set of edges is $E = \{E_{16}, E_{61}, E_{26}, E_{62}, \ldots, E_{910}, E_{109}\}$.

The UG model is simple and very common for various types of networks. There are many cases where modeling ad hoc networks with a UG is suitable. Also there is a significant amount of research on the UG model. In this model, the geometric properties of the wireless networks cannot be applied. Thus, this model results in more complicated approximation algorithm designs with probably higher resource requirements compared with the models with defined geometric property like a UDG. By not assuming a geometric wireless transmission pattern, this model may also be defined as pessimistic. One of the most important disadvantages of this model compared with the UDG and partially QUDG model is the undirected link assumption wherein real networks it may not be realistic. Also in a UG, node and edge weights cannot be modeled.

3.2.1.4 Directed Graph

A directed graph (DG) is described as UG: $G = (V, E)$, where E may contain one of E_{xy} and E_{yx}. A sample DG model is given in Figure 3.4. In this model, the set of vertices is $V = \{V_1, V_2, V_3, \ldots, V_{10}\}$ and the set of edges is $E = \{E_{16}, E_{26}, E_{38}, \ldots, E_{107}\}$. DG is an extended model of UG that captures the behavior of the heterogeneous ad hoc networks of nodes with different transmission ranges. In Figure 3.4, the transmission ranges of the nodes are depicted with the dotted circles of different sizes. Like a UG, a DG cannot assume a geometric transmission property and does not model the edge and node weights.

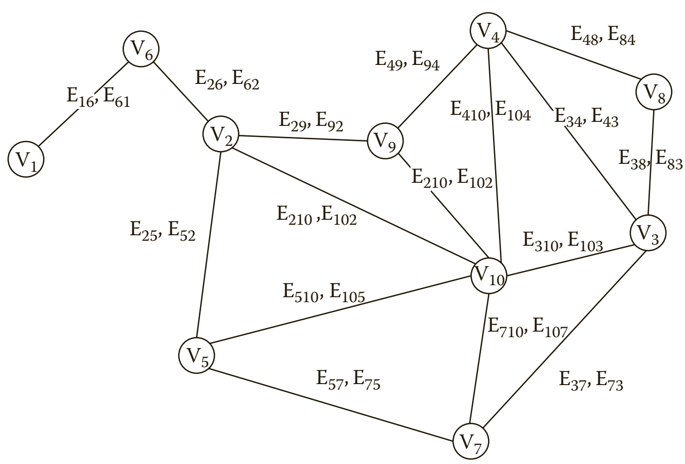

Figure 3.3 Undirected graph model.

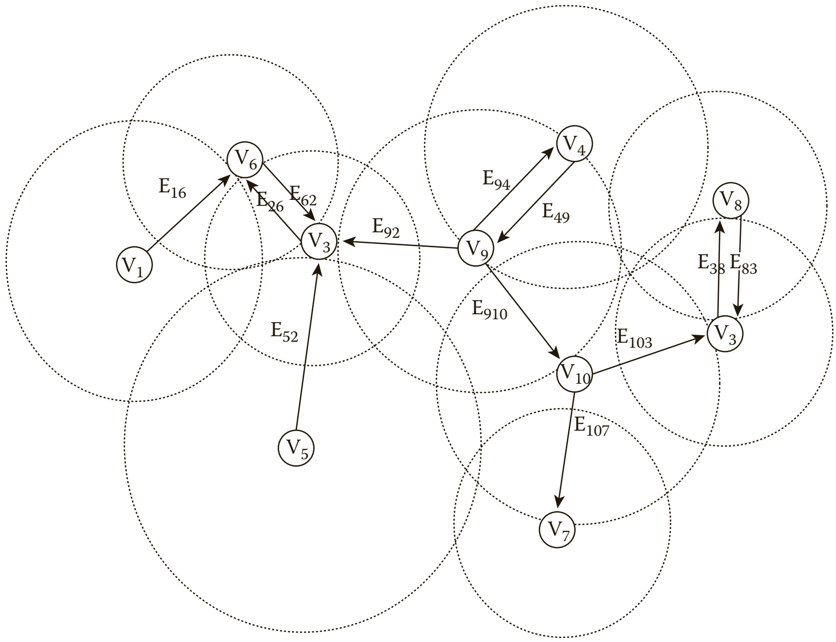

Figure 3.4 Directed graph model.

3.2.1.5 Weighted Graph

A weighted graph (WG) G_w can be *node weighted graph*: $G_{nw} = (V_w, E)$; *edge weighted graph*: $G_{ew} = (V, E_w)$; or the combination of both: $G_{new} = (V_w, E_w)$. Also a WG can be *undirected weighted graph* (UWG) or *directed weighted graph* (DWG). The weight of a node can be mobility, energy, nodal degree, etc., or a combination of all. The weight of an edge can be the signal strength, distance, etc. The weights are usually positive numbers, but negative numbers may also be used. Sometimes the cost term is used instead of weight.

An example directed node and edge weighted graph is depicted in Figure 3.5. The transmission ranges of the nodes are not identical; thus, connectivity between two nodes may be both unidirectional and bidirectional. The weight of a node in this figure is assumed to be 1/energy. An edge is represented with the signal strength. Like UG and DG, a DWG does not use geometric properties of the wireless transmission; thus, it is a pessimistic model.

3.2.2 Topology Control Models

3.2.2.1 Independent Set

An independent set (IS) is a set of nodes in which none of the nodes are adjacent. If this set cannot be extended by adding a new node, then IS is called the maximal IS. The IS with the greatest number of nodes is called the maximum IS. In Figure 3.6a, six gray-filled nodes are the elements of the maximal IS. However, this set cannot be extended by adding a new node; removing some nodes from this set and adding other nodes may increase the size. In Figure 3.6b, the maximum IS with eight nodes is shown. In the weighted version of this problem, a weight is assigned to each node,