mobile communications series

Ramjee Prasad
Albena Mihovska
editors

NEW HORIZONS IN MOBILE AND WIRELESS COMMUNICATIONS

VOLUME 4 Ad Hoc Networks and PANs

sidemirror

New Horizons in Mobile and Wireless Communications

Volume 4
Ad Hoc Networks and PANs

Ramjee Prasad
Albena Mihovska

Editors

ARTECH HOUSE
BOSTON | LONDON
artechhouse.com

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the U.S. Library of Congress.

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

ISBN-13: 978-1-60783-973-6

Cover design by Igor Valdman

685 Canton Street
Norwood, MA 02062

10 9 8 7 6 5 4 3 2 1

New Horizons in Mobile and Wireless Communications

Volume 4
Ad Hoc Networks and PANs

For a list of recent related titles in the *Artech House Universal Personal Communications Series*, please turn to the back of this book.

Acknowledgments

First of all, the editors would like to acknowledge Ms. Dua Idris from CTIF at Aalborg University for her big effort towards the completion of this book. Dua was involved in the FP6 IST project SIDEMIRROR as a research engineer. Her consistent hard work and passionate efforts toward improving the quality of the content are very commendable.

Further, this book would not have been possible without the strong support of the European Union project officers from the Directorate General Information Society (DG INFSO) of the European Commission in Brussels, namely, Dr. Jorge M. Pereira, Dr. Manuel Monteiro, and Dr. Francisco Guirao Moya, who guided the project work and ensured strong cooperation with the rest of the FP6 IST projects in the area. Their effort was an essential prerequisite for the successful editing of the available research results. The material in this book was collected and structured with the support of the European Commission within the framework of the IST supporting project SIDEMIRROR, in an effort that spanned a period of five years. It originated from the technical reports and documentation of the projects involved in the FP6 IST R&D initiatives *Mobile and Wireless Systems Beyond 3G* and *Broadband for All.*

The project SIDEMIRROR consisted of two member organizations, Aalborg University and Artech House Publishers. The editors would like to acknowledge the support of their colleagues from Artech House toward the completion of this manuscript. Finally, the editors would like to thank the administrative and IT staff from Aalborg University for providing the required administrative and IT project support.

Ramjee Prasad
Albena Mihovska
Aalborg, Denmark
September 2009

The Artech House Universal Personal Communications Series

Ramjee Prasad, Series Editor

4G Roadmap and Emerging Communication Technologies, Young Kyun Kim and Ramjee Prasad

802.11 WLANs and IP Networking: Security, QoS, and Mobility, Anand R. Prasad and Neeli R. Prasad

CDMA for Wireless Personal Communications, Ramjee Prasad

From WPANs to Personal Networks: Technologies and Applications, Ramjee Prasad and Luc Deneire

IP/ATM Mobile Satellite Networks, John Farserotu and Ramjee Prasad

Multicarrier Techniques for 4G Mobile Communications, Shinsuke Hara and Ramjee Prasad

New Horizons in Mobile and Wireless Communications, Ramjee Prasad and Albena Mihovska, editors
Volume 1: Radio Interfaces
Volume 2: Networks, Services, and Applications
Volume 3: Reconfigurability
Volume 4: Ad Hoc Networks and PANs

OFDM Towards Broadband Wireless Access, Uma Shanker and Jha Ramjee Prasad

OFDM for Wireless Communications Systems, Ramjee Prasad

OFDM for Wireless Multimedia Communications, Richard van Nee and Ramjee Prasad

Practical Radio Resource Management in Wireless Systems, Sofoklis A. Kyriazakos and George T. Karetsos

Radio over Fiber Technologies for Mobile Communications Networks, Hamed Al-Raweshidy and Shozo Komaki, editors

Simulation and Software Radio for Mobile Communications, Hiroshi Harada and Ramjee Prasad

Space-Time Codes and MIMO Systems, Mohinder Jankiraman

TDD-CDMA for Wireless Communications, Riaz Esmailzadeh and Masao Nakagawa

Technology Trends in Wireless Communications, Ramjee Prasad and Marina Ruggieri

Third Generation Mobile Communication Systems, Ramjee Prasad, Werner Mohr, and Walter Konhäuser, editors

Towards a Global 3G System: Advanced Mobile Communications in Europe, Volume 1, Ramjee Prasad, editor

Towards a Global 3G System: Advanced Mobile Communications in Europe, Volume 2, Ramjee Prasad, editor

Towards the Wireless Information Society: Heterogeneous Networks, Ramjee Prasad, editor

Towards the Wireless Information Society: Systems, Services, and Applications, Ramjee Prasad, editor

Universal Wireless Personal Communications, Ramjee Prasad

WCDMA: Towards IP Mobility and Mobile Internet, Tero Ojanperä and Ramjee Prasad, editors

Wideband CDMA for Third Generation Mobile Communications, Tero Ojanperä and Ramjee Prasad, editors

Wireless Communications Security, Hideki Imai, Mohammad Ghulam Rahman and Kazukuni Kobara

Wireless IP and Building the Mobile Internet, Sudhir Dixit and Ramjee Prasad, editors

WLAN Systems and Wireless IP for Next Generation Communications, Neeli Prasad and Anand Prasad, editors

WLANs and WPANs towards 4G Wireless, Ramjee Prasad and Luis Muñoz

For further information on these and other Artech House titles, including previously considered out-of-print books now available through our In-Print-Forever® (IPF®) program, contact:

Artech House
685 Canton Street
Norwood, MA 02062
Phone: 781-769-9750
Fax: 781-769-6334
e-mail: artech@artechhouse.com

Artech House
16 Sussex Street
London SW1V 4RW UK
Phone: +44 (0)20 7596-8750
Fax: +44 (0)20 7630-0166
e-mail: artech-uk@artechhouse.com

Find us on the World Wide Web at: www.artechhouse.com

Contents

CHAPTER 1

Introduction

Ad hoc networks are important enablers for next generation communications. Generally, such networks can be formed and deconfigured on-the fly and do not require a particular underlying infrastructure (i.e., there is no need for a fixed base station, routers, or cables). Ad hoc networks can be mobile, stand-alone or internetworked with other networks.

A *wireless* ad hoc network is a collection of autonomous nodes or terminals that communicate with each other by forming a multihop radio network and maintaining connectivity in a decentralized manner. Just as any radio network, wireless ad hoc networks, suffer from issues such as noise, interference, fading, insufficient bandwidth, and so forth.

Ad hoc networks are at the basis of concepts such as reconfigurability, self-organization, pervasiveness, ubiquity, dynamics, and user-centricity, which have been recognized as the main characteristics of next generation communication systems. Therefore, research in the area of ad hoc networking is receiving much attention from academia, industry, and government. These networks pose many complex issues and many open problems.

The European-funded research under the umbrella of the Framework Program Six (FP6) provided significant contributions to the advancement of the ad hoc network concepts and standards [1, 2]. In particular, it contributed to the developments in the area of sensor networks, personal networks and federations, wireless mesh networks, multihop communications and their integration with cellular systems and the backbone infrastructure, reconfigurability, routing, and some others.

This book provides a comprehensive overview of the main contributions realized by the FP6 EU-funded projects in the area of Information Society Technology (IST) and under the themes *Mobile and Wireless Systems Beyond 3G* and *Broadband for All*. This chapter introduces into the topic of ad hoc networks. In particular, Section 1.1 gives an overview of the current state of the art in the area, and describes the main types of ad hoc networks and their characteristics. Section 1.2 gives an overview of the standardization and regulation activities in the area. Section 1.3 provides and overview of the book.

1.1 Wireless Ad Hoc Networks

A wireless ad hoc network can be understood as a computer network with wireless communication links where each node has the capacity to forward the data to other nodes. The decision for determining what nodes are to forward the data and to whom are made dynamically based on the connectivity in the concerned network. This feature makes it different from the wired network technologies where designated nodes with custom hardware are forwarding the data or from the managed wireless networks where a special node is assigned to manage the communication between other nodes. The main features of the ad hoc networks are their minimum requirements for configuration and quick deployment.

Each node in a wireless ad hoc network functions as both a host and a router, and the control of the network is distributed among the nodes. The network topology is in general dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes. Hence, there is a need for efficient routing protocols to allow the nodes to communicate over multihop paths consisting of possibly several links in a way that does not use an excess of network resources.

There are two main types of ad hoc networks, *mobile ad hoc networks* (MANETs) and *wireless sensor networks* (WSNs).

1.1.1 Mobile Ad Hoc Networks (MANETs)

A mobile ad hoc network (MANET) is a self-configuring network consisting of mobile routers that are interconnected by (usually bandwidth-constrained) wireless links. The vision of MANETs is to support robust and efficient operation in mobile wireless networks by incorporating a routing functionality into the mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies, which are likely composed of relatively bandwidth-constrained wireless links. The network is decentralized and all network activity including the discovery of the topology and the delivery of messages is executed by the mobile nodes themselves.

MANETs can range from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue [3]. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. The determination of viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns, especially when MANETs are used in the context of defense or dual-use applications [4]. A lapse in any of these requirements may degrade the performance and dependability of the network.

Mobile ad hoc devices are able to detect the presence of other ad hoc devices, establish communication links among each other, and communicate information such as packetized digital data. The traditional work around MANETs had largely focused on homogeneous nodes and single parameter optimization [5]. Within the FP6 IST program, the projects MAGNET and MAGNET Beyond [5] extended these concepts in support of PN technologies.

1.1.1.1 Self-Organization Capabilities

Current radio technologies offer, up to a certain extent, self-organizational capabilities at the link layer: 802.11 provides link-level self-organization, Bluetooth networks organize themselves by forming piconets or even scatternets. Self-organization at the network layer is also receiving a lot of attention in the context of MANETs, in which nodes need to cooperate to organize themselves and to provide network functionality, due to the absence of any fixed infrastructure.

In the context of PNs [5], the problem has a completely different dimension, because self-organization spans over multiple network technologies and strongly builds on the concept of trust between the *personal nodes* and *devices*. Security, privacy, and trust solutions were another research challenge undertaken within the frames of the FP6 IST projects.

A PN should be self-organizing and self-maintaining, handling mobility and thereby providing its own addressing and routing mechanisms for its internal communication (i.e., support of dynamic behavior). Therefore, developing PN networking solutions can build to a certain extent on ad hoc networking techniques and concepts. Due to the specific nature and context of PNs, existing solutions for mobile ad hoc networks cannot be adopted directly. A PN has a specific wireless/wired geographically dispersed network topology, which, to a certain extent, can rely on the fixed infrastructure (e.g., edge routers, for providing networking solutions). Also, PNs are built around a specific trust relation concept, on which higher layer protocols can rely, which is absent in traditional ad hoc networks. Therefore, the overall PN architecture proposed in the IST project MAGNET was quite novel [5].

1.1.1.2 Mobility

The field of mobile ad hoc networks has seen a rapid expansion due to the proliferation of wireless devices, witnessed by the efforts in the IETF MANET working group [6]. A lot of attention was given to the development of routing protocols, with the MANET group working on the standardization of a general reactive and proactive routing protocol, and, in a lesser extent, to addressing and Internet connectivity [7]. Mobility of individual devices, mobility of complete clusters and splitting and merging of clusters (especially in the context of PNs), requires efficient mobility solutions. Worth mentioning in this context are the activities on mobile networks within the Mobile IP (MIP) Working Group [8] of the IETF, the work on the extensions of MIP for mobile ad hoc networks interconnection [9], and the work within the Network Mobility (NEMO) working group that is concerned with the mobility of an entire network. People are beginning to carry multiple Internet-enabled devices such as cell phones, PDAs, laptop computers, and music players. Instead of each device connecting to the Internet separate, all of the devices could connect to the Internet through a PAN. Using NEMO, one device, such as a cell phone, would act as the mobile router providing continuous access to the rest of the devices. Mobility solutions for PNs can borrow from this work, but should be adapted to fit the underlying PN architecture and addressing schemes.

The NEMO architecture was adopted in the FP6 IST project DAIDALOS to allow a network to move as a whole [10]. A single point, the *mobile router* (MR), manages the mobility of the network.

Initially, the DAIDALOS architecture was designed and developed as a stand-alone subsystem, supporting the following three main functionalities:

- Network mobility basic support, by implementing partially the NEMO basic support protocol [11];
- Route optimization support for local fixed nodes and nested configurations [12];
- Multicast support for mobile networks [13].

Integration efforts are required to develop new solutions that make possible the provision of QoS and security to mobile networks, as well as the efficient support of mobile nodes roaming between moving networks and infrastructure-based access networks [14]. In addition to these features, the NEMO architecture was enhanced by means of improved route optimization solutions (supporting also VisitingMobileNodes), by enriched multicast mechanisms, and the support for localized mobility solutions (based on an extension of the *network-based localized mobility management*—NetLMM protocol) [15].

The MANETs in DAIDALOS II can be seen as multihop networks connected to the core network by means of one or more gateways. Because the access clouds could be considered as local mobility domains, the integration of the MANET within the overall architecture required the analysis of the interaction between these networks with the local mobility management protocol. Such interactions depend on the number of gateways supported and their location, in the same or different local domains. This, in turn, has impact on the ad hoc nodes address configuration and on the mobility management.

The concept of multihoming can also be applied to MANETs where multiple egress/ingress points (gateways) are considered. In the case of multiple gateways inside the same local domain, or in different local domains, the implementation and integration of MANETs (e.g., the DAIDALOS implementation) also provides QoS and security support. Inside the MANET the solutions can be specifically built according to the MANET unstable and dynamic characteristics; however, once these are integrated with the infrastructure, they are not visible to the outside of the MANET. The integration of the MANET concept in the overall DAIDALOS architecture is shown in Figure 1.1.

Figure 1.1 includes the basic network components and protocols, which build-up a mobility and QoS integrated architecture, including the MANET and NEMO networks, and the support of multicast services [15]. The various network devices exchange differing control information depending on the service that is being delivered.

The requirements taken into account for the design of the architecture are the following:

- Access network operators can implement their own mobility solution (within their domains). The solution must be independent of external mobility operators (including home);
- Minimize complexity in the terminal;
- Efficient use of wireless resources;

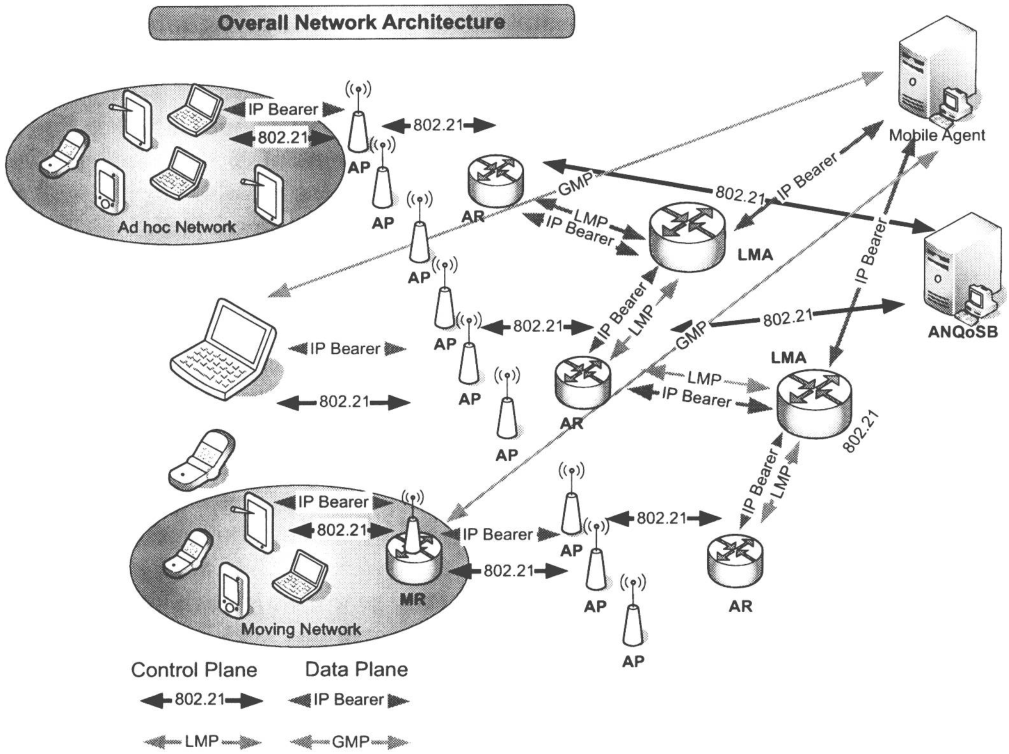

Figure 1.1 Integration of the MANET and NEMO concepts in the DAIDALOS architecture [15].

- Reduced signaling overhead in the network;
- The solution must be security friendly;
- Seamless handover support;
- Multihoming support;
- Scalability for routing;
- Minimize network side nodes modifications;
- Support for heterogeneous networking;
- QoS provision.

1.1.1.3 Security, Privacy, and Trust for Ad Hoc Networks

Easy, secure, and simple establishment of connections between devices and networks is the key to support data exchange in various scenarios. Current solutions and protocols are very heavy and not user friendly for secure access to network, services, and devices, which makes these unsuitable for use in MANET0 scenarios. Routing is one of the main processes on the networking abstraction level, which is responsible for the finding and establishment of the routes among the communicating nodes. Current ad hoc routing protocols inherently trust all participants. Most ad hoc routing protocols are cooperative by nature and depend on neighboring nodes to route packets. Such a naive trust model allows malicious nodes to paralyze an ad hoc network by inserting erroneous routing updates, replaying old messages, changing routing updates or advertising incorrect routing information. None of the protocols such as the *Ad Hoc On Demand Distance Vector Routing* (AODV), *Dynamic Source Routing* (DSR), Ariadne, the *Authenticated Routing for Ad Hoc Networks* (ARAN), the *Security Aware Routing* (SAR), or the *Server Routing Protocol* (SRP), provide a solution to the requirements of certain discovery, isolation, or robustness. The routing process must be shielded by solutions that will grant the integrity and the availability of the networking procedures [16].

The capability to provide secure context transfer is essential in achieving fast performance in a wireless environment. Secure fast context transfer in handovers between heterogeneous access technologies/network types is needed. Furthermore, providing context-aware, adaptive and personalized services to the user, poses many opportunities, challenges, and risks. The ability to offer secure, intuitive, and easy-to-use solutions for accessing contextual services that have to be location-aware and time-sensitive; personal preference and network bandwidth aware, and finally, device-capability aware, is a big challenge. In addition to routing and context transfer, key management is a fundamental prerequisite for any cryptography-based security solution. For example, in personal area networks (PANs) most personal nodes are low-capacity devices, therefore, the security protocols in both lower and upper layers, must rely on optimized cryptographic algorithms, which consume less resources but hence provide the necessary security features.

In the future ad hoc network, trust, identity management, and privacy will need considerable effort if end-to-end security is required. Thus, a mechanism of enabling extension of the trust between individual nodes needs to be defined. Also, protection of user location, identity, and privacy need to be considered. The user's location, identity and privacy requirements must be taken into account by the mobility procedures. The precise nature of these requirements may have a considerable impact on the mobility procedures.

1.1.1.4 Vehicular Ad Hoc Networks (VANETs)

The *vehicular ad hoc network* (VANET) is a form of MANET, which is used for communication among vehicles and between vehicles and roadside equipment. The VANET formed by a number of nearby peers is organized in a fully decentralized fashion, in order to cope with continuous arrival and disappearance of peers.

The 802.11p [17] amendment of the IEEE 802.11 family of standards is currently drafted specifically for such vehicular ad hoc communications. However, IEEE 802.11p is predicted to be limited in situations with a high peer density, compromising reliable transmission of time-critical safety related messages. Safety improving messages may also arrive from sensors installed along roads through a low data rate air interface based on, for example, IEEE 802.15.4. Access via roadside units that are part of some VANETs are a further possibility. Additionally, some peers may be part of a *wireless personal area network* (WPAN) based on e.g., Bluetooth. Besides, some peers might have access to the infrastructure. Possible access networks are UMTS, WLANs available in hot spots, or WiMAX.

The *intelligent vehicular ad hoc network* (InVANET) makes use of WiFi IEEE 802.11b/802.11g/802.11p and WiMAX IEEE 802.16 for providing easy, accurate, effective communication between multiple vehicles on dynamic mobility.