



Christina Belisario  
Research Coordinator  
Morrison Foerster  
12531 High Bluff Drive, Suite 200  
San Diego, CA 92130-2040  
USA

14 November 2025

Dear Christina

**Fundamentals of Mobile and Pervasive Computing by Frank Adelstein,  
Sandeep K. S. Gupta, Golden G. Richard III and Loren Schwiebert – McGraw-  
Hill, 2005. Shelf mark: YK.2007.a.14266**

According to our records, this item was receipted by The British Library on **2 May 2007** and would have been available for public use from that date.

A copy of the title and copyright page a stamp indicating the date of availability has been attached along with the contents pages and Appendix A.

Please note that we can only provide the date that the British Library made this item available for public use; for the actual date of publication, please contact the publisher.

Yours sincerely

**Tony Corsini**

British Library Research Service  
Tel: +44 (0) 20 7412 7903 bipc-research@bl.uk

McGRAW-HILL PROFESSIONAL ENGINEERING



# Fundamentals of Mobile and Pervasive Computing

- ✓ Embedded wireless sensor networking
- ✓ Wireless security
- ✓ Ubiquitous computing
- ✓ Middleware

---

Frank Adelstein  
Sandeep K.S. Gupta  
Golden G. Richard III  
Loren Schwiebert

---

# **Fundamentals of Mobile and Pervasive Computing**

**Frank Adelstein  
Sandeep K. S. Gupta  
Golden G. Richard III  
Loren Schwiebert**

**McGraw-Hill**

New York Chicago San Francisco Lisbon London Madrid  
Mexico City Milan New Delhi San Juan Seoul  
Singapore Sydney Toronto

The McGraw-Hill Companies

CIP Data is on file with the Library of Congress

Copyright © 2005 by The McGraw-Hill Companies, Inc. All rights reserved. Printed in the United States of America. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a data base or retrieval system, without the prior written permission of the publisher.

2 3 4 5 6 7 8 9 0 IBT / IBT 0 1 0 9 8 7

ISBN 978-0-07-141237-7

ISBN 0-07-141237-9

*The sponsoring editor for this book was Stephen S. Chapman and the production supervisor was Sherri Souffrance. It was set in Century Schoolbook by International Typesetting and Composition. The art director for the cover was Anthony Landi.*

Printed and bound by IBT Global.

McGraw-Hill books are available at special quantity discounts to use as premiums and sales promotions, or for use in corporate training programs. For more information, please write to the Director of Special Sales, McGraw-Hill Professional, Two Penn Plaza, New York, NY 10121-2298. Or contact your local bookstore.



This book is printed on recycled, acid-free paper containing a minimum of 50% recycled, de-inked fiber.

Information contained in this work has been obtained by The McGraw-Hill Companies, Inc. ("McGraw-Hill") from sources believed to be reliable. However, neither McGraw-Hill nor its authors guarantee the accuracy or completeness of any information published herein and neither McGraw-Hill nor its authors shall be responsible for any errors, omissions, or damages arising out of use of this information. This work is published with the understanding that McGraw-Hill and its authors are supplying information but are not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought.



To my f

---

# Contents

|                                                               |           |
|---------------------------------------------------------------|-----------|
| Preface                                                       | xv        |
| Acknowledgments                                               | xix       |
| <br>                                                          |           |
| <b>Chapter 1. Mobile Adaptive Computing</b>                   | <b>1</b>  |
| 1.1 What Is Mobile Computing?                                 | 1         |
| 1.2 Adaptability—The Key to Mobile Computing                  | 3         |
| 1.2.1 Transparency                                            | 4         |
| 1.2.2 Constraints of mobile computing environments            | 5         |
| 1.2.3 Application-aware adaptation                            | 6         |
| 1.3 Mechanisms for Adaptation                                 | 8         |
| 1.3.1 Adapting functionality                                  | 8         |
| 1.3.2 Adapting data                                           | 9         |
| 1.4 How to Develop or Incorporate Adaptations in Applications | 11        |
| 1.4.1 Where can adaptations be performed?                     | 12        |
| 1.5 Support for Building Adaptive Mobile Applications         | 19        |
| 1.5.1 Odyssey                                                 | 19        |
| 1.5.2 Rover                                                   | 22        |
| 1.6 Summary                                                   | 24        |
| <br>                                                          |           |
| <b>Chapter 2. Mobility Management</b>                         | <b>27</b> |
| 2.1 Mobility Management                                       | 27        |
| 2.2 Location Management Principles and Techniques             | 30        |
| 2.2.1 Registration area-based location management             | 33        |
| 2.3 Location Management Case Studies                          | 48        |
| 2.3.1 PCS location management scheme                          | 49        |
| 2.3.2 Mobile IP                                               | 50        |
| 2.4 Summary                                                   | 53        |
| <br>                                                          |           |
| <b>Chapter 3. Data Dissemination and Management</b>           | <b>55</b> |
| 3.1 Challenges                                                | 59        |
| 3.2 Data Dissemination                                        | 61        |
| 3.2.1 Bandwidth allocation for publishing                     | 63        |
| 3.2.2 Broadcast disk scheduling                               | 65        |

|                                                                             |     |                   |
|-----------------------------------------------------------------------------|-----|-------------------|
| 3.3 Mobile Data Caching                                                     | 67  | 6.2 Mobile Ag     |
| 3.3.1 Caching in traditional distributed systems                            | 68  | 6.2.1 Wh          |
| 3.3.2 Cache consistency maintenance                                         | 69  | 6.2.2 Ag          |
| 3.3.3 Performance and architectural issues                                  | 70  | 6.2.3 Mi          |
| 3.4 Mobile Cache Maintenance Schemes                                        | 72  | 6.2.4 Co          |
| 3.4.1 A taxonomy of cache maintenance schemes                               | 72  | 6.3 Summary       |
| 3.4.2 Cache maintenance for push-based information dissemination            | 74  |                   |
| 3.4.3 Broadcasting invalidation reports                                     | 75  | Chapter 7. Servi  |
| 3.4.4 Disconnected operation                                                | 77  | 7.1 Common        |
| 3.4.5 Asynchronous stateful (AS) scheme                                     | 78  | 7.2 Services      |
| 3.4.6 To cache or not to cache?                                             | 84  | 7.2.1 Un          |
| 3.5 Mobile Web Caching                                                      | 86  | 7.2.2 Sta         |
| 3.5.1 Handling disconnections                                               | 87  | 7.2.3 Te          |
| 3.5.2 Achieving energy and bandwidth efficiency                             | 87  | 7.2.4 Usi         |
| 3.6 Summary                                                                 | 88  | 7.3 More on C     |
|                                                                             |     | 7.3.1 Un          |
| Chapter 4. Context-Aware Computing                                          | 91  | 7.3.2 Mu          |
| 4.1 Ubiquitous or Pervasive Computing                                       | 92  | 7.3.3 Ser         |
| 4.2 What Is a Context? Various Definitions and Types of Contexts            | 94  | 7.4 Garbage C     |
| 4.2.1 Enumeration-based                                                     | 94  | 7.4.1 Lea         |
| 4.2.2 Role-based                                                            | 96  | 7.4.2 Ad          |
| 4.3 Context-Aware Computing and Applications                                | 96  | 7.5 Eventing      |
| 4.3.1 Core capabilities for context awareness                               | 97  | 7.6 Security      |
| 4.3.2 Types of context-aware applications                                   | 98  | 7.6.1 Jin         |
| 4.3.3 Developing context-aware applications                                 | 100 | 7.6.2 Ser         |
| 4.4 Middleware Support                                                      | 102 | 7.6.3 Nin         |
| 4.4.1 Contextual services                                                   | 103 | 7.7 Interopera    |
| 4.4.2 Actuator service                                                      | 104 | 7.7.1 Inte        |
| 4.4.3 An example: context toolkit                                           | 104 | 7.8 Summary       |
| 4.4.4 Providing location context                                            | 105 |                   |
| 4.5 Summary                                                                 | 106 | Chapter 8. Introc |
|                                                                             |     | 8.1 Overview      |
| Chapter 5. Introduction to Mobile Middleware                                | 109 | 8.1.1 Out         |
| 5.1 What Is Mobile Middleware?                                              | 109 | 8.2 Properties    |
| 5.2 Adaptation                                                              | 110 | 8.2.1 No          |
| 5.3 Agents                                                                  | 111 | 8.2.2 Lim         |
| 5.4 Service Discovery                                                       | 111 | 8.2.3 Pow         |
|                                                                             |     | 8.2.4 No          |
| Chapter 6. Middleware for Application Development:<br>Adaptation and Agents | 113 | 8.3 Unique Fe     |
| 6.1 Adaptation                                                              | 113 | 8.3.1 Dire        |
| 6.1.1 The spectrum of adaptation                                            | 114 | 8.3.2 Usu         |
| 6.1.2 Resource monitoring                                                   | 114 | 8.3.3 Ver         |
| 6.1.3 Characterizing adaptation strategies                                  | 115 | 8.3.4 Ope         |
| 6.1.4 An application-aware adaptation architecture: Odyssey                 | 117 | 8.3.5 Spe         |
| 6.1.5 A sample Odyssey application                                          | 119 | 8.4 Proposed      |
| 6.1.6 More adaptation middleware                                            | 120 | 8.4.1 Mil         |
|                                                                             |     | 8.4.2 Mec         |
|                                                                             |     | 8.4.3 Ind         |
|                                                                             |     | 8.4.4 Env         |
|                                                                             |     | 8.4.5 Oth         |

|     |            |                                                                  |     |
|-----|------------|------------------------------------------------------------------|-----|
| 67  |            |                                                                  |     |
| 68  |            |                                                                  |     |
| 69  |            | 6.2 Mobile Agents                                                | 123 |
| 70  |            | 6.2.1 Why mobile agents? And why not?                            | 125 |
| 72  |            | 6.2.2 Agent architectures                                        | 127 |
| 72  |            | 6.2.3 Migration strategies                                       | 130 |
| 72  |            | 6.2.4 Communication strategies                                   | 131 |
| 74  | semination | 6.3 Summary                                                      | 133 |
| 75  |            |                                                                  |     |
| 77  |            | Chapter 7. Service Discovery Middleware: Finding Needed Services | 137 |
| 78  |            | 7.1 Common Ground                                                | 140 |
| 84  |            | 7.2 Services                                                     | 142 |
| 86  |            | 7.2.1 Universally unique identifiers                             | 142 |
| 87  |            | 7.2.2 Standardization                                            | 144 |
| 87  |            | 7.2.3 Textual descriptions                                       | 145 |
| 88  |            | 7.2.4 Using interfaces for standardization                       | 149 |
|     |            | 7.3 More on Discovery and Advertisement Protocols                | 150 |
| 91  |            | 7.3.1 Unicast discovery                                          | 150 |
| 92  |            | 7.3.2 Multicast discovery and advertisement                      | 151 |
| 94  | cts        | 7.3.3 Service catalogs                                           | 155 |
| 94  |            | 7.4 Garbage Collection                                           | 156 |
| 96  |            | 7.4.1 Leasing                                                    | 156 |
| 96  |            | 7.4.2 Advertised expirations                                     | 158 |
| 97  |            | 7.5 Eventing                                                     | 159 |
| 98  |            | 7.6 Security                                                     | 163 |
| 100 |            | 7.6.1 Jini                                                       | 163 |
| 102 |            | 7.6.2 Service location protocol                                  | 164 |
| 103 |            | 7.6.3 Ninja                                                      | 165 |
| 104 |            | 7.7 Interoperability                                             | 166 |
| 104 |            | 7.7.1 Interoperability success stories                           | 167 |
| 105 |            | 7.8 Summary                                                      | 167 |
| 106 |            |                                                                  |     |
|     |            | Chapter 8. Introduction to Ad Hoc and Sensor Networks            | 171 |
| 109 |            | 8.1 Overview                                                     | 171 |
|     |            | 8.1.1 Outline of chapter                                         | 172 |
| 109 |            | 8.2 Properties of an Ad Hoc Network                              | 175 |
| 110 |            | 8.2.1 No preexisting infrastructure                              | 175 |
| 111 |            | 8.2.2 Limited access to a base station                           | 175 |
| 111 |            | 8.2.3 Power-limited devices                                      | 177 |
|     |            | 8.2.4 No centralized mechanisms                                  | 178 |
|     |            | 8.3 Unique Features of Sensor Networks                           | 178 |
|     |            | 8.3.1 Direct interaction with the physical world                 | 178 |
| 113 |            | 8.3.2 Usually special-purpose devices                            | 179 |
|     |            | 8.3.3 Very limited resources                                     | 180 |
| 113 |            | 8.3.4 Operate without a human interface                          | 181 |
| 114 |            | 8.3.5 Specialized routing patterns                               | 181 |
| 114 |            | 8.4 Proposed Applications                                        | 182 |
| 115 |            | 8.4.1 Military applications                                      | 182 |
| 117 | ay         | 8.4.2 Medical applications                                       | 185 |
| 119 |            | 8.4.3 Industrial applications                                    | 186 |
| 120 |            | 8.4.4 Environmental applications                                 | 187 |
|     |            | 8.4.5 Other application domains                                  | 188 |

|                                        |            |
|----------------------------------------|------------|
| <b>Chapter 9. Challenges</b>           | <b>191</b> |
| 9.1 Constrained Resources              | 191        |
| 9.1.1 No centralized authority         | 192        |
| 9.1.2 Limited power                    | 193        |
| 9.1.3 Wireless communication           | 196        |
| 9.1.4 Limited computation and storage  | 197        |
| 9.1.5 Storage constraints              | 198        |
| 9.1.6 Limited input and output options | 199        |
| 9.2 Security                           | 200        |
| 9.2.1 Small keys                       | 200        |
| 9.2.2 Limited computation              | 201        |
| 9.2.3 Changing network membership      | 201        |
| 9.2.4 Arbitrary topology               | 202        |
| 9.3 Mobility                           | 203        |
| 9.3.1 Mobility requirements            | 204        |
| 9.3.2 Loss of connectivity             | 205        |
| 9.3.3 Data loss                        | 206        |
| 9.3.4 Group communication              | 207        |
| 9.3.5 Maintaining consistent views     | 208        |
| 9.4 Summary                            | 209        |

|                                                    |            |
|----------------------------------------------------|------------|
| <b>Chapter 10. Protocols</b>                       | <b>213</b> |
| 10.1 Autoconfiguration                             | 213        |
| 10.1.1 Neighborhood discovery                      | 214        |
| 10.1.2 Topology discovery                          | 215        |
| 10.1.3 Medium access control schedule construction | 216        |
| 10.1.4 Security protocol configuration             | 220        |
| 10.2 Energy-Efficient Communication                | 221        |
| 10.2.1 Multihop routing                            | 222        |
| 10.2.2 Communication scheduling                    | 225        |
| 10.2.3 Duplicate message suppression               | 226        |
| 10.2.4 Message aggregation                         | 228        |
| 10.2.5 Dual-radio scheduling                       | 230        |
| 10.2.6 Sleep-mode scheduling                       | 232        |
| 10.2.7 Clustering                                  | 232        |
| 10.3 Mobility Requirements                         | 235        |
| 10.3.1 Movement detection                          | 235        |
| 10.3.2 Patterns of movement                        | 236        |
| 10.3.3 Changing group dynamics                     | 237        |
| 10.3.4 Resynchronization                           | 239        |
| 10.4 Summary                                       | 240        |

|                                             |            |
|---------------------------------------------|------------|
| <b>Chapter 11. Approaches and Solutions</b> | <b>245</b> |
| 11.1 Deployment and Configuration           | 245        |
| 11.1.1 Random deployment                    | 246        |
| 11.1.2 Scalability                          | 246        |
| 11.1.3 Self-organization                    | 247        |
| 11.1.4 Security protocol configuration      | 247        |

|                  |
|------------------|
| 11.1.5 Re        |
| 11.1.6 Lo        |
| 11.2 Routing     |
| 11.2.1 Ev        |
| 11.2.2 Pe        |
| 11.2.3 Dif       |
| 11.2.4 Dir       |
| 11.2.5 Gr        |
| 11.2.6 Sy        |
| 11.3 Fault Toler |
| 11.3.1 FE        |
| 11.3.2 Ag        |
| me               |
| 11.3.3 De        |
| 11.4 Energy Effi |
| 11.4.1 Uni       |
| 11.4.2 Ser       |
| 11.4.3 MA        |
| 11.4.4 Tra       |
| 11.5 Summary     |

|                           |
|---------------------------|
| <b>Chapter 12. Wirele</b> |
| 12.1 Traditional S        |
| 12.1.1 Inte               |
| 12.1.2 Con                |
| 12.1.3 Non                |
| 12.1.4 Ava                |
| 12.2 Mobile and           |
| 12.2.1 Dete               |
| 12.2.2 Res                |
| 12.2.3 Phys               |
| 12.2.4 Thef               |
| 12.2.5 War                |
| 12.3 Mobility             |
| 12.4 Problems in          |
| 12.4.1 Rou                |
| 12.4.2 Prek               |
| 12.4.3 Rec                |
| 12.4.4 Host               |
| 12.5 Additional Is        |
| 12.5.1 Liabi              |
| 12.5.2 Fear               |
| 12.5.3 Frau               |
| 12.5.4 Big t              |
| 12.6 Additional Ty        |
| 12.6.1 "Man               |
| 12.6.2 Traffi             |
| 12.6.3 Repl               |
| 12.6.4 Buffe              |
| 12.7 Summary              |

|     |                                                                   |     |
|-----|-------------------------------------------------------------------|-----|
| 191 | 11.1.5 Reconfiguration/redeployment                               | 249 |
| 191 | 11.1.6 Location determination                                     | 249 |
| 192 | 11.2 Routing                                                      | 252 |
| 193 | 11.2.1 Event-driven routing                                       | 253 |
| 196 | 11.2.2 Periodic sensor readings                                   | 254 |
| 197 | 11.2.3 Diffusion routing                                          | 260 |
| 198 | 11.2.4 Directional routing                                        | 265 |
| 199 | 11.2.5 Group communication                                        | 268 |
| 200 | 11.2.6 Synchronization                                            | 271 |
| 200 | 11.3 Fault Tolerance and Reliability                              | 273 |
| 201 | 11.3.1 FEC and ARQ                                                | 273 |
| 201 | 11.3.2 Agreement among sensor nodes (Reliability of measurements) | 274 |
| 202 | 11.3.3 Dealing with dead or faulty nodes                          | 278 |
| 203 | 11.4 Energy Efficiency                                            | 279 |
| 204 | 11.4.1 Uniform power dissipation                                  | 280 |
| 205 | 11.4.2 Sensor component power management                          | 281 |
| 206 | 11.4.3 MAC layer protocols                                        | 282 |
| 207 | 11.4.4 Tradeoffs between performance and energy efficiency        | 283 |
| 208 | 11.5 Summary                                                      | 284 |
| 209 |                                                                   |     |
| 213 | Chapter 12. Wireless Security                                     | 287 |
| 213 | 12.1 Traditional Security Issues                                  | 287 |
| 214 | 12.1.1 Integrity                                                  | 287 |
| 215 | 12.1.2 Confidentiality                                            | 288 |
| 216 | 12.1.3 Nonrepudiation                                             | 288 |
| 220 | 12.1.4 Availability                                               | 288 |
| 221 | 12.2 Mobile and Wireless Security Issues                          | 290 |
| 222 | 12.2.1 Detectability                                              | 290 |
| 225 | 12.2.2 Resource depletion/exhaustion                              | 291 |
| 226 | 12.2.3 Physical intercept problems                                | 291 |
| 228 | 12.2.4 Theft of service                                           | 291 |
| 230 | 12.2.5 War driving/walking/chalking                               | 292 |
| 232 | 12.3 Mobility                                                     | 293 |
| 232 | 12.4 Problems in Ad Hoc Networks                                  | 293 |
| 235 | 12.4.1 Routing                                                    | 294 |
| 235 | 12.4.2 Prekeying                                                  | 294 |
| 236 | 12.4.3 Reconfiguring                                              | 295 |
| 237 | 12.4.4 Hostile environment                                        | 295 |
| 239 | 12.5 Additional Issues: Commerce                                  | 295 |
| 240 | 12.5.1 Liability                                                  | 296 |
|     | 12.5.2 Fear, uncertainty, and doubt                               | 296 |
|     | 12.5.3 Fraud                                                      | 296 |
| 245 | 12.5.4 Big bucks at stake                                         | 297 |
| 245 | 12.6 Additional Types of Attacks                                  | 297 |
| 246 | 12.6.1 "Man in the middle" attacks                                | 297 |
| 246 | 12.6.2 Traffic analysis                                           | 298 |
| 247 | 12.6.3 Replay attacks                                             | 298 |
| 247 | 12.6.4 Buffer-overflow attacks                                    | 298 |
| 247 | 12.7 Summary                                                      | 299 |

|                                                                    |                |
|--------------------------------------------------------------------|----------------|
| <b>Chapter 13. Approaches to Security</b>                          | <b>301</b>     |
| 13.1 Limit the Signal                                              | 301            |
| 13.1.1 Wire integrity and tapping                                  | 301            |
| 13.1.2 Physical limitation                                         | 301            |
| 13.2 Encryption                                                    | 302            |
| 13.2.1 Public and private key encryption                           | 302            |
| 13.2.2 Computational and data overhead                             | 303            |
| 13.3 Integrity Codes                                               | 304            |
| 13.3.1 Checksum versus cryptographic hash                          | 304            |
| 13.3.2 Message authentication code (MAC)                           | 305            |
| 13.3.3 Payload versus header                                       | 306            |
| 13.3.4 Traffic analysis                                            | 307            |
| 13.4 IPSec                                                         | 307            |
| 13.4.1 Authentication header (AH)                                  | 307            |
| 13.4.2 Encapsulating security payload (ESP)                        | 308            |
| 13.5 Other Security-Related Mechanisms                             | 308            |
| 13.5.1 Authentication protocols                                    | 308            |
| 13.5.2 AAA                                                         | 313            |
| 13.5.3 Special hardware                                            | 315            |
| 13.6 Summary                                                       | 315            |
| <br><b>Chapter 14. Security in Wireless Personal Area Networks</b> | <br><b>317</b> |
| 14.1 Basic Idea                                                    | 317            |
| 14.1.1 Bluetooth specifications                                    | 317            |
| 14.1.2 Bluetooth network terms                                     | 318            |
| 14.1.3 Bluetooth security mechanisms                               | 320            |
| 14.2 Bluetooth Security Modes                                      | 320            |
| 14.3 Basic Security Mechanisms                                     | 321            |
| 14.3.1 Initialization key                                          | 322            |
| 14.3.2 Unit key                                                    | 322            |
| 14.3.3 Combination key                                             | 322            |
| 14.3.4 Master key                                                  | 323            |
| 14.4 Encryption                                                    | 323            |
| 14.5 Authentication                                                | 325            |
| 14.6 Limitations and Problems                                      | 325            |
| 14.7 Summary                                                       | 327            |
| <br><b>Chapter 15. Security in Wireless Local Area Networks</b>    | <br><b>329</b> |
| 15.1 Basic Idea                                                    | 329            |
| 15.2 Wireless Alphabet Soup                                        | 331            |
| 15.3 Wired-Equivalent Privacy (WEP)                                | 333            |
| 15.3.1 WEP goals                                                   | 333            |
| 15.3.2 WEP data frame                                              | 334            |
| 15.3.3 WEP encryption                                              | 334            |
| 15.3.4 WEP decryption                                              | 335            |
| 15.3.5 WEP authentication                                          | 335            |
| 15.3.6 WEP flaws                                                   | 336            |
| 15.3.7 WEP fixes                                                   | 338            |

|                  |
|------------------|
| 15.4 WPA         |
| 15.5 802.11i     |
| 15.5.1 Enc       |
| 15.5.2 Acc       |
| 15.6 Fixes and " |
| 15.6.1 Any       |
| 15.6.2 Knc       |
| 15.6.3 Use       |
| 15.6.4 Enc       |
| 15.6.5 Fire      |
| 15.6.6 Use       |
| 15.7 Summary     |

|                          |
|--------------------------|
| <b>Chapter 16. Secur</b> |
| 16.1 Broadband           |
| 16.2 IEEE 802.16         |
| 16.3 802.16 Secu         |
| 16.3.1 Key               |
| 16.3.2 Seci              |
| 16.3.3 Keyi              |
| 16.3.4 Sub               |
| 16.3.5 Enci              |
| 16.4 Problems ar         |
| 16.5 Summary             |

|                           |
|---------------------------|
| <b>Chapter 17. Securi</b> |
| 17.1 Basic Idea           |
| 17.2 CDMA                 |
| 17.3 GSM                  |
| 17.3.1 GSM                |
| 17.3.2 GSM                |
| 17.4 Problems wi          |
| 17.4.1 Sess               |
| 17.4.2 Weal               |
| 17.4.3 Enchr              |
| 17.4.4 Limit              |
| 17.4.5 Othe               |
| 17.5 The Four Ger         |
| 17.6 3G                   |
| 17.7 Limitations          |
| 17.8 Summary              |

|                  |
|------------------|
| Appendix A Brief |
| and N            |
| Appendix B Ques  |
| Index 389        |

|     |                                                                      |     |
|-----|----------------------------------------------------------------------|-----|
| 301 | 15.4 WPA                                                             |     |
| 301 | 15.5 802.11i                                                         | 340 |
| 301 | 15.5.1 Encryption protocols                                          | 340 |
| 301 | 15.5.2 Access control via 802.1x                                     | 340 |
| 302 | 15.6 Fixes and "Best Practices"                                      | 342 |
| 302 | 15.6.1 Anything is better than nothing                               | 344 |
| 303 | 15.6.2 Know thine enemy                                              | 344 |
| 304 | 15.6.3 Use whatever wireless security mechanisms are present         | 344 |
| 304 | 15.6.4 End-to-end VPN                                                | 345 |
| 305 | 15.6.5 Firewall protection                                           | 345 |
| 306 | 15.6.6 Use whatever else is available                                | 346 |
| 307 | 15.7 Summary                                                         | 348 |
| 307 |                                                                      |     |
| 308 | Chapter 16. Security in Wireless Metropolitan Area Networks (802.16) | 349 |
| 308 | 16.1 Broadband Wireless Access                                       | 349 |
| 308 | 16.2 IEEE 802.16                                                     | 350 |
| 313 | 16.3 802.16 Security                                                 | 350 |
| 315 | 16.3.1 Key management                                                | 351 |
| 315 | 16.3.2 Security associations                                         | 351 |
|     | 16.3.3 Keying material lifetime                                      | 352 |
|     | 16.3.4 Subscriber station (SS) authorization                         | 353 |
| 317 | 16.3.5 Encryption                                                    | 353 |
| 317 | 16.4 Problems and Limitations                                        | 354 |
| 317 | 16.5 Summary                                                         | 354 |
| 318 |                                                                      |     |
| 320 | Chapter 17. Security in Wide Area Networks                           | 357 |
| 320 | 17.1 Basic Idea                                                      | 357 |
| 321 | 17.2 CDMA                                                            | 359 |
| 322 | 17.3 GSM                                                             | 360 |
| 322 | 17.3.1 GSM authentication                                            | 360 |
| 323 | 17.3.2 GSM encryption                                                | 360 |
| 323 | 17.4 Problems with GSM Security                                      | 361 |
| 325 | 17.4.1 Session life                                                  | 362 |
| 325 | 17.4.2 Weak encryption algorithm                                     | 362 |
| 327 | 17.4.3 Encryption between mobile host and base station only          | 363 |
|     | 17.4.4 Limits to the secret key                                      | 363 |
|     | 17.4.5 Other problems                                                | 364 |
| 329 | 17.5 The Four Generations of Wireless: 1G-4G                         | 364 |
| 329 | 17.6 3G                                                              | 364 |
| 331 | 17.7 Limitations                                                     | 366 |
| 333 | 17.8 Summary                                                         | 366 |
| 333 |                                                                      |     |
| 334 | Appendix A Brief Introduction to Wireless Communication              | 369 |
| 334 | and Networking                                                       |     |
| 335 | Appendix B Questions                                                 | 375 |
| 335 | Index                                                                | 389 |
| 336 |                                                                      |     |
| 338 |                                                                      |     |

## Brief Introduction to Wireless Communication and Networking

### A.1 Wireless Communication Basics

Similar to wired communication, a one-way (simplex) wireless communication requires a *transmitter* (transmitter electronics plus antenna) generating (electromagnetic) signals that can be properly received and deciphered by a *receiver* (receiving electronics plus antenna). Bidirectional communication requires a pair of *transceivers*—each transceiver consists of a transmitter and a receiver. Although it is possible for a transceiver to be designed such that it can transmit and receive at the same time, for various reasons such as the cost of the unit and its weight, a transceiver is designed with shared components (such as antenna) between its transmitter and receiver—leading it to either send or receive signals at any given time. Hence, bidirectional communication in wireless networks is usually half duplex. Various factors such as the power used for amplification of the wireless signal, properties of the medium, sensitivity of the receiver, and the signal interference from various other sources affect the distance at which a wireless transceiver's signal can be received. Directionality of the transceiver's antenna also plays a crucial role in this. An *omnidirectional antenna* radiates signals with almost equal strength in all the directions, whereas a *directional antenna* radiates signals with substantially more strength in some directions than others. The region around a transceiver within which the signal of a transceiver can be satisfactorily received is called the *coverage area* of the transceiver. Conceptually, a bidirectional wireless link exists between a pair of transceivers within the coverage area of each other since each

can receive signals sent by the other. All other factors remaining constant, the coverage area of a transceiver can be increased or decreased by adjusting the power used for amplifying the signal.

Suppose that the receiver and the transmitter are separated by a distance  $R$ . The average power  $P_r$  of the signal received by the receiver is proportional to the (average) power  $P_t$  of the transmitted signal. Under some simplifying assumptions (which we will not go into here) the relationship between  $P_t$  and  $P_r$  can be expressed as follows:

$$P_r = \frac{P_l K}{R^a} \quad (1)$$

where  $\alpha$  is the propagation loss exponent and  $K$  is the proportionality constant, which depends on the characteristics of the antennas. The value of the propagation loss exponent is usually between 2 and 5. It should be noted here that the above relationship holds when the receiving antenna is in the far-field region (as opposed to near-field region), i.e.,  $R$  is greater than some minimum distance that marks the boundary of the near-field region around the transmitting antenna.

Depending on the sensitivity of the receiver, the received power has to be greater than a certain minimum threshold value  $P_{r\text{-th}}$  for the receiver to be able to detect the transmitted signal. Hence the maximum distance  $R_{\text{max}}$  that a receiver can be from the transmitter and still detect the signal from it can be determined from Eq. (1):

$$R_{\max} = \left( \frac{P_t K}{P_{r,\text{th}}} \right)^{1/a} \quad (2)$$

As can be seen from Eq. (2), as  $P_t$  increases  $R_{\max}$  increases, although very slowly.

Conceptually,  $R_{\max}$  is the radius of the region around the transmitter within which a mobile unit can communicate with a transmitter, called the *cell* (assuming an omnidirectional transmitting antenna). In reality, the cell boundary in a given direction may depend on many factors such as the directionality of the antenna and the terrain. So, although we denote the cells as circular regions, in reality a cell may have very irregular geometry. In fact there are two power thresholds that may be associated with the receiver:

1.  $P_{r\text{-th-detect}}$ : the threshold above which the transmitter detects that the channel is busy and refrains from transmission.
2.  $P_{r\text{-th-recv}}$ : the threshold above which the transmitter is able to correctly receive a packet.

Obviously,  $P$

Wireless tran  
frequency rang  
tent with the fr  
require a licens  
Industrial Scie  
licenses for usin  
user abides by  
greater than 1

The signal power spectral density (PSD) is the frequency of the signal. The PSD is the power per unit frequency. Hence, at high frequencies, the power is low. In the line-of-sight (LOS) region, the signal is received from various objects. Wireless signal fading is a result of the term fading and the available bandwidth. The results in much more in-depth coverage of fading and books available.

## A.2 Wireless

There are seven  
Figure A.1 shows  
tures. Figure A.  
ecture, Fig. A.  
(3) shows a mo  
tures is desc

### A.2.1 Wireless LAN and mobile IP

An access point connected to the wireless link with 802.11 or Bluetooth (appropriate protocols for the receiver) to communicate with Wireless LANs "spots" or "oases" like shopping malls, and

aining constant,  
r decreased by

arated by a dis-  
e receiver is pro-  
al. Under some  
the relationship

(1)

proportionality  
e antennas. The  
ween 2 and 5. It  
when the receiv-  
ear-field region),  
arks the bound-  
ntenna.  
eived power has  
lue  $P_{r-th}$  for the  
ce the maximum  
r and still detect

(2)

reases, although

d the transmitter  
ansmitter, called  
ntenna). In real-  
l on many factors  
ain. So, although  
ll may have very  
olds that may be

itter detects that  
n.

is able to correctly

Obviously,  $P_{r-th-detect} \leq P_{r-th-recv} \rightarrow R_{max-detect} \geq R_{max-recv}$ .

Wireless transceivers are usually designed to operate within a certain frequency range called a *frequency band*. Frequency bands are consistent with the frequency bands allocated by the FCC. Most of these bands require a license issued by the FCC to use them. The exceptions are the Industrial Scientific and Medical (ISM) bands that do not require licenses for using them, and hence they can be freely used as long as the user abides by the FCC guidelines of not using transmission power greater than 1 W.

The signal propagation properties vary with the frequency. As the frequency of the signal increases, its penetrability decreases and the distance to which it can propagate within a medium (say air) decreases. Hence, at higher frequencies (such as infrared) the transceivers have to be in the line-of-sight of each other. At lower frequencies (such as radio frequencies) the line-of-sight is not required, since signal can be reflected from various objects and reach the receiver from various indirect paths. Wireless signals experience fading. There are two types of fading: short-term fading and long-term fading. This results in severe variability of the available bandwidth of a wireless link. Fading in a wireless medium results in much higher bit error rates than in wired communication. For more in-depth coverage, interested readers can consult many excellent books available on wireless communication (Rappaport, 1996).

## A.2 Wireless Network Architectures

There are several types of wireless networks being currently used. Figure A.1 shows three different types of mobile network architectures. Figure A.1 (1) shows a wireless LAN and mobile IP-based architecture, Fig. A.1 (2) shows a mobile cellular architecture, and Fig. A.1 (3) shows a mobile ad hoc network architecture. Each of these architectures is described below.

### A.2.1 Wireless local area network (WLANs) and mobile IP

An access point (AP) is usually a (mostly static) wireless transceiver connected to the wired network. A mobile station can establish a bidirectional link with an access point using a common protocol such as IEEE 802.11 or Bluetooth. Of course, the mobile station has to have the appropriate protocol stack and hardware (e.g., PCMCIA card or built-in transceiver) to communicate with an IEEE 802.11 or a Bluetooth access point. Wireless LANs are being used to provide wireless access called "hot spots" or "oases" in places such as airports, coffee shops, hotels, shopping malls, and homes. A wireless LAN permits mobility within the

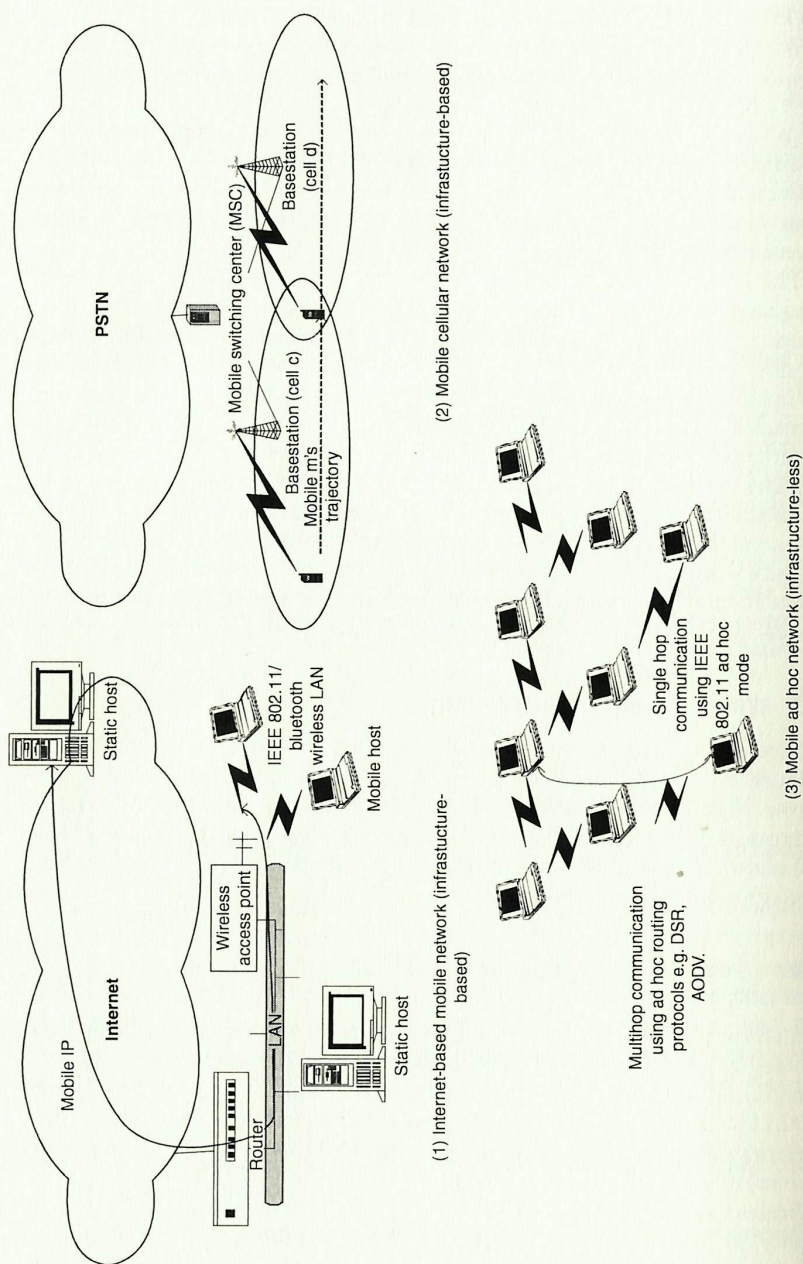


Figure A.1 Different types of mobile networks.

coverage area of the coverage of RFIDS, around this can range around 300 m satellite cells Mobile IP is a less mobility

## A.2.2 Wireless

In a wireless (BS), are deployed the range of a communicate with each wireless) network cell.

When an application in communication it (or the system) in order to connect a cellular network allow a smooth to another. Full (bandwidth) is channel is wide enough. Adjoining interference.

**Mobile ad hoc** established by an application capability establishing a computer is likely deliver a packet routing protocol routing (DSR) mobile ad hoc of the network in the network node's energy in the development networks is an

coverage area of the access point. For short-range technology, the radius of the coverage area can be a few meters (e.g., around few meters for RFIDS, around 10 m for Bluetooth), whereas for long-range technology this can range from several hundred to several thousand meters (e.g., around 300 m for IEEE 802.11 Wireless LANs, several kilometers for satellite cells). Protocols such as mobile IP provide wide-area mobility. Mobile IP is an extension of the Internet Protocol (IP) to support seamless mobility across IP networks.

### A.2.2 Wireless cellular networks

In a wireless cellular network, several access points, called base stations (BS), are deployed such that each location in the service area is within the range of at least one base station. These base stations can communicate with each other and other static computers via a wired (or another wireless) network. The coverage area of a base station is called its (wireless) cell.

When an active mobile station (a mobile unit that is actively involved in communication) moves out of the coverage area of one base station, it (or the system) tries to establish a connection to another base station in order to continue communicating this process is called a *hand-off*. In a cellular network, cells of adjoining base stations usually overlap to allow a smooth hand-off of a mobile's connections from one base station to another. Further, in wireless telephony the available frequency range (bandwidth) is divided into wireless communication channels. A channel is wide enough (minimum of 64 kbps) to accommodate one voice circuit. Adjoining cells use different (sets of) channels to reduce (co-channel) interference.

**Mobile ad hoc networks.** A mobile ad hoc network is a network established by an ad hoc group of mobile computers with wireless transmission capabilities. IEEE 802.11 has an ad hoc mode that permits establishing such networks. Since the transmission range of each mobile computer is limited, multihop packet transmission may be needed to deliver a packet to its destination mobile computer. Several multihop routing protocols have been developed, for example, dynamic source routing (DSR) and ad hoc distance vector (AODV). Multihop routing in mobile ad hoc networks poses several challenges. For one, the topology of the network changes as the nodes move around. Further, the nodes in the network are mostly battery powered and so an intermediate node's energy is depleted in forwarding a packet for someone else. Hence, the development of energy-efficient routing protocols for mobile ad hoc networks is an active area of research.

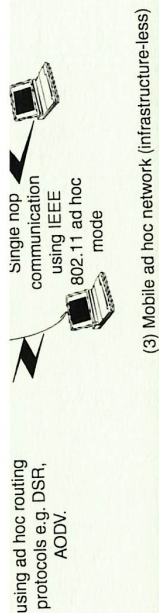


Figure A.1 Different types of mobile networks.

For more in-depth coverage, interested readers can consult many excellent books available on wireless and mobile networks (Pahlavan and Krishnamurthy, 2002).

### A.3 References

- T. Rappaport, *Wireless Communications and Principles*, Prentice Hall, Upper Saddle River, New Jersey, 1996.  
K. Pahlavan and P. Krishnamurthy, *Principles of Wireless Networks*, Prentice Hall, Upper Saddle River, New Jersey, 2002.

### Chapter

1. W  
co
2. C  
ir
3. C  
w
4. W  
E
5. A  
(s  
g  
a  
G  
rc  
cl
6. A  
d  
d  
th
7. A  
al  
on  
(s  
bo